Corporate Governance Committee

You are requested to attend a meeting of the Corporate Governance Committee to be held in The John Meikle Room, The Deane House, Belvedere Road, Taunton on 19 May 2014 at 18:15.

Agenda

1 Appointment of Chairman

2 Appointment of Vice-Chairman

3 Apologies.

4 Minutes of the meeting of the Corporate Governance Committee held on 10 March 2014 (attached).

5 Public Question Time.

6 Declaration of Interests
To receive declarations of personal or prejudicial interests, in accordance with the Code of Conduct.

7 External Audit Plan 2013/14. Report of the Grant Thornton Audit Manager (attached).

Reporting Officer: Peter Lappin

8 External Audit Update. Report of the Assistant Director Corporate Services and Grant Thornton Audit Manager (attached).

Reporting Officers: Peter Lappin
Richard Sealy

9 External Audit - Fees Report. Report of the Assistant Director Corporate Services (attached).

Reporting Officer: Richard Sealy

10 Regulations of Investigatory Powers Act (RIPA) - Policy and Procedure Update. Report of the Assistant Chief Executive and Monitoring Officer (attached).

Reporting Officer: Bruce Lang

11 Whistle Blowing Policy Refresh. Report of the Strategic Finance Officer (attachec).

Reporting Officer: Maggie Hammond

12 Money Laundering Policy Refresh. Report of the Strategic Finance Officer (attached).

Reporting Officer: Maggie Hammond

13 Update on the Internal Audit Plan 2013/14 actions from Corporate Governance Meeting 10 March 2014. Report of the Strategic Finance Officer and Assistant Director Corporate Services (attached).

Reporting Officers: Maggie Hammond
Richard Sealy

14 Corporate Governance Committee Forward Plan - details of forthcoming items to be considered by the Corporate Governance Committee and the opportunity for Members to suggest further items (attached)

Bruce Lang
Assistant Chief Executive

16 June 2014

Members of the public are welcome to attend the meeting and listen to the discussions.

There is time set aside at the beginning of most meetings to allow the public to ask questions.

Speaking under "Public Question Time" is limited to 4 minutes per person in an overall period of 15 minutes. The Committee Administrator will keep a close watch on the time and the Chairman will be responsible for ensuring the time permitted does not overrun. The speaker will be allowed to address the Committee once only and will not be allowed to participate further in any debate.

Except at meetings of Full Council, where public participation will be restricted to Public Question Time only, if a member of the public wishes to address the Committee on any matter appearing on the agenda, the Chairman will normally permit this to occur when that item is reached and before the Councillors begin to debate the item.

This is more usual at meetings of the Council's Planning Committee and details of the "rules" which apply at these meetings can be found in the leaflet "Having Your Say on Planning Applications". A copy can be obtained free of charge from the Planning Reception Desk at The Deane House or by contacting the telephone number or e-mail address below.

If an item on the agenda is contentious, with a large number of people attending the meeting, a representative should be nominated to present the views of a group.

These arrangements do not apply to exempt (confidential) items on the agenda where any members of the press or public present will be asked to leave the Committee Room.

Full Council, Executive, Committees and Task and Finish Review agendas, reports and minutes are available on our website: www.tauntondeane.gov.uk

 Lift access to the John Meikle Room and the other Committee Rooms on the first floor of The Deane House, is available from the main ground floor entrance. Toilet facilities, with wheelchair access, are also available off the landing directly outside the Committee Rooms.

 An induction loop operates to enhance sound for anyone wearing a hearing aid or using a transmitter.

For further information about the meeting, please contact the Corporate Support Unit on 01823 356414 or email r.bryant@tauntondeane.gov.uk

If you would like an agenda, a report or the minutes of a meeting translated into another language or into Braille, large print, audio tape or CD, please telephone us on 01823 356356 or email: **enquiries@tauntondeane.gov.uk**

Corporate Governance Committee Members:-

Councillor D Reed	(Chairman)
Councillor S Coles	(Vice-Chairman)
Councillor A Beaven	
Councillor B Denington	
Councillor E Gaines	
Councillor A Govier	
Councillor T Hall	
Councillor J Horsley	
Councillor J Hunt	
Councillor S Lees	
Councillor Miss F Smith	
Councillor P Smith	
Councillor V Stock-Williams	
Councillor Mrs E Waymouth	
Councillor A Wedderkopp	

AGENDA ITEM NO. 4

Corporate Governance Committee – 10 March 2014

Present: Councillor D Reed (Chairman)
Councillor Coles (Vice-Chairman)
Councillors Beaven, Denington, Hall, Horsley, Hunt, Mrs Stock-Williams, Tooze, Mrs Waymouth, D Wedderkopp and A Wedderkopp.

Officers: Catrin Brown (Health and Safety Officer), Kate Woollard (DLO Health and Safety Co-ordinator), Maggie Hammond (Strategic Finance Officer), Fiona Kirkham (Strategic ICT Lead), Heather Tiso (Head of Revenues and Benefits Service), Helen Vile (Overpayments, Investigation and Support Team Lead), Dan Webb (Performance Lead), Richard Sealy (Assistant Director Corporate Services), Shirlene Adam (Director of Operations) and Emma Hill (Corporate Support Officer).

Also Present: Peter Lappin (Audit Manager, Grant Thornton),
Sarah Crouch (Executive, Grant Thornton)
Alastair Woodland (South West Audit Partnership)

(The meeting commenced at 6.15 pm)

1. Apologies

Councillor Gaines, A Govier and R Lees

2. Minutes

The minutes of the meeting held on 9 December 2013 were taken as read and were signed.

3. Declaration of Interests

Councillors Coles, Hunt, D Wedderkopp and A Wedderkopp declared personal interests as Members of Somerset County Council. Councillor Tooze declared a personal interest as an employee of UK Hydrographic Office. Councillor D Reed declared a personal interest as a Director of the Taunton Town Centre Company.

4. Update on the Health and Safety Performance and Strategy for 2013 – 2014

Considered report previously circulated, which provided an update on the progress of a range of Health and Safety matters across the organisation.

The figures below were a comparison of summary of the accidents and incidents from 1 April 2013 to 31 March 2014:-

- Overall there had been 38 incidents or accidents. This was a reduction on last year's figures.
- Of which, 7 were Core Council, 28 were DLO and 3 were public.
- There had been 3 reportable incidents, 33 non-reportable and 2 near misses.

- There had been two accident investigations since 1 January 2014.

Whilst the Council did not have significant numbers of serious accidents, in order for appropriate lessons to be learned it was important to ensure that all incidents were reported. This would be addressed in the Health and Safety Strategy for 2014 -15 and the accident reporting procedure for the organisation.

The Strategy had been produced as a three year plan, which would be reviewed on an annual basis to ensure that key performance indicators remained applicable.

South West Audit Partnership (SWAP) was currently undertaking an audit of the Health and Safety service. The Strategy for 2014 - 15 addressed many of the weaknesses identified by the previous audit of the service.

Updates were also provided on the arrangements for the Health and Safety Committee and agreed actions, training on health and safety matters and the provision of health and safety information.

During the discussion of this item, Members made comments and statements and asked questions which included: - (Responses were shown in italics)

- It was felt that the timescales for incident and accident investigation stated were too long. The initial investigation should take place within the first week and concluded within three weeks. *The investigation timescales could be both longer and shorter than the stated timescales. This was dependant on the type of incident or accident and the number of witnesses.*
- DLO incident investigations should be sooner than within a week, due to the nature of the work and the incidents. This view was supported by Members.
- What was meant by a non-reportable incident? *This referred to incidents where the member of staff concerned did not require to take any time off work after the incident. The Council wanted to encourage all staff to report incidents or accidents no matter how minor to enable the Council to prevent these incidents from re-occurring or becoming more serious.*

Resolved that the report be noted.

5. Grant Thornton – Certification of Grant Claims

Considered report previously circulated, which presented the External Auditors findings from their 2012/2013 review work.

Grant Thornton and the Audit Commission had certified three claims and returns for the financial year, relating to expenditure of £79 million.

The Certification of Claims and Returns report highlighted several areas where improvements could be made and the action plan reflected this.

It was reported that the number of claims that required certification had reduced and also the Council had fewer claims amended in 2012/2013 than in 2011/2012.

The validation check report was discussed and it was recommended that future validation programme "bug" checks should be run before the claim was prepared.

Grant Thornton had explained previously that the fees varied from year to year depending on the complexity of the cases sampled. With the validation "bug" report not being run before the preparation of the claim meant that the results had to be followed up.

During the discussion of this item, Members made comments and statements and asked questions which included: - (Responses were shown in italics)

- Looking at the amber RAG alert, this would suggest to Members that there was still some concern regarding this area but this did not appear to be so from the accompanying text. *This area would have been green status if everything had been complete and satisfactory but there were a number of incomplete elements. Grant Thornton were not able to go through each individual grant claim due to the vast number of them so a sample was taken and this was audited and the results from this sample had been presented to Members.*
- Clarification was sought as to the breakdown of Grant Thornton's fees within the report. *The variance and differences in the fees related to the considerable amount of assistance from the Revenues and Benefits department.*

Resolved that the report be noted.

6. Grant Thornton – External Audit Update

Considered report previously circulated, on the External Audit Update.

The report provided a useful update on progress against each piece of 'regular' work carried out by our external auditors.

Additionally, the update report shared headlines on some national issues that would have had an impact on the Council. This would help Councillors ensure they were sighted on "big issues" and, where appropriate, engage with the officers to progress.

The report was split into two parts:-

(1) Progress as at 20 February 2014 which included:-

- 2012/13 certification work;
- 2013/14 Accounts Audit Plan;
- Interim accounts audit;
- 2013/14 final accounts audit; and
- 2013/14 Value for Money conclusion; and
- Other activities; and

(2) Emerging issues and developments which included information on:-

- Local Government guidance – Audit Commission research – Tough Times 2013 and Local Audit and Accountability Act;
- Grant Thornton – 2016 tipping point? Challenging the current; Alternative delivery models in local government; and Reaping the benefits : first impressions of the impact of welfare reform; and
- Accounting and audit issues – Business Rate appeals provisions.

Resolved that the report be noted.

7. SAP Access Audit Report

Considered report previously circulated, concerning the recently completed audit report in relation to SAP access by ICT staff for Somerset County Council (SCC) that had recently been completed by Grant Thornton.

The report had identified a number of actions required to resolve some areas of concern relating to SAP system access.

The Council along with the other partners had recently had a chance to discuss the audit report with SCC and Grant Thornton. The report had highlighted some areas of concern relating to SAP access and the main issues were:-

- There were users of SAP who could access all company and partner records; and
- Some users could access personally identifiable data.

All large computer systems had a user based security and access management system in place to ensure users of the system could only access the parts of the system and data that were relevant to their job role. The ICT team responsible for supporting the entire system, and for developing and implementing changes to that system needed privileged access to the system in order to perform that role.

The SAP system allowed control of these so-called Superuser permissions. As a result, no individual member of the ICT team had all Superuser permissions. Most support activities required the input from more than one member of the ICT team to complete.

Noted that a series of non-technical controls known as Secondary Controls were also in place, and took the form of documented processes and written approvals to perform certain changes to the system.

One of the report findings was that allocation of the subset of Superuser privileges appeared to be excessive. Further analysis identified that some reduction in permissions allocated to certain individuals within the ICT team would be possible without preventing them performing their job roles. Implementation of these changes was underway and would be completed by the end of March 2014.

The Council had also worked with Southwest One to develop an action plan to address the findings.

Three of the twelve issues had an Amber status as work was still in progress. This work was due to be completed by the end of March 2014 and was being monitored.

The remainder were closed and had a Green status, demonstrating that significant work that had been completed since the original report was released.

During the discussion of this item, Members made comments and statements and asked questions which included: - (Responses were shown in italics)

- Concerns were raised over the length of time it took to bring about changes recommended by an audit. *The Council was following the guidelines and there were rigorous secondary controls in place, despite a few technical issues.*
- Referring to the secondary controls, should not the Council know if there were any defects? *This might be something the Council should be informed and sighted on in the future testing.*
- Some Members were not receiving a warning message on the OWA system when their password was about to expire. *This would be investigated.*

Resolved that the Grant Thornton report and the actions being taken to address the concerns raised be noted.

8. Corporate Anti-Fraud and Error Policy

Considered report previously circulated, concerning the Council's Corporate Anti-Fraud and Error Policy.

The Council had recognised that it needed to do more to secure the gateways of fraud, corruption and bribery within the authority and to extend the focus across the entire organisation.

The proposed Corporate Anti-Fraud Policy set out the high level priorities the Council needed to meet to achieve the Council's vision of zero tolerance for fraud, corruption and bribery throughout the authority by creating a strong and effective anti-fraud, anti-corruption and anti-bribery culture.

The policy brought together existing policies on Whistleblowing and Anti-Bribery as well as updating the Revenues and Benefits Service's anti-fraud measures. It also set out the context and anti-fraud activities in other Council services such as Housing and Procurement as well as plans and protocols to effectively mitigate against fraud within the Council.

In developing the Corporate Fraud Policy the Council had drawn on good practice provided by the Chartered Institute of Public Finance and Accountancy, the Audit Commission as well as the National Fraud Strategy published by the Attorney General's Office.

The Audit Commission's Use of Resources fraud checklist had formed the foundation for the Corporate Anti-Fraud Action Plan. The Action Plan was a "living" document that the Council would update as and when new guidance, legislation or good practice was available.

During the discussion of this item, Members made comments and statements and asked questions which included: - (Responses were shown in italics)

- *The Government had announced that they were making money available to Local Authorities to deal with Corporate Fraud.*
- Was the Council planning to publicise the Council's new approach to show it meant business in this area? *There would be extensive publicity when the new Corporate Fraud Team was introduced.*
- The Council had already put aside £70,000 towards the creation of a new Corporate Fraud Team. Would this additional Government funding be in addition to the Council money or put to another use? *Currently the make-up of the team was likely to consist of a manager, two full time investigators and one full time administration assistant. The money from the Government would go towards bridging the gap between what the Council could afford*
- Would the Corporate Fraud Team have the relevant access to SAP elements? *Yes, the Council would look to employ highly skilled and qualified investigators.*
- The Council must not lose sight that there were other areas in the Council that suffered with fraud issues, not just in Revenues and Benefits. *The Corporate Fraud Team would take a much wider view of all Council areas and aspects of fraud.*

Resolved that the Executive be recommended to adopt the Corporate Anti-Fraud and Error Policy.

9. Risk Management

Considered report previously circulated, which provided an update on progress with the Council's approach to Risk Management.

The new Joint Management Team (JMT) had recently undertaken a fundamental review and refresh of the Corporate Risk Register. This had been created as a new joint risk register for Taunton Deane and West Somerset, which would enable JMT to manage strategic risks for both Councils by the new 'One Team' organisation.

A Risk Management Action Plan had been prepared and a copy had been circulated to all Members of the Committee. This outlined the key areas of focus to further improve and embed Risk Management during 2014.

Reported that the focus for the next few months would be the adoption of the new approach to joint risk management for both Councils.

The specific actions required in moving Risk Management forward were set out in detail in the report under the headings:-

- Strategic actions;
- Programmes, Projects, Services and Partnerships; and
- Other considerations.

During the discussion of this item, Members made comments and statements and asked questions which included: - (Responses were shown in italics)

- Had the risk to Members when they were making decisions been assessed?
- How would this be quantified?
- Surely a Ward Councillor's priority was to those people they represented within their Ward. *Risk management was a continuing process and it was therefore hoped that Members discussed risk at every opportunity with other Members and officers so the Council had a more informed position of risk. The more feedback, the officers received from Members the more informed the Council would be.*
- Could the inclusion of a RAG Status column be considered for the Risk Register to allow Members to gauge its progress? *Yes.*
- Concerns were raised that because the Council was concentrating on certain areas of risk that it may miss other areas of importance. *There were other Risk Registers throughout the Council for a variety of projects and departments but this particular one was the Corporate Risk Register for the whole Council.*
- The Risk Register as a document, Could the Risk Register be simplified or did Members want or need the level of detail it contained? *As this was a completely new Register it was considered appropriate for Members to see the full version. In future, summaries would be brought to the Committee for information/consideration.*
- Would this document become more detailed and complicated with the inclusion of the shared services with West Somerset? *This new register showed a combined risk position for both Councils. There was a column indicating who the risk related to.*
  The benefit to having a combined Risk Register. *It would be the same register even if it only related to Taunton Deane.*
- Members expressed a desire to discuss this topic further at a future meeting of Committee.

Resolved that the progress with Corporate Risk Management, the Corporate Risk Register and the approach and actions to achieve joint Risk Management for Taunton Deane Borough Council and West Somerset Councils, be noted.

10. Internal Audit Plan 2013/2014 – Progress Report

Considered report previously circulated, which summarised the work of the Council's Internal Audit Service and provided:-

- Details of any new significant weaknesses identified during internal audit work completed since the last report to the Committee in September 2013; and
- A schedule of audits completed during the period, detailing their respective assurance opinion rating, the number of recommendations and the respective priority ranking of these.

Members noted that where a partial assurance had been awarded, Internal Audit would follow up on the agreed management responses to provide assurance that risk exposure had been reduced.

During the discussion of this item, Members made comments and statements and asked questions which included: - (Responses were shown in italics)

- The current issues that the South West Audit Partnership was having with getting the correct SAP access should be raised and chased for a resolution. *Southwest One was moving this matter forward towards a resolution and this would continue to be monitored.*
- Who authorised the dropping of Audits? *The Section 151 Officer was responsible for authorising changes to audits.*
- A request was made for a progress update on the partial audit of procurement cards as well as an update of the ICT audit progress. *These updates would be added to the forward plan on the agenda of the next meeting.*

Resolved that the progress made in the delivery of the 2013/2014 Internal Audit Plan and the significant findings be noted.

11. Internal Audit Plan 2014/2015

Submitted for consideration the Internal Audit Plan 2014/2015, a copy of which had been circulated to Members of the Committee. The Plan also incorporated an 'Internal Audit Charter' which set out the operational relationship between the Council and the South West Audit Partnership (SWAP).

The Plan was a flexible plan that could be amended during the year to deal with shifts in priorities.

It focussed on key risk areas and would help provide assurance on internal controls. The Plan had been discussed and supported by the Joint Management Team.

The internal audit service provided by SWAP, worked to a Charter that defined its roles and responsibilities and the roles and responsibilities of the Council's managers as they related to internal audit. Best practice in corporate governance required that the Charter be reviewed and approved annually by the Corporate Governance Committee.

Noted that the Charter had only recently been updated to reflect the changes in roles and responsibilities and to address some of the minor requirements of the

Public Sector Internal Audit Standards. There were no further changes required at this time.

Resolved that:-

(1) The Internal Audit Plan for 2014/2015 be approved; and

(2) The Internal Audit Charter be also approved.

12. South West Audit Partnership Directors Governance Arrangements

Considered report previously circulated, concerning an amendment to the governance arrangements for the Council with regard to the South West Partnership Limited (SWAP).

Just over twelve months ago, the Council supported the formation of the company.

Since formation, the representation on the Members Board had been undertaken by the Chairman of the Corporate Governance Committee.

Representation at officer level, as a Director on the Board, had been undertaken by the Deputy Section 151 Officer (with the Client and Corporate Services Manager acting as Alternate).

Clearly with the new Joint Management Team arrangements now in place the Council needed to amend this to reflect new roles and responsibilities.

Proposed that the Assistant Director – Corporate Services who was responsible for the audit function should now be this Council's Director on the SWAP and that the "Alternate" should be the Assistant Director – Resources.

Resolved that Full Council be recommended to approve the following nominations:-

(a) The Assistant Director – Corporate Services as this Councils Director on the Board of South West Audit Partnership Limited; and

(b) The Assistant Director – Resources as the Alternate Director.

13. Corporate Governance Committee Forward Plan

Submitted for information the proposed Forward Plan of the Corporate Governance Committee.

Resolved that the Corporate Governance Committee Forward plan be noted.

(The meeting ended at 8.24pm).

AGENDA ITEM NO. 6

Declaration of Interests

Corporate Governance Committee

- Members of Somerset County Council – Councillors Coles, A Govier, Hunt, D Wedderkopp and A Wedderkopp

- Employee of UK Hydrographic Office – Councillor Tooze

- Director of the Taunton Town Centre Company - Councillor D Reed

AGENDA ITEM NO. 7

Taunton Deane Borough Council

Corporate Governance Committee – 19 May 2014

External Audit Plan 2013/14

Report of the Assistant Director - Corporate Services (Richard Sealy)
(This matter is the responsibility of the Leader of the Council, Councillor John Williams)

1. Executive Summary

This report introduces the External Audit Plan for 2013/14. This is prepared by our external auditors, Grant Thornton, and is detailed in the appendix to the report.

The report, which will be presented by Grant Thornton, summarises their approach to the 2013/14 audit programme, provides information on the work already undertaken, the tasks yet to be completed, the timescales and the auditors view on risk.

2. Background

2.1 Each year our external auditors, Grant Thornton, provide a plan, which details their approach to the audit work required in respect of the preceding financial year (2013/14). Specifically this audit work focuses on the provision of an audit opinion in relation to the accounts, value for money (VFM) and associated key risks.

2.2 The plan for 2013/14 is set out in Appendix A.

3. Finance Comments

3.1 The report sets out the external auditors view on key risk areas for the Council and their approach to auditing them.

4. Legal Comments

4.1 There are no legal implications from this report.

5. Links to Corporate Aims

5.1 There are no direct implications.

6. Environmental Implications

6.1 There are no implications.

7. Community Safety Implications

7.1 There are no implications.

8. Equalities Impact

8.1 There are no implications.

9. Risk Management

9.1 Any risks identified will feed into the corporate risk management process.

10. Partnership Implications

10.1 The Assistant Director – Corporate Services and the Internal Audit Team (SWAP) will take the issues flagged in this report into account when reviewing the areas of risk to be reviewed by Internal Audit in the current and future years.

11. Recommendations

11.1 Members are requested to note the External Audit Plan for 2013/14 received from Grant Thornton.

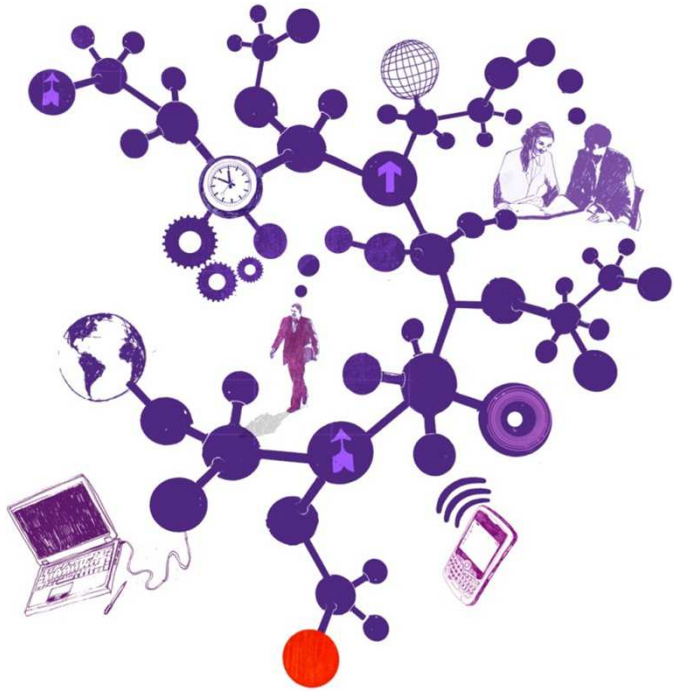
Contact: Richard Sealy
(01823) 358690
r.sealy@tauntondeane.gov.uk

APPENDIX A – The Audit Plan for Taunton Deane Borough Council for the year ending 31 March 2014

The Audit Plan for Taunton Deane Borough Council

Year ended 31 March 2014

19 May 2014



Peter Barber
Engagement Lead
T 0117 305 7897
E peter.a.barber@uk.gt.com

Ashley Allen
Manager
T 0117 305 7629
E ashley.j.allen@uk.gt.com

Sarah Crouch
Executive
T 0117 305 7881
E sarah.crouch@uk.gt.com

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 the Council or any weaknesses in your internal controls. This report has been prepared solely for your benefit and should not be quoted in whole or in part without our prior written consent. We do not accept any responsibility for any loss occasioned to any third party acting, or refraining from acting on the basis of the content of this report, as this report was not prepared for, nor intended for, any other purpose.

Contents

1. Understanding your business

In planning our audit we need to understand the challenges and opportunities the Council is facing. We set out a summary of our understanding below.

Challenges/opportunities

1. Medium Term Financial Plan (MTFP) – Revenue expenditure

- In setting its budget for 2014/15 the Council has closed a budget gap of £1m through a programme of savings plans.
- The Council is also forecasting that it will be able to balance its budget for 2015/16 but that it will have to find further significant savings for 2016/17 and beyond as a result of further reductions to Government grants.
- In the medium term, the Council will need to plan to deliver a more sustainable financial position matching recurrent expenditure and income.

2. Local Government Finance Act

- The Local Government Resource Review made three significant areas of reform to Local Government Finance:-
  - The local retention of Business Rates
  - The replacement of Council Tax Benefit by provision for Local Council Tax support from 1 April 2013 .
  - Discretion on the level and period of discount to be applied to certain classes of empty property.

3. Capital Expenditure

The Council has major capital spending programmes of around £37 million for housing revenue account (HRA) and £7million for General Fund over the next 5 years in addition to £10m spent in 2013/14.

4. Accounts

At the end of our 2012-13 audit, we recommended that the Council should

- address the recommendations from the review of the IT controls
- review the bad debt provision for housing debts, and
- retain expense claims and supporting receipts.

5. Shared Services and Joint Management with West Somerset District Council

- The Council agreed to share management and services, beginning with the Chief Executive in October 2013 and Directors from January 2014.
- Both Councils are relying on the sharing and transformation of services to deliver significant savings and enhanced service resilience

Our response

- We will continue to monitor progress against the Medium Term Financial Plan and review progress in achieving the savings plans.
- We will continue to review the arrangements for securing future economies to inform our Value for Money conclusion and ensure that a balanced budget will be achieved in future years.
- We will follow up recommendations from our Financial Resilience report and Annual Audit Letter from last year.

- As part of our Value for Money work we will consider the financial planning arrangements in place to address the risks surrounding these financing changes.
- We will discuss and review the accounting impact of these changes with the finance team.

We will consider the Council's capital programme in reaching our VFM conclusion, but we are not expecting to carry out any specific work on individual schemes .

- We will review the progress made by the Council in response to our audit recommendations.
- We will continue to discuss key issues in advance of the audit with the finance team.

- We will review delivery of savings from sharing services and the impact on current budgets and medium term financial plan
- We will review the basis of how costs have been shared between each Council

2. Developments relevant to your business and the audit

In planning our audit we also consider the impact of key developments in the sector and take account of national audit requirements as set out in the Code of Audit Practice ('the code') and associated guidance.

Developments and other requirements					
1.Financial reporting • Changes to the CIPFA Code of Practice • Clarification of Code requirements around PPE valuations • Changes to NDR accounting and provisions for business rate appeals	**2. Legislation** • Local Government Finance settlement • Welfare reform Act 2012	**3. Corporate governance** • Annual Governance Statement (AGS) • Explanatory foreword	**4. Pensions** • The impact of 2013/14 changes to the Local Government pension Scheme (LGPS)	**5. Financial Pressures** • Managing service provision with less resource • Progress against savings plans	**6. Other requirements** • The Council is required to submit a Whole of Government accounts pack on which we review. • The Council completes grant claims and returns on which audit certification is required
Our response					
We will ensure that • the Council complies with the requirements of the CIPFA Code of Practice and business rate appeals through discussions with management and our substantive testing	• We will discuss the impact of the legislative changes with the Council through our regular meetings with senior management and those charged with governance, providing a view where appropriate	• We will review the arrangements the Council has in place for the production of the AGS • We will review the AGS and the explanatory foreword to consider whether they are consistent with our knowledge	• We will review how the Council dealt with the impact of the 2013/14 changes through our meetings with senior management	• We will review the Council's performance against the 2013/14 budget, including consideration of performance against the savings plan • We will undertake a review of Financial Resilience as part of our VFM conclusion	• We will carry out work on the WGA pack in accordance with requirements • We will certify grant claims and returns in accordance with Audit Commission requirements

3. Our audit approach

Global audit technology

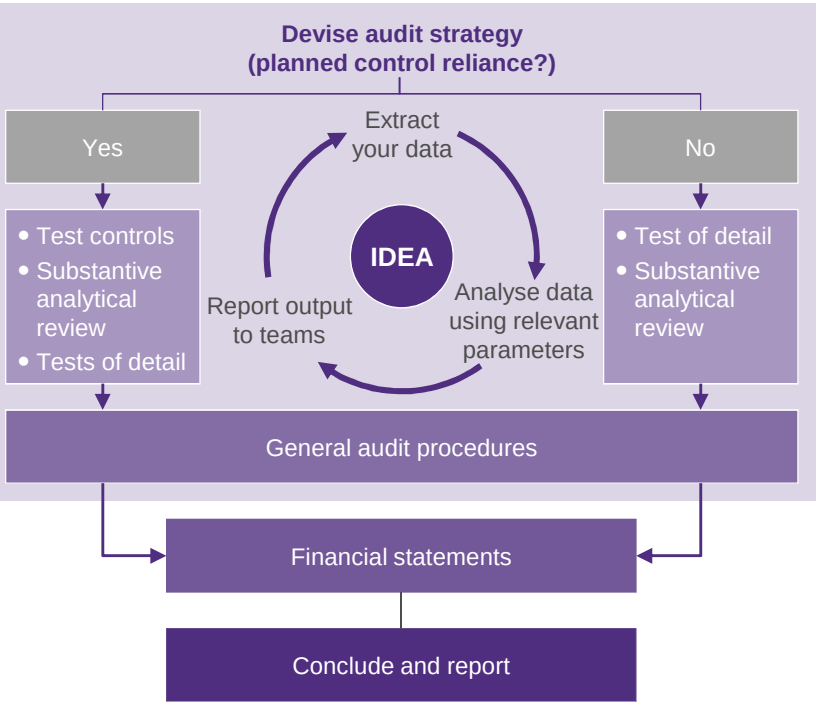
Ensures compliance with International Standards on Auditing (ISAs)

- Understanding the environment and the entity
- Understanding the business
- Understanding management's focus
- Evaluating the year's results

→ Inherent risks, Significant risks, Other risks, Material balances →

Develop audit plan to obtain reasonable assurance that the Financial Statements as a whole are free from material misstatement and prepared in all material[a] respects with the CIPFA Code of Practice framework using our global methodology and audit software

Note:
a. An item would be considered material to the financial statements if, through its omission or non-disclosure, the financial statements would no longer show a true and fair view.



Voyager

Creates and tailors audit programs

Stores audit evidence

Documents processes and controls

4. Significant risks identified

'Significant risks often relate to significant non-routine transactions and judgmental matters. Non-routine transactions are transactions that are unusual, either due to size or nature, and that therefore occur infrequently. Judgmental matters may include the development of accounting estimates for which there is significant measurement uncertainty' (ISA 315).

In this section we outline the significant risks of material misstatement which we have identified. There are two presumed significant risks which are applicable to all audits under auditing standards (International Standards on Auditing – ISAs) which are listed below:

Significant risk	Description	Substantive audit procedures
The revenue cycle includes fraudulent transactions	Under ISA 240 there is a presumed risk that revenue may be misstated due to the improper recognition of revenue.	**Work planned:** • Review and testing of revenue recognition policies • Testing of material revenue streams
Management over-ride of controls	Under ISA 240 there is a presumed risk that the risk of management over-ride of controls is present in all entities.	**Work completed to date:** • Review of accounting estimates, judgments and decisions made by management **Further work planned:** • Review of accounting estimates, judgments and decisions made by management • Testing of journal entries • Review of unusual significant transactions

5. Other risks identified

The auditor should evaluate the design and determine the implementation of the entity's controls, including relevant control activities, over those risks for which, in the auditor's judgment, it is not possible or practicable to reduce the risks of material misstatement at the assertion level to an acceptably low level with audit evidence obtained only from substantive procedures (ISA 315).

In this section we outline the other risks of material misstatement which we have identified as a result of our planning.

Other reasonably possible risks	Description	Work completed to date	Further work planned
Operating expenses	Creditors understated or not recorded in the correct period	• Walkthrough tests of design and operation of controls	• Substantive testing of operating expenditure and year end adjustments / reconciliations • Review and testing of creditors/liability balances of unusual and large amounts • Review of unrecorded liabilities and after date payments to ensure all liabilities identified
Employee remuneration	Employee remuneration accrual understated	• Walkthrough tests of design and operation of controls • Initial substantive testing of Employees for months one to 11 to underlying supporting documentation	• Substantive testing of the month 12 payroll payments to underlying evidence • Agreement of payroll accruals to schedules and underlying evidence. • Review of senior officers pay disclosures and agreement to underlying data. • Analytical procedures over the payroll figures throughout the year to ensure that it is reasonable and complete. • Reconciliation of the payroll system figures to the general ledger figures
Welfare Expenditure	Welfare benefit expenditure improperly computed	• Walkthrough tests of design and operation of controls	• Substantive testing of welfare expenditure will occur for the whole year to gain assurance over the welfare expenditure figures

5. Other risk identified (continued)

Other reasonably possible risks	Description	Work completed to date	Further work planned
Housing Rent Revenue Account	Revenue transactions not recorded	• Walkthrough tests of design and operation of controls	• Testing to ensure that the Council has recognised all material HRA revenue including the review of • the reasonableness of the total rent debit and • reconciliations to rent accounts to the total properties in the HRA
Property, Plant & Equipment	PPE activity not valid	• None – work to be completed at the year end.	• Walkthrough test to review the design and operation of controls over the PPE system. • Testing of a sample of additions and disposals • Testing of depreciation
Property, Plant & Equipment	Revaluation measurement not correct	• None – work to be completed at the year end.	• Walkthrough test to review the design and operation of controls over the PPE system. • Testing the revaluation figures to ensure that they are reasonable. • Testing the revaluation figures in the Fixed Asset Register to the Valuer's Report.

6. Results of interim audit work

The findings of our interim audit work, and the impact of our findings on the accounts audit approach, are summarised in the table below:

	Work performed and findings	Conclusion
Internal audit	We have reviewed internal audit's overall arrangements in accordance with auditing standards. Our work has not identified any issues which we wish to bring to your attention. We also reviewed internal audit's work on the Council's key financial systems to date. We have not identified any significant weaknesses impacting on our responsibilities.	Overall, we have concluded that the internal audit service continues to provide an independent and satisfactory service to the Council and that internal audit work contributes to an effective internal control environment at the Council. Our review of internal audit work has not identified any weaknesses which impact on our audit approach.
Walkthrough testing	We have completed walkthrough tests of controls operating in areas where we consider that there is a risk of material misstatement to the financial statements. Our work has not identified any issues which we wish to bring to your attention. Internal controls have been implemented in accordance with our documented understanding.	Our work has not identified any weaknesses which impact on our audit approach.
Journal entry controls	We have reviewed the Council's journal entry policies and procedures as part of determining our journal entry testing strategy and have not identified any material weaknesses which are likely to adversely impact on the Council's control environment or financial statements.	Overall, no significant issues have been identified in the journal policies or procedures, or the journals identified and tested to date. Further journal testing will occur to ensure that testing on the journals in the remainder of the year will be completed.
Early substantive testing	Some early substantive testing has been carried out on Payroll transactions in months one to 11, and some initial trend analysis has been undertaken.	No issues have been identified with the testing that has been completed to date. Further testing will need to be undertaken to cover the remainder of the year.

7. Value for money

Value for money

The Code requires us to issue a conclusion on whether the Council has put in place proper arrangements for securing economy, efficiency and effectiveness in its use of resources. This is known as the Value for Money (VfM) conclusion.

Our VfM conclusion is based on the following criteria specified by the Audit Commission:

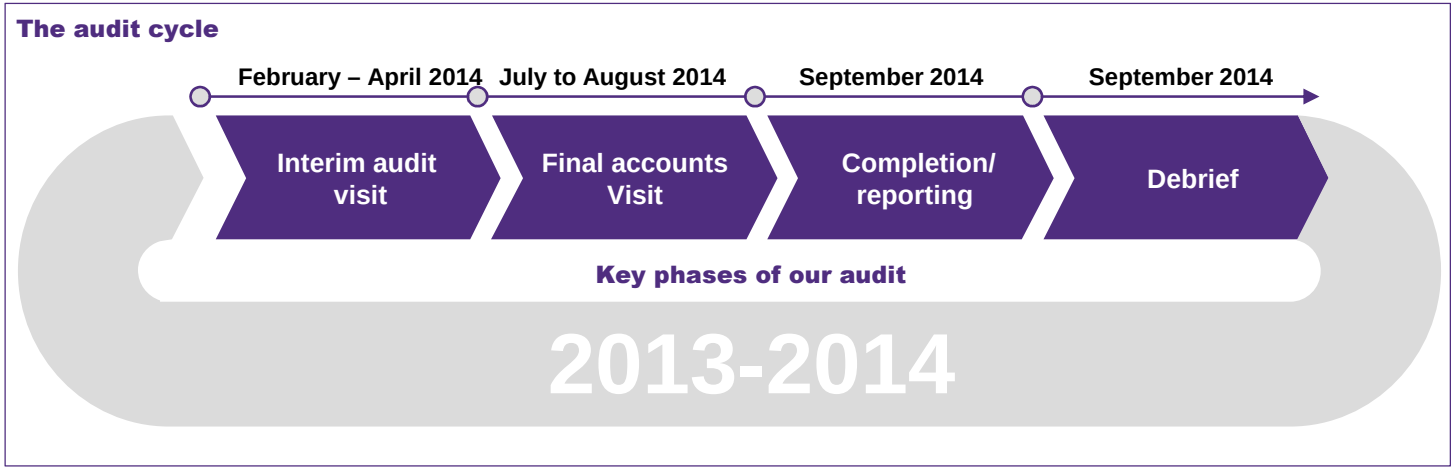
VfM criteria	Focus of the criteria
The organisation has proper arrangements in place for securing financial resilience	The organisation has robust systems and processes to manage financial risks and opportunities effectively, and to secure a stable financial position that enables it to continue to operate for the foreseeable future
The organisation has proper arrangements for challenging how it secures economy, efficiency and effectiveness	The organisation is prioritising its resources within tighter budgets, for example by achieving cost reductions and by improving efficiency and productivity

We have undertaken a risk assessment to identify areas of risk to our VfM conclusion. We will undertake work in the following areas to address the risks identified:

- key indicators of financial performance
- strategic financial planning
- financial governance
- financial control
- delivery of savings against the 2013/14 budget
- the medium term financial plan (MTFP) and capital programme

The results of our VfM audit work and the key messages arising will be reported in our Audit Findings report and in the Annual Audit Letter.

8. Key dates



Date	Activity
February	Planning
February to April 2014	Interim site visit
May 2014	Presentation of audit plan to Corporate Governance Committee
July to September 2014	Year end fieldwork
September 2014	Audit findings clearance meeting with Director of Operations
September 2014	Report audit findings to those charged with governance (Corporate Governance Committee)
September 2014	Sign financial statements opinion

9. Fees and independence

Fees

	£
Council audit	66,605
Grant certification (indicative)	15,606
Total fees (excluding VAT)	**82,211**

Fees for other services

Service	Fees £
None	Nil

Our fee assumptions include:

- Supporting schedules to all figures in the accounts are supplied by the agreed dates and in accordance with the agreed upon information request list
- The scope of the audit, and the Council and its activities, have not changed significantly
- The Council will make available management and accounting staff to help us locate information and to provide explanations

Independence and ethics

We confirm that there are no significant facts or matters that impact on our independence as auditors that we are required or wish to draw to your attention. We have complied with the Auditing Practices Board's Ethical Standards and therefore we confirm that we are independent and are able to express an objective opinion on the financial statements.

Full details of all fees charged for audit and non-audit services will be included in our Audit Findings report at the conclusion of the audit.

We confirm that we have implemented policies and procedures to meet the requirement of the Auditing Practices Board's Ethical Standards.

10. Communication of audit matters with those charged with governance

International Standards on Auditing (ISA) 260, as well as other ISAs, prescribe matters which we are required to communicate with those charged with governance, and which we set out in the table opposite.

This document, The Audit Plan, outlines our audit strategy and plan to deliver the audit, while The Audit Findings will be issued prior to approval of the financial statements and will present key issues and other matters arising from the audit, together with an explanation as to how these have been resolved.

We will communicate any adverse or unexpected findings affecting the audit on a timely basis, either informally or via a report to the Council.

Respective responsibilities

This plan has been prepared in the context of the Statement of Responsibilities of Auditors and Audited Bodies issued by the Audit Commission (www.audit-commission.gov.uk).

We have been appointed as the Council's independent external auditors by the Audit Commission, the body responsible for appointing external auditors to local public bodies in England. As external auditors, we have a broad remit covering finance and governance matters.

Our annual work programme is set in accordance with the Code of Audit Practice ('the Code') issued by the Audit Commission and includes nationally prescribed and locally determined work. Our work considers the Council's key risks when reaching our conclusions under the Code.

It is the responsibility of the Council to ensure that proper arrangements are in place for the conduct of its business, and that public money is safeguarded and properly accounted for. We have considered how the Council is fulfilling these responsibilities.

Our communication plan	Audit plan	Audit findings
Respective responsibilities of auditor and management/those charged with governance	✓	
Overview of the planned scope and timing of the audit. Form, timing and expected general content of communications	✓	
Views about the qualitative aspects of the entity's accounting and financial reporting practices, significant matters and issue arising during the audit and written representations that have been sought		✓
Confirmation of independence and objectivity	✓	✓
A statement that we have complied with relevant ethical requirements regarding independence, relationships and other matters which might be thought to bear on independence. Details of non-audit work performed by Grant Thornton UK LLP and network firms, together with fees charged. Details of safeguards applied to threats to independence	✓	✓
Material weaknesses in internal control identified during the audit		✓
Identification or suspicion of fraud involving management and/or others which results in material misstatement of the financial statements		✓
Non compliance with laws and regulations		✓
Expected modifications to the auditor's report, or emphasis of matter		✓
Uncorrected misstatements		✓
Significant matters arising in connection with related parties		✓
Significant matters in relation to going concern		✓

grant-thornton.co.uk

AGENDA ITEM NO. 8

Taunton Deane Borough Council

Corporate Governance Committee – 19 May 2014

External Audit Update Report

Report of the Assistant Director - Corporate Services (Richard Sealy)
(This matter is the responsibility of the Leader of the Council, Councillor John Williams)

1. Executive Summary

This report provides a progress update from our external auditors, Grant Thornton, in respect of the 2013/14 audit work for TDBC and on emerging national issues, which may be relevant to the Council.

The report will be presented by Grant Thornton.

2. Background

2.1 Each year our external auditors, Grant Thornton, are required to carry out "set" audit work. The attached report provides a useful progress update in relation to that work.

2.2 Additionally, the attached report shares the headlines on emerging national issues and developments, which may have a bearing on the Council. Specifically the attached report focuses on the 2013/14 Code for valuing property and assets and changes to the Local Government Pension Scheme.

3. Finance Comments

3.1 The report is an update report only.

4. Legal Comments

4.1 There are no legal implications from this report.

5. Links to Corporate Aims

5.1 There are no direct implications.

6. Environmental Implications

6.1 There are no direct implications.

7. Community Safety Implications

7.1 There are no direct implications.

8. Equalities Impact

8.1 There are no implications arising from this report.

9. Risk Management

9.1 Any risks identified will feed into the corporate risk management process.

10. Partnership Implications

10.1 There are no implications.

11. Recommendations

11.1 Members are requested to note the Update Report from Grant Thornton.

Contact: Officer Name Richard Sealy
Direct Dial No (01823) 358690
E-mail address r.sealy@tauntondeane.gov.uk

APPENDIX A Grant Thornton Corporate Governance Committee Update

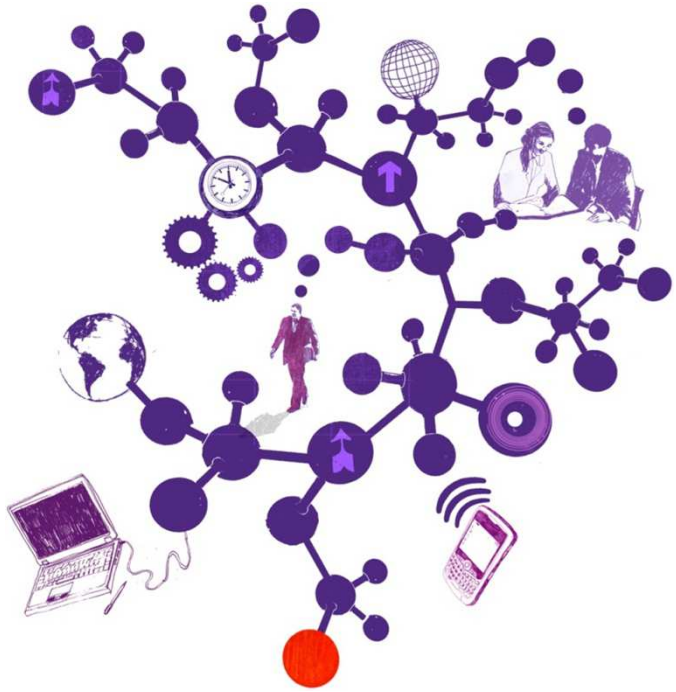
Corporate Governance Committee Update for Taunton Deane Borough Council

Year ended 31 March 2014

19 May 2014

Peter Barber
Associate Director
T +44 (0)117 305 7897
E peter.a.barber@uk.gt.com

Ashley Allen
Manager
T +44 (0)117 305 7629
E ashley.j.allen@uk.gt.com



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

.

Contents

Introduction

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

- a summary of emerging national issues and developments that may be relevant to you as a district council in respect of these emerging issues which the Committee may wish to consider.

Members of the Corporate 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 – 'Local Government Governance Review 2013', 'Towards a tipping point?', 'The migration of public services', 'The developing internal audit agenda', 'Preparing for the future', 'Surviving the storm: how resilient are local authorities?'

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

Peter Barber
Engagement Lead
T 0117 305 7897
E peter.a.barber@uk.gt.com

Ashley Allen
Audit Manager
T 0117 305 7629
E ashley.j.allen@uk.gt.com

Progress at 5 May 2014

Work	Planned date	Complete?	Comments
2013-14 Accounts Audit Plan We are required to issue a detailed accounts audit plan to the Council setting out our proposed approach in order to give an opinion on the Council's 2013-14 financial statements.	March 2014	Yes	Our audit plan sets out our approach for the final accounts visit in the summer of 2014. The plan is informed by our interim accounts audit.
Interim accounts audit Our interim fieldwork visit includes: • updating our review of the Council's control environment • updating our understanding of financial systems • review of Internal Audit reports on core financial systems • early work on emerging accounting issues • early substantive testing • proposed Value for Money conclusion.	January to March 2014	Yes	We have updated our understanding of the Council's financial systems and we are undertaking walk-through tests.

Progress at 5 May 2014

Work	Planned date	Complete?	Comments
2013-14 final accounts audit Including: • audit of the 2013-14 financial statements • proposed opinion on the Council's accounts • proposed Value for Money conclusion.	July to September 2013	Not yet due	None
2013-14 Value for Money (VfM) conclusion The scope of our work to inform the 2013/14 VfM conclusion comprises: • a detailed review of financial resilience • a review of arrangements for securing economy and efficiency • a follow up of recommendations made last year.	Summer 2014	Not yet due	None
Other activities • Accounts workshop in the South West to help local authorities in the preparation of the financial statements for 2013/14.	February 2014	Yes	We have worked with CIPFA to deliver workshops in Exeter and Bristol.

Revaluing your assets – clarification of accounting guidance

Accounting and audit issues

Property, plant and equipment valuations

The 2013/14 Code has clarified the requirements for valuing property, plant and equipment and now states explicitly that revaluations must be 'sufficiently regular to ensure that the carrying amount does not differ materially from that which would be determined using the fair value at the end of the reporting period.' This means that a local authority will need to satisfy itself that the value of assets in its balance sheet is not materially different from the amount that would be given by a full valuation carried out on 31 March 2014. This is likely to be a complex analysis which might include consideration of:

- the condition of the authority's property portfolio at 31 March 2014
- the results of recent revaluations and what this might mean for the valuation of property that has not been recently valued
- general information on market prices and building costs
- the consideration of materiality in its widest sense - whether an issue would influence the view of a reader of the accounts.

The Code also follows the wording in IAS 16 more closely in the requirements for valuing classes of assets:

- items within a class of property, plant and equipment are to be revalued simultaneously to avoid selective revaluation of assets and the reporting of amounts in the financial statements that are a mixture of costs and values as at different dates
- a class of assets may be revalued on a rolling basis provided revaluation of the class of assets is completed within a short period and provided the revaluations are kept up to date.

There has been much debate on what is a short period and whether assets that have been defined as classes for valuation purposes should also be disclosed separately in the financial statements. These considerations are secondary to the requirement that the carrying value does not differ materially from the fair value. However, we would expect auditors to report to those charged with governance where, for a material asset class:

- all assets within the class are not all valued in the same year
- the class of asset is not disclosed separately in the property, plant and equipment note.

Accounting for pensions

Accounting and audit issues

Accounting for and financing the local government pension scheme costs

Accounting issues

The 2013/14 Code follows amendments to IAS 19 and changes the accounting requirements for defined benefit pension liabilities such as those arising from the local government pension scheme (LGPS). This is a change in accounting policy and will apply retrospectively. The main changes we expect to see are:

- a reallocation of amounts charged in the comprehensive income and expenditure statement (CIES)
- more detailed disclosures.

We do not expect changes to balance sheet items (the net pension liability and pension reserve balance). This means that whilst we would expect the CIES to be restated, a third balance sheet is not required. Actuaries should be providing local authorities with the information they need to prepare the financial statements, including restated comparatives.

Financing issues

The amount to be charged to the general fund in a financial year is the amount that is payable for that financial year as set out in the actuary's rates and adjustments certificate. Some local authorities are considering paying pension fund contributions early in exchange for a discount but not charging the general fund until later.

Local authorities must be satisfied that the amounts charged to the general fund in a financial year are the amounts payable for that year. Where local authorities are considering making early payments, we would expect them to obtain legal advice (either internally or externally) to determine the amounts that are chargeable to the general fund. We would expect this to include consideration of:

- the actuary's opinion on the amounts that are payable by the local authority into the pension fund
- the agreement between the actuary and the local authority as to when these payments are to be made
- the wording in the rates and adjustments certificate setting out when amounts are payable for each financial year.

For example, if a local authority agrees to make a payment to the pension fund in a single year and proposes to charge this amount to the general fund over a three-year period, we would expect the rates and adjustments certificate to show, unambiguously, that the amount payable is spread over the three years.

Changes to the public services pension scheme

Accounting and audit issues

Changes to the Local Government Pension Scheme

The Public Service Pensions Bill received Royal Assent in April 2013, becoming the Public Service Pensions Act 2013 ('the Act'). The Act makes provision for new public service pension schemes to be established in England, Wales & Scotland. Consequent regulations have been laid to introduce changes to the LGPS in England and Wales from 1st April 2014. (The regulations for the changes in Scotland have not yet been laid and will only impact from 1 April 2015).

These introduce a number of changes including:

- a change from a final salary scheme to a career average scheme
- introduction of a 50/50 option whereby members can choose to reduce their contributions by 50% to receive 50% less benefit
- calculation of contributions based on actual salary which could lead to some staff with irregular patterns of working moving between contribution rate bandings on a regular basis
- changes in employee contribution rates and bandings
- transitional protection for people retiring within 10 years of 1 April 2014 (further regulations are still awaited).

The above changes have implications for all employers involved in the LGPS introducing required changes to their payroll systems to ensure pension contributions are calculated correctly. This has consequent implications for administering authorities to communicate with employers and consider how they will obtain assurance over the accuracy and completeness of contributions going forwards since the calculations are more complex going forwards and less predictable. In addition changes are also required to pension administration/payment systems as well as much more detailed processes around maintaining individual pension accounts for all members to ensure the correct payment of future pensions.
The Act also requires changes to the governance arrangements although regulations for the LGPS have not yet been laid for these and the changes in governance arrangements are not expected to be implemented until 1 April 2015.

grant.thornton.co.uk

AGENDA ITEM NO. 9

Taunton Deane Borough Council

Corporate Governance Committee – 19 May 2014

External Audit Fees 2014/15

Report of the Assistant Director - Corporate Services (Richard Sealy)
(This matter is the responsibility of the Leader of the Council, Councillor John Williams)

1. Executive Summary

The report details the fee position for external audit services for 2014/15.

2. Background

2.1 The external audit function for Taunton Deane transferred from the Audit Commission to Grant Thornton during 2012. This change was part of a national programme of "outsourcing" the external audit work and has resulted in significant savings for local authorities.

2.2 The attached letter provides details of the agreed fee for 2014/15.

2.3 The letter also sets out details of the process and timetable for completing the external audit work for 2014/15 together with details of the team who will lead the work. However, since receiving the letter we have been notified of a change to the team – Peter Lappin will be replaced by Ashley Allen as Engagement Manager. Peter is moving on to other responsibilities within Grant Thornton.

2.4 Any additional audit work, outside of the planned audit and grant fee work, will be billed separately and in addition to the fee quoted.

3. Finance Comments

3.1 The indicative audit fee for 2014/15 is £76,955. The £76,955 is split between the fee for the main audit of £66,605 (which remains the same as the previous year) and the grant certification work of £10,350 (which represents a reduction of £7,210 from the previous year).

3.2 The fee is within the Council's budget allocation for 2014/15.

4. Legal Comments

4.1 There are no legal implications from this report.

5. **Links to Corporate Aims**

5.1 There are no direct implications.

6. Environmental Implications

6.1 There are no direct implications.

7. Community Safety Implications

7.1 There are no direct implications.

8. Equalities Impact

8.1 There are no implications arising from this fee reduction.

9. Risk Management

9.1 No specific risks have been identified in relation to the fee reduction.

10. Partnership Implications

10.1 There are no implications.

11. Recommendations

11.1 Members are requested to note the Grant Thornton Audit Fee letter for 2014/15.

Contact: Richard Sealy
(01823) 358690
r.sealy@tauntondeane.gov.uk

APPENDIX A Grant Thornton Audit Fee letter dated 15 April 2013

Grant Thornton

An instinct for growth™

Penny James
Chief Executive
Taunton Deane Borough Council
The Deane House
Belvedere Road
Taunton
Somerset
TA1 1HE

Grant Thornton UK LLP
Hartwell House
55-61 Victoria Street
Bristol BS1 6FT

T +44 (0)117 305 7600
F +44 (0)117 305 7784

www.grant-thornton.co.uk

14 April 2014

Dear Penny

Planned audit fee for 2014/15

The Audit Commission has set its proposed work programme and scales of fees for 2014/15. In this letter we set out details of the audit fee for the Council along with the scope and timing of our work and details of our team.

Scale fee

The Audit Commission defines the scale audit fee as "the fee required by auditors to carry out the work necessary to meet their statutory responsibilities in accordance with the Code of Audit Practice. It represents the best estimate of the fee required to complete an audit where the audited body has no significant audit risks and it has in place a sound control environment that ensures the auditor is provided with complete and materially accurate financial statements with supporting working papers within agreed timeframes."

The Council's scale fee for 2014/15 has been set by the Audit Commission at £66,605, which is unchanged from the fee for 2013/14.

Further details of the work programme and individual scale fees for all audited bodies are set out on the Audit Commission's website at: www.audit-commission.gov.uk/audit-regime/audit-fees/proposed-work-programme-and-scales-of-fees-201415

The audit planning process for 2014/15, including the risk assessment, will continue as the year progresses and fees will be reviewed and updated as necessary as our work progresses.

Scope of the audit fee

The scale fee covers:

- our audit of your financial statements
- our work to reach a conclusion on the economy, efficiency and effectiveness in your use of resources (the value for money conclusion)
- our work on your whole of government accounts return.

Value for Money conclusion

Under the Audit Commission Act, we must be satisfied that the Council has adequate arrangements in place to secure economy, efficiency and effectiveness in its use of resources, focusing on the arrangements for:

- securing financial resilience; and
- prioritising resources within tighter budgets.

We undertake a risk assessment to identify any significant risks which we will need to address before reaching our value for money conclusion. We will assess the Council's financial resilience as part of our work on the VfM conclusion and a separate report of our findings will be provided.

Certification of grant claims and returns

The Council's composite indicative grant certification fee has been set by the Audit Commission at £10,390.

Billing schedule

Fees will be billed as follows:

Main Audit fee	£
September 2014	16,652
December 2014	16,651
March 2015	16,651
June 2015	16,651
	66,605
Grant Certification	
December 2015	10,390
Total	**76,995**

Outline audit timetable

We will undertake our audit planning and interim audit procedures in December 2014 to February 2015. Upon completion of this phase of our work we will issue a detailed audit plan setting out our findings and details of our audit approach. Our final accounts audit and work on the VfM conclusion will be completed from July to September 2015 and work on the whole of government accounts return in September 2015.

Phase of work	Timing	Outputs	Comments
Audit planning and interim audit	December 2014 to February 2015	Audit plan	The plan summarises the findings of our audit planning and our approach to the audit of the Council's accounts and VfM.
Final accounts audit	June to Sept 2015	Audit Findings (Report to those charged with governance)	This report sets out the findings of our accounts audit and VfM work for the consideration of those charged with governance.
VfM conclusion	Jan to Sept 2015	Audit Findings (Report to those charged with governance)	As above
Financial resilience	Jan to Sept 2015	Financial resilience report	Report summarising the outcome of our work.
Whole of government accounts	September 2015	Opinion on the WGA return	This work will be completed alongside the accounts audit.
Annual audit letter	October 2015	Annual audit letter to the Council	The letter will summarise the findings of all aspects of our work.
Grant certification	June to December 2015	Grant certification report	A report summarising the findings of our grant certification work

Our team

The key members of the audit team for 2014/15 are:

	Name	Phone Number	E-mail
Engagement Lead	Peter Barber	0117 305 7897 07880 456122	peter.a.barber@uk.gt.com
Engagement Manager	Peter Lappin	0117 305 7865 07880 456135	peter.lappin@uk.gt.com
Audit Executive	Sarah Crouch	0117 305 7881	sarah.crouch@uk.gt.com

Additional work

The scale fee excludes any work requested by the Council that we may agree to undertake outside of our Code audit. Each additional piece of work will be separately agreed and a detailed project specification and fee agreed with the Council.

Quality assurance

We are committed to providing you with a high quality service. If you are in any way dissatisfied, or would like to discuss how we can improve our service, please contact me in the first instance. Alternatively you may wish to contact John Golding, our Public Sector Assurance regional lead partner john.golding@uk.gt.com.

Yours sincerely

Peter Barber
For Grant Thornton UK LLP

cc Shirlene Adam, Director of Operations

AGENDA ITEM NO. 10

Taunton Deane Borough Council

Corporate Governance Committee – 19 May 2014

Regulation of Investigatory Powers Act – Policy and Procedures updated

Report of the Assistant Chief Executive & Monitoring Officer
(This matter is the responsibility of the Leader Councillor John Williams**)**

1. Executive Summary

The Council's policy needs to be updated to reflect the amendments made to the Regulation of Investigatory Powers Act 2000 (RIPA) by the The Protection of Freedoms Act 2012. In addition changes also need to be made to reflect the Council's new management structure and the appropriate authorising officers.

2. Background

2.1 The council has had a corporate policy dealing with the Regulation of Investigatory Powers Act 2000 since July 2008.

2.2 The Policy details various aspects of the legislation and guides officers and the relevant processes and procedures that need to be followed. In addition, it also sets out details of the relevant authorising officers for the Council.

2.3 In 2012, the Protection of Freedoms Act made amendments to RIPA to provide that following authorisation by an authorised Council officer to use the Act no surveillance can be conducted until that authorisation is approved by a Justice of the Peace. Therefore the Council's policy needs to be updated to reflect this change in process.

2.4 In addition, following the changes to the Council's management structure new officers are required to be authorising officers and the policy has been updated to reflect these changes.

3. Finance Comments

3.1 There are no financial implications in this report.

4. Legal Comments

4.1 The Council must ensure that it follows the procedures set out in this policy. A failure to do so may lead to evidence being inadmissible or the Council being guilty of maladministration.

5. Links to Corporate Aims (Please refer to the current edition of the Corporate Strategy)

5.1 There are no direct links to the Council's corporate aims.

6. Environmental Implications (If appropriate, consider impact on: carbon emissions; gas / electricity / other fuel usage including transport; biodiversity; and water and air quality. If appropriate, also consider adaptation requirements to the longer term impacts and opportunities of climate change such as increased heat and water stress, more flooding and stronger, more damaging wind speeds)

6.1 There are no environmental implications in this report.

7. Community Safety Implications (if appropriate, such as measures to combat anti-social behaviour)

7.1 There are no community safety implications in this report, although there will be community safety implications in assessing any applications under this policy.

8. Equalities Impact (An Equalities Impact Assessment should be carried out in respect of:-

- New initiatives/projects with an impact on staff, service or non-service users;
- New services/changes to the way services are delivered;
- New or refreshed Strategies;
- Events – Consultation/Training; and
- Financial/budget decisions.

8.1 There are no equalities impacts in this report.

9. Risk Management (if appropriate, such as reputational and health and safety risks. If the item the subject of the report has been included in a Service Plan, the result of the risk assessment undertaken when the plan was prepared should be entered here.

9.1 If the policy is not followed then the Council may suffer a risk to its reputation. In addition health and safety must be assessed as part of any authorisation request.

10. Partnership Implications (if any)

10.1 There are no partnership implications within this report.

11. Recommendations

11.1 The Committee are recommended to approve the policy as set out in Appendix 1 of this report.

Contact: Bruce Lang,
Assistant Chief Executive & Monitoring Officer
01823 356391
BDLang@westsomerset.gov.uk

CORPORATE POLICIES AND PROCEDURES ON THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

ISSUE DETAILS	
TITLE:	**RIPA Policy & Procedures Guide**
VERSION CONTROL	1.2 dated 3rd July 2008 1.3 dated 20 February 2009 1.4 dated March 2009 1.5 dated June 2010 (FINAL) 1.6 dated February 2014 (updated)
OWNER	Assistant Chief Executive and Monitoring Officer
APPROVED By:	Corporate Governance Committee 19 May 2014
REVIEW DATE	(1) March 2015 (2) March 2016

Contact: Bruce Lang
Assistant Chief Executive & Monitoring Officer
Taunton Deane Borough Council
The Deane House
Belvedere Road
Taunton TA1 1HE

Tel: 01823 356391 E-mail: BDLang@westsomerset.gov.uk

CONTENTS PAGE

A. Introduction and Key Messages

1. This Policy & Procedures Document is based upon the requirements of the Regulation of Investigatory Powers Act 2000 ('RIPA') and the Home Office's Code of Practices on Covert Surveillance and Covert Human Intelligence Sources (covert surveillance would be used only rarely and in exceptional circumstances).

2. The authoritative position on RIPA is, of course, the Act itself and any Officer who is unsure about any aspect of this document should contact, at the earliest possible opportunity, the Monitoring Officer, for advice and assistance.

3. Copies of this document and related forms will be placed on the intranet, once this Document has been approved by the Council and the Office of Surveillance Commissioners. This guide (but not the RIPA forms or the list of Authorising Officers) will be placed on the TDBC website.

4. The Monitoring Officer will maintain (and check) the Corporate Register of all RIPA authorisations, reviews, renewals, cancellations and rejections. However, it is the responsibility of the relevant Authorised Officer to ensure that the Monitoring Officer receives a copy of the relevant forms within 1 week of authorisation, review, renewal, cancellation or rejection.

5. RIPA and this document are important for the effective and efficient operation of the Council's actions with regard to covert surveillance and Covert Human Intelligence Sources. This document will, therefore, be kept under 12-monthly review by the Monitoring Officer. Authorised Officers must bring any suggestions for the improvement of this document to the attention of the Monitoring Officer at the earliest possible opportunity. The Council takes responsibility for ensuring that RIPA procedures are continuously improved.

6. The Monitoring Officer is the Council's nominated Single Point of Contact (SPOC) Officer who will be the normal point of contact for the Surveillance Commissioner and will field enquiries relating to RIPA.

7. If you are in any doubt on RIPA, this document or the related legislative provisions, please consult the Monitoring Officer or at the earliest possible opportunity.

8. This policy will be approved and monitored by the Corporate Governance Committee on a regular basis.

B. Council Policy Statement

1. The Council takes its statutory responsibilities seriously and it will at all times act in accordance with the law and take action that is both necessary and proportionate to the discharge of such statutory responsibilities. In that regard, the Monitoring Officer is duly authorised by the Council to keep this document up to date and to amend, delete, add or substitute relevant provisions, as necessary. For administrative and operational effectiveness, the Monitoring Officer is also authorised to add or substitute Officers authorised for the purposes of RIPA.

C. Effective Date of Operation : 1 March 2009 and Authorised Officer Responsibilities

1. The Corporate Policy, Procedures and the forms provided in this document will become operative with effect from the date of the Policy's approval.

2. Prior to the operative date, the Monitoring Officer will ensure that sufficient numbers of Authorised Officers are (after suitable training on RIPA and this document) duly certified to take action under this document.

3. Authorised Officers will also ensure that staff who report to them follow this Policy & Procedures Document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

4. Authorised 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 Authorised Officer approve any RIPA form unless and until s/he is satisfied that the health and safety of Council employees has been suitably addressed, and/or risks minimised so far as is possible, and that those health and safety considerations and risks are proportionate to/with the surveillance being proposed. If an Authorised Officer is in any doubt, s/he should obtain prior guidance.

5. Authorised Officers must also ensure that when sending copies of any forms to the Monitoring Officer, (or any other relevant authority), the same are sent in SEALED envelopes and marked 'Strictly Private & Confidential'.

D. General Information on RIPA

1. The Human Rights Act 1998 (which brought much of the European Convention on Human Rights and Fundamental Freedoms 1950 into UK domestic law) requires the Council (and organisations working on its behalf) to respect the private and family life of citizens, their home and their correspondence. See Article 8 of the European Convention.

2. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere with the citizen's right mentioned above, if such interference is:

    (a) in accordance with the law;

    (b) necessary (as defined in this document); and

    (c) proportionate (as defined in this document).

3. The Regulation of Investigatory Powers Act 2000 ('RIPA') provides a statutory mechanism (i.e. 'in accordance with the law') for authorising covert surveillance and the use of a 'covert human intelligence source' ('CHIS') - e.g. undercover agents, informers. 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 seeks to ensure that 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 RIPA during the time they are working for the Council. Therefore, all external agencies must comply with RIPA and work carried out by agencies on the Council's behalf must be properly authorised by one of the Council's designated Authorised Officers. Authorised Officers are those whose posts appear in Appendix (1) to this document (as added to or substituted by the Monitoring Officer).

5. If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration may be made to the Ombudsman, and/or the Council may be ordered to pay compensation. Were this to happen the good reputation of the Council will be damaged and it will undoubtedly be the subject of adverse press and media interest. Therefore, it is essential that all involved with RIPA comply with this document and any further guidance that may be issued from time to time by the Monitoring Officer.

6. A flowchart of the procedures to be followed appears at Appendix (2).

E. What RIPA Does and Does Not Do

1. RIPA does:

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

2. RIPA does not:

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

3. If the Authorised Officer or any Applicant is in any doubt, s/he should ask the Monitoring Officer before any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

F. Types of Surveillance

1. 'Surveillance' includes

- monitoring, observing, listening to people, watching or following their movements, listening to their conversations and other such activities or communications.

- recording anything mentioned above in the course of authorised surveillance.

- surveillance by, or with the assistance of, appropriate surveillance device(s).

Surveillance can be overt or covert.

2. Overt Surveillance

Most of the surveillance carried out by the Council will be done overtly - there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be behaving in the same way as a normal member of the public and/or will be going about Council business openly.

3. Similarly, surveillance will be overt if the subject has been told it will happen.

4. Covert Surveillance

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

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

6. Directed Surveillance

Directed Surveillance is surveillance which:-

- is covert; and

- is not intrusive surveillance (see definition below - the Council must not carry out any intrusive surveillance);

- is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it; and

- is undertaken for the purpose of a specific investigation or operation in a manner likely to obtain private information about an individual (whether or not that person is specifically targeted for purposes of an investigation). (Section 26(10) of RIPA).

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

8. Similarly, although overt town centre CCTV cameras do not normally require authorisation, authorisation will be required if the camera is tasked for a specific purpose which involves prolonged surveillance on a particular person. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others.

9. For the avoidance of doubt, only those Officers designated and certified to be 'Authorised Officers' for the purpose of RIPA can authorise 'Directed Surveillance' if, and only if, the RIPA authorisation procedures detailed in this document are followed. If an Authorised Officer has not been 'certified' for the purposes of RIPA, s/he cannot carry out or approve/reject any action set out in this Corporate Policy & Procedures Document.

   Further, an Authorised Office for RIPA purposes cannot delegate his/her power of authorisation to another officer unless that officer is also an Authorised Officer for RIPA purposes (and listed in Appendix 1), in which case that officer would be authorising in his own right. If in doubt, check with the Monitoring Officer. Officers will bear personal responsibility for ensuring correct RIPA authorisation procedures.

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

11. Intrusive Surveillance

This is when surveillance:

- is covert;

- relates to residential premises and private vehicles; and

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

12. Intrusive surveillance can be carried out only by police and other law enforcement agencies. Council Officers must not carry out intrusive surveillance.

13. Examples of different types of Surveillance

Type of Surveillance	Examples
Overt	- Police Officer or Parks Warden on patrol. - Signposted Town Centre CCTV cameras (in normal use). - Most test purchases (where the officer behaves no differently from a normal member of the public).
Covert but not requiring prior authorisation	- CCTV cameras providing general traffic, crime or public safety information.
Directed (must be RIPA authorised)	- Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit or genuinely on long term sick leave from employment. - Test purchases where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop-owner, e.g. where s/he is suspected of running his business in an unlawful manner.
Intrusive - (Council cannot do this)	- Planting a listening or other device (bug) in a person's home or in their private vehicle.
(See Appendix 6)	(Examples of different types of surveillance)

G. Conduct and Use of a Covert Human Intelligence Source (CHIS)

Who is a CHIS?

1. Someone who establishes or maintains a personal or other relationship for the covert purpose of covertly using or covertly disclosing information obtained by that relationship. In common parlance, an informer or 'under cover' Council Officer.

2. RIPA does not apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or where the public contact telephone numbers set up by the Council to receive information.

What must be authorised?

3. The Conduct or Use of a CHIS require prior authorisation.

   - Conduct of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or incidental to the covert purpose of) obtaining and passing on information.

   - Use of a CHIS = Covers inducing, asking, or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

4. The Council can use CHIS's if, and only if, the RIPA procedures, detailed in this document are followed.

Juvenile Sources

5. Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 years of age). On no account can a child under 16 years of age be authorised to give information against his or her parents.

Vulnerable Individuals

6. 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.

7. A Vulnerable Individual will only be authorised to act as a source in the most exceptional of circumstances.

Test Purchases

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

9. 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 for directed surveillance.

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

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

11. Recording sound on private premises could constitute intrusive surveillance unless it is done overtly. It will be possible to record noise levels without it being intrusive surveillance if the noisemaker is given written warning that such recording or monitoring will occur. (Such a warning should be repeated at least every 2 months if the operation is on-going). Placing a stationary or mobile video camera outside a building to record anti-social behaviour on residential estates will require prior authorisation.

    Noise recordings should only ever be made from a complainant’s property or land that is open to the pubic. Covert recording within the premises of the alleged noise-maker would constitute Intrusive Surveillance, and is not permitted for Council Staff.

H. Authorisation Procedures

1. Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised and in strict accordance with the terms of the authorisation. Appendix (2) provides a flow chart of the authorisation process from application consideration to recording of information.

2. The Regulation of Investigatory Powers (Directed Surveillance and Cover Human Intelligence Sources) (Amendment) Order 2012 (made on 11 June 2012) comes into force on 1st November 2012 and will further restrict the Council's powers to grant a RIPA authorisation.

3. From this date authorisations can only be granted where the authorisation is for the purpose of preventing or detecting crime and that crime constitutes one or more criminal offences. Additionally the criminal offences being contemplated must be ones which are punishable by a prison sentence of at least six months. There are exceptions to this requirement covering various offences under s146 and s147 Licensing Act 2003 (effectively selling alcohol to children).

4. On 1st May 2012, the Protection of Freedoms Bill received Royal Assent to become the Protection of Freedoms Act 2012.

5. The Protection of Freedoms Act 2012 (Commencement No.2) Order 2012 (SI 2012/2075) ('the Order') was made on 7th August 2012 bringing in various provisions of the Protections of Freedoms Act 2012 into force during 2012.

6. Article 4 of the Order commences amendments to the Regulation of Investigatory Powers Act 2000 ("RIPA") on 1st November 2012.

7. The amendment in respect of RIPA authorisations is that when an authorisation is granted it will not take effect until such time (if any) as a Justice of the Peace has made an order approving the grant of the authorisation.

Authorised Officers

8. Forms can only be signed by Authorised Officers who hold a Certificate of RIPA Eligibility from the Monitoring Officer as shown in Appendix (3). Authorised Officer posts are listed in Appendix (1). This Appendix will be kept up to date by the Monitoring Officer and added to as needs require. The Monitoring Officer has been duly authorised to add, delete or substitute posts listed in Appendix (1).

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

Training Records

10. Proper training will be given or approved by the Monitoring Officer before Authorised Officers are issued with a Certificate of RIPA Eligibility enabling them

to sign any RIPA forms. The issue of a Certificate of RIPA Eligibility will also have the dual purpose of confirming that the Officer has been RIPA trained and a Corproate Register of all those individuals who have been issued with such Certificates will be kept by the Monitoring Officer.

11. If the Monitoring Officer feels at any time that an Authorised Officer has not complied fully with the requirements of this document, or the training provided to him, the Monitoring Officer is duly authorised to retract that Officer's Certificate of RIPA Eligibility until s/he has undertaken further approved training. Were this to happen the Officer could no longer authorise RIPA Procedures.

Application Forms

12. Only the approved RIPA forms set out in this document must be used.

For the most up to date forms see:-

http://www.homeoffice.gov.uk/government/collections/ripa-forms-2

Grounds for Authorisation

13. Directed Surveillance or the Conduct and Use of the CHIS can be authorised by the Council only for the prevention or detection of crime or preventing disorder.

Assessing the Application Form

14. Before an Authorised Officer signs a form, they must:

(a) Be mindful of this Policy & Procedures Document, the training provided or approved by the Monitoring Officer and any other guidance issued, from time to time, by the Monitoring Officer on such matters;

(b) Satisfy themselves that the RIPA authorisation is:

(i) in accordance with the law;
(ii) necessary in the circumstances of the particular case on one of the grounds mentioned in paragraph 13 above; and
(iii) proportionate to what it seeks to achieve.

(c) In assessing whether or not the proposed surveillance is proportionate, consider other appropriate means of gathering the information. 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) unnecessary collateral intrusion into the lives of those not directly connected with the investigation or operation. 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) Allocate a Unique Reference Number (URN) for the application as follows:
Year / Group / Number of Application

(g) Ensure that the RIPA Service Register is duly completed, and that a copy of the RIPA forms (and any review/cancellation of the same) is forwarded to the Monitoring Officer for inclusion in the Corporate Register within one week of the relevant authorisation, review, renewal, cancellation or rejection.

Additional Safeguards when Authorising a CHIS

15. When authorising the conduct or use of a CHIS, the Authorised 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 these arrangements 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; and

(e) ensure records contain particulars and that they are not available except on a need to know basis.

16. The Authorised Officer must record a clear description of what authority is being granted for by reference to subjects, property or location and the type of surveillance permitted. This may not be the same as what is being requested.

17. If an application is granted, the Authorising Officer must set a date for its review, and ensure that it is reviewed on that date. Records must be kept in relation to all RIPA applications and authorisations.

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

19. A ‘Surveillance Log Book’ should be completed by the investigating officer(s) to record all operational details of authorized covert surveillance or the use of a CHIS. Once completed, the Log Book should be passed to their relevant RIPA

co-ordinator for safe keeping in a secure place. Each group will also maintain a record of the issue and movement of all Surveillance Log Books.

Urgent Authorisations

20. Urgent authorisations should not be necessary. However, in exceptional circumstances, urgent authorisations may be given orally if the time that will elapse before a written authorisation can be granted will be likely to endanger life or jeopardise the investigation or operation for which the authorisation is being given.

21. It will not be urgent or an exceptional circumstance where the need for authorisation has been neglected or the situation is of the Officer's own making.

22. Urgent authorisations last for no more than 72 hours. They must be recorded in writing on the standard form as soon as practicable and the extra boxes on the form must be completed to explain why the authorisation is urgent.

Duration

23. The form must be reviewed in the time stated, and cancelled once it is no longer needed. The 'authorisation' to carry out/conduct the surveillance lasts for 3 months (from date of authorisation) for Directed Surveillance, and 12 months (from date of authorisation) for a CHIS. Any adjustments to the time period must be made by means of either a cancellation or a renewal.

24. However, whether or not the surveillance is carried out/conducted in the relevant period has no bearing on the authorisation becoming spent. In other words, the forms do not expire! The forms have to be reviewed and/or cancelled (once they are no longer required).

25. An urgent oral authorisation (if not already ratified in a written authorisation) will cease to have effect after 72 hours, beginning with the time when the authorisation was granted.

26. Authorisations shall be renewed in writing when the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred.

27. The renewal will begin on the day when the authorisation would have expired. In exceptional circumstances, renewals may be granted orally in urgent cases (but see above) and they last for a period of 72 hours.

I. Working With / Through Other Agencies

1. When another agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and its forms must be used by the Council Officers concerned (in accordance with the normal procedure), the agency advised and kept informed of the various RIPA requirements. They must be made explicitly aware of what they are authorised to do, preferably in writing (with a copy of the written instructions countersigned by the agency by way of acknowledgement of their instructions and returned to the instructing officer). If for reasons of urgency oral instructions are initially given, written confirmation must be sent and acknowledged within 4 working days. Officers must be satisfied that agencies are RIPA competent & RIPA trained before they are used.

2. When some other agency (e.g. Police, Customs & Excise, Inland Revenue etc):

(a) Wish to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and before any Officer agrees to allow the Council's resources to be used for the other agency's purposes s/he must obtain a copy of that agency's completed RIPA form for the Council's records (a copy of which must be passed to the Monitoring Officer for the Corporate Register) or relevant extracts from the agencies RIPA form which are sufficient for the purposes of protecting the Council and use of its resources;

(b) Wish to use the Council's premises for their own RIPA action, the Council Officer concerned should normally co-operate with such a request, 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 need to be sought from the other agency to protect the Council's legal position (the Council's insurance officer and/or the Monitoring Officer can advise on this issue). In such cases the Council's own RIPA forms should not be used as the Council is only 'assisting' and not being 'involved' in the RIPA activity of the external agency.

3. With regard to 2(a) above, if the Police or other agency wish to use Council resources for general surveillance (as opposed to specific RIPA operations) an appropriate letter requesting the proposed use (and detailing the 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. The insurance/indemnity considerations mentioned above may still need to be addressed.

4. In addition should any officer wish to work in partnership with any other agency where the Council intend to share with that other agency any evidence obtained through surveillance activities then the advice of the Monitoring Officer or the Deputy Monitoring Officer should be first sought.

5. If in doubt, please consult with the Monitoring Officer at the earliest opportunity.

J. Records Management

1. The Council must keep a detailed record of all authorisations, renewals, cancellations and rejections generated by officers and a Corporate Register of all Authorisation forms will be maintained and monitored by the Monitoring Officer.

2. Records maintained by individual services

The following documents must be retained:

- a copy of any completed application form together with any supplementary documentation and notification of the approval given by the Authorised Officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorised 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;
- a copy of any cancellation of an authorisation;
- the date and time when any instruction was given by the Authorised Officer;
- the Unique Reference Number for the authorisation (URN).

3. Each form will have a URN. The cross-referencing of each URN takes place within the forms for audit purposes. Rejected forms will also have URN's.

Corporate Register maintained by the Monitoring Officer

4. Authorised Officers must forward details of each form to the Monitoring Officer for the Corporate Register within 1 week of the authorisation, review, renewal, cancellation or rejection. The Monitoring Officer will monitor the same and give appropriate guidance from time to time or amend this document, as necessary.

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

K. Material obtained during investigations

1. Generally, all material (in whatever media) obtained or produced during the course of investigations subject to RIPA authorisations should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 1998, the Freedom of Information Act 2000, any other legal requirements including those of confidentiality. The following paragraphs give guidance on some specific situations, but advice should be sought from the Monitoring Officer or the Data Protection Officer where appropriate.

2. Where material is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should not be destroyed, but retained in accordance with legal disclosure requirements.

3. Where material is obtained, which is not related to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to suspect that it will be relevant to any future civil or criminal proceedings, it should be destroyed immediately.

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

5. Where material obtained is of a confidential nature then the following additional precautions should be taken:

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

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

L. Amendments to this guidance document

1. The Monitoring Officer is duly authorised to keep this guidance document up to date, and to amend, delete, add or substitute any provisions as s/he deems necessary. For administrative and operational effectiveness, s/he is also authorised to amend the list of 'Authorising Officer Posts" set out in Appendix 1, by adding, deleting or substituting any posts.

2. The RIPA Corporate Officers Working Group shall supplement any training requirements with exchanges of experiences in the operation of this document and any recommendations to improve this document will be considered by the Council's Monitoring Officer.

M. Complaints Handling

1. Taunton Deane Borough Council's Surveillance Complaints Procedure

Complaints concerning breaches of the code may be made to the Council's Chief Executive, Taunton Deane Borough Council, The Deane House, Belvedere Road, Taunton, Somerset, TA1 1HE.

If a complaint is received from a member of the public or a person who has been subject to any form of surveillance the complaint will be referred to the Monitoring Officer for investigation.

Thereafter a decision will be taken, as to what action, if any, should be taken in line with the Council's Complaints Policy.

2. Independent Tribunal

The Regulation of Investigatory Powers Act 2000 also establishes an independent tribunal made up of Senior Members of the Judiciary and the Legal Profession and is independent of the government. The tribunal has full powers to investigate and decide any case within its jurisdiction. If a complaint is therefore received from an individual who has been subject to surveillance or by a member of the public then that person or persons should be referred immediately to the Investigatory Powers Tribunal.

The address for the Investigatory Powers Tribunal is PO Box 33220 London SW1H 9ZQ.

N. Useful contacts

6.1 Local Authorities Coordinators of Regulatory Services (LACORS) - www.lacors.gov.uk

6.2 Office of the Surveillance Commissioner – https://osc.independent.gov.uk/

6.3 RIPA forms- https://www.gov.uk/government/collections/ripa-forms--2

6.4 RIPA codes of practice- https://osc.independent.gov.uk/

6.5 RIPA home office guidance – https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa

O. Concluding Remarks of the Monitoring Officer

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

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

3. Authorised 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 both their personal responsibilities and the Council's responsibilities under RIPA and the European Convention.

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

5. Those carrying out surveillance must inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation.

6. For further advice and assistance on RIPA, please contact the Monitoring Officer. Details are provided on the front of this document.

APPENDIX 1

List of Authorised Officer Posts

OVERALL RESPONSIBILITY: BRUCE LANG, ASSISTANT CHIEF EXECUTIVE/MONITORING OFFICER.

Authorising Officer's Name	**Designation**
Penny James	Chief Executive
Bruce Lang	Assistant Chief Executive & Monitoring Officer
James Barrah	Director of Housing & Communities
Tim Burton	Assistant Director of Planning & Environment
Paul Fitzgerald	Assistant Director of Resources
Chris Hall	Assistant Director of Operational Development
Simon Lewis	Assistant Director of Housing & Communities
Heather Tiso	Head of Revenues and Benefits Service

IMPORTANT NOTES

A. Even if a post is identified in the above list the persons currently employed in such posts are not authorised to sign RIPA forms (including a renewal or cancellation) unless s/he has been certified by the Monitoring Officer to do so by the issue of a Certificate of RIPA Eligibility.

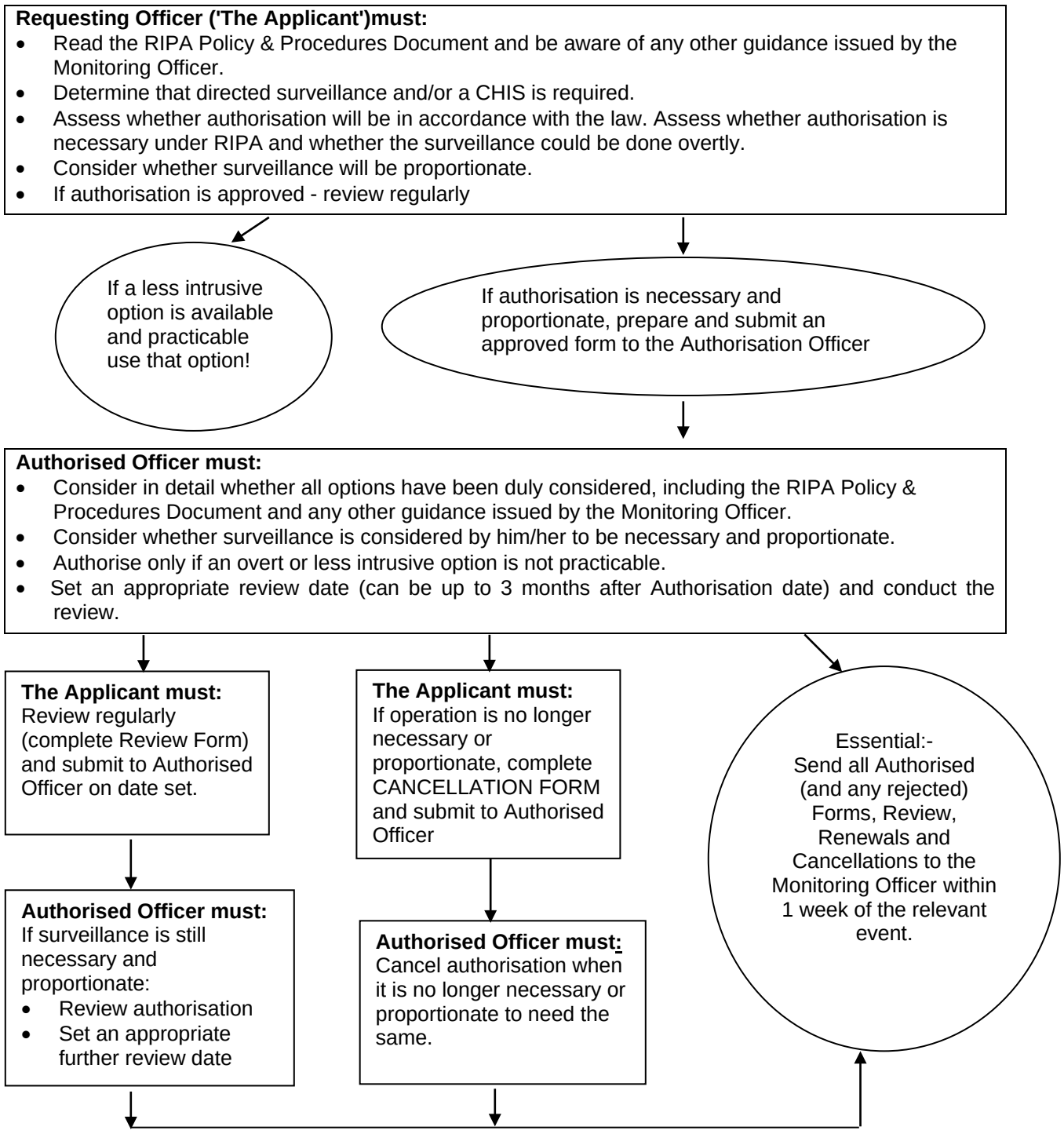
B. Only the Chief Executive and the Assistant Chief Executive & Monitoring Officer (Bruce Lang as of January 2014) are authorised to sign forms relating to Juvenile Sources and Vulnerable Individuals (see paragraph G of this document).

C. Particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. In cases where through the use of surveillance it is likely that knowledge of confidential information will be acquired, the use of surveillance is subject to a higher level of authorisation; such authorisations will only be given by the CEO or by Bruce Lang.

D. If in doubt, ask the Monitoring Officer before any directed surveillance and/or CHIS is authorised, renewed, rejected or cancelled.

APPENDIX 2

RIPA FLOW CHART



NB: If in doubt, ask the Monitoring Officer before any directed surveillance and/or CHIS is authorised, renewed, cancelled, or rejected.

PROCEDURE FOR MAGISTRATES COURT

Once authorisation has been granted, an application must be made to the Magistrates Court for a hearing.

The Investigating Officers must be authorized to appear in order to give evidence.

The Magistrates will need a copy of the original authorisation/notice and two copies of the judicial application/order.

The hearing will be held in private by one Justice of the Peace and the application must stand on its own.

If granted the Justice of the Peace will sign the order and a copy must be retained.

Advice and assistance can be sought from the Monitoring Officer or the Deputy Monitoring Officer and reference should be made to the Home Office guidance before making the application.

APPENDIX 3

TAUNTON DEANE BOROUGH COUNCIL

RIPA AUTHORISING OFFICER CERTIFICATE
No. [ ] / 200-

I HEREBY CERTIFY that the Officer whose personal details are given below is an Authorising Officer for the purposes of authorising covert surveillance and the use and/or conduct of Covert Human Intelligence Sources ('CHIS') under the provisions of the Regulation of Investigatory Powers Act 2000.

It is further certified that this Officer has received training to perform such authorisation procedures.

Certificate issued to:
[Full name of Officer] _____

Job Title: _____

Service: _____

Location: _____

Certificate date: _____

(signed) _____

Bruce Lang
Monitoring Officer
(Taunton Deane Borough Council)

(Please note:- This certificate and the authorisation granted by it is personal to the officer named in it and cannot be transferred. Any change in personal details must be notified in writing to the Monitoring Officer immediately. This certificate can be revoked at any time by the Monitoring Officer by written revocation issued to the officer concerned. It is the named officer's personal responsibility to ensure full compliance with RIPA authorisation procedures and to ensure that s/he is fully trained in such procedures and that such training is kept up to date).

APPENDIX 4

For the latest forms please go to this link

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

APPENDIX 5

EXAMPLES OF COVERT SURVEILLANCE

The following are examples of covert surveillance operations that may be conducted by Council staff, with indications as to whether RIPA authorisation may be needed.

If there are any special circumstances to an operation which, in general terms, matches one of the examples below, then the need for authorisation should be re-assessed by the Case Officer.

Example 1 -

Use of fixed CCTV cameras to record fly-tipping in the area around Recycling Centres in Council Car Parks.

Points to consider:

a) The cameras are in plain view and are therefore not covert, even if they are being used as part of a defined and pre-planned Operation.

b) By definition, these are well-used public areas and any expectation as to privacy would be minimal.

c) Collateral intrusion and the opportunity to obtain private information is unlikely.

Recommendation:

Unless there are additional and unusual features to the Operation, RIPA Authorisation would not be required.

Example 2 –

Use of temporary surveillance cameras to record fly-tipping in a public area such as a layby or a wooded area close to a road.

Points to consider:

a) Cameras and recording equipment would be deliberately concealed from view.

b) Although the area is accessible to the public, it is likely to be less frequented than, for example, a Council car park. There would therefore be a heightened expectation as to privacy.

c) The fact that fly-tipping is an illegal act does not reduce the perpetrators' rights to be protected.

d) Collateral intrusion and the opportunity to obtain private information, are more likely than in Example 1, above.

Recommendation:

On balance, RIPA authorisation for Directed Surveillance should be obtained.

This could be avoided by the publication in the local press beforehand of an article explaining that a given area would be placed under surveillance for a given period of time. However, this would largely negate the usefulness of the Operation.

Example 3 –

Use of noise recording equipment, in a complainant's property, with the tape recorder being operated by the complainant when noise events occur.

Points to consider:

a) The equipment is concealed from the occupants of the premises under surveillance (the Object). It is therefore a covert operation, unless the occupants of the premises under audio surveillance had been warned, in writing, that surveillance may be carried out within a given period of time.

b) The premises under surveillance are not public in any sense, and the expectation as to privacy would be very high.

c) Noise events coming from the premises under surveillance and affecting the complainant's premises might be regarded as no longer being private, as boundaries into other areas had been crossed by the time the noise was recorded.

However, there may well be instances (for example between poorly insulated flats or rooms within bedsits) where this consideration does not apply.

d) The possibility of collateral intrusion and the opportunity to obtain private information, are likely.

e) As the tape recording is operated by the complainant, it is possible (s)he is acting as a Covert Human Intelligence Source (CHIS).

Recommendation:

a) RIPA authorisation for Directed Surveillance should be sought by the Case Officer when the premises under surveillance are residential, unless:

i) The occupants of the premises under surveillance had been warned, in writing and in advance, that audio surveillance may be used, and/or

ii) There is such separation between the complainant's property and the property under surveillance that it could not be claimed that noise events passing from one to the other were of a private nature.

b) RIPA authorisation of the complainant as a CHIS should be considered if there was any form of relationship between the complainant and the occupants of the premises under surveillance. A relationship may include, for example, long-term neighbours who regularly speak to each other and who may, generally, be on good terms.

However, the need for Authorisation would only seem to apply if it is the clear intention to use this relationship, covertly, for the express purpose of obtaining confidential information. Clearly, in practically every case, this would not be the intention.

However, if the complainant may be able to influence the onset of a noise event from the object premises by using their relationship with the object, then the use of monitoring equipment, with or without RIPA Authorisation(s) would be inappropriate. To give an extreme example, the complainant may say to the object "…we are going out tonight, so you can play your music as loud as you like!".

Note: If the complainant, including any member of their household who may operate noise recording equipment, is judged to be acting as a CHIS, then it is immaterial whether or not the object has been informed of the likelihood of audio surveillance. Authorisation as a CHIS would still be required.

As part of the CHIS Authorisation, careful consideration must be given to the conditions to be imposed to prevent misuse of the relationship between complainant and object.

Example 4 –

Covert observation of a Night Club entrance to determine the number of patrons in the premises.

Points to consider:

a) No image or sound recording equipment is in use, so the opportunities for either collateral intrusion or of obtaining private information do not apply.

b) No individual person is under surveillance.

c) The queue that forms outside a Night Club is, by its nature, in a public place and is likely to be one that is well used.

Expectations as to privacy by any person outside the Club premises would therefore be very low.

Recommendation:

Unless there are additional and unusual features to the Operation, RIPA Authorisation would not be required.

Example 5 –

Asking a disabled person to book a taxi and complete a journey to determine whether the taxi driver was discriminatory and to report back to Licensing for possible enforcement action.

Points to consider:

a) The purpose of the journey would be to gather information.

b) It would be pre-planned.

c) It would be designed to be covert.

d) The nature and duration of the exercise make it likely that that a relationship, in legal terms, would be formed.

e) The expectation as to privacy would be high.

f) It is likely that, whether planned or not, confidential information would be obtained.

Recommendation:

a) It is considered that an Authorisation for Directed Surveillance would be required.

b) It is also considered that the disabled person would qualify as a CHIS, so that additional Authorisation would be required specifically for that aspect.

c) If it were intended to record conversation between the parties, this would constitute Intrusive Surveillance. Authorisation would not be possible and the surveillance itself would be unlawful.

END

March 2014

Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)

Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance

Home Office

October 2012

Contents

1. INTRODUCTION: HOW THE LAW HAS CHANGED

1. On 1 November 2012 two significant changes will take effect governing 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[1] will mean that local authority authorisations and notices under RIPA for the use of particular covert techniques can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace (JP).
- **Directed surveillance crime threshold**: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order")[2] mean that a local authority can now only grant an authorisation under RIPA for the use of directed surveillance where the local authority is investigating particular types of criminal offences. These are criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco.

2. This guidance is non-statutory but provides advice on how local authorities can best approach these changes in law and the new arrangements that need to be put in place to implement them effectively. It is supplementary to the legislation and to the statutory Codes of Practice. If a local authority has any doubts about the new regime they should consult their legal advisers. This guidance is intended for local authority investigation teams that may use covert techniques, including Trading Standards, Environmental Health and Benefit Fraud Officers. However, it will also be of use to authorising officers and designated persons and to those who oversee the use of investigatory techniques in local authorities including elected members.

3. Separate guidance is available for Magistrates' Courts in England and Wales and local authorities in Scotland.

1 Sections 37 and 38 of the Protection of Freedoms Act 2012 amend RIPA and will come into force on 1 November 2012.
2 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 [SI 2010/521] will be amended by the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 [SI 2012/1500] on 1 November 2012. See Section 5 for links.

2. LOCAL AUTHORITY USE OF RIPA

THE EXISTING REGULATORY FRAMEWORK

4. RIPA sets out a regulatory framework for the use of covert investigatory techniques by public authorities. RIPA does not provide any powers to carry out covert activities. If such activities are conducted by council officers, then RIPA regulates them in a manner that is compatible with the European Convention on Human Rights (ECHR), particularly Article 8, the right to respect for private and family life.

5. RIPA limits local authorities to using three covert techniques (details set out below) for the purpose of preventing or detecting crime or preventing disorder.

6. Use of these techniques has to be authorised internally by an authorising officer or a designated person. They can only be used where it is considered necessary (e.g. to investigate a suspected crime or disorder) and proportionate (e.g. balancing the seriousness of the intrusion into privacy against the seriousness of the offence and whether the information can be obtained by other means). The relevant Codes of Practice should be referred to for further information on the scope of powers, necessity and proportionality.[3]

THE TECHNIQUES WHICH LOCAL AUTHORITIES MAY USE

7. **Directed surveillance** is essentially covert surveillance in places other than residential premises or private vehicles[4].

8. Local authorities cannot conduct 'intrusive' surveillance (i.e. covert surveillance carried out in residential premises or private vehicles[5]) under the RIPA framework.

9. A **covert human intelligence source (CHIS) includes** undercover officers, public informants and people who make test purchases.

10. **Communications data** (CD) is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). RIPA groups CD into three types:

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

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

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

3 See section 5 for links to the relevant legislation and codes of practice.
4 Further information on directed surveillance can be found in the Covert Surveillance and Property Interference Code of Practice.
5 Places where legal consultations are likely to take place will also be treated as intrusive surveillance.

RANK OF LOCAL AUTHORITY AUTHORISING OFFICERS/DESIGNATED PERSONS

13. Local authority authorising officers/designated persons will remain as designated by RIPA consolidating orders SI 2010 Nos.480 and 521:

- Director, Head of Service, Service Manager[6] or equivalent.

14. The authorisation of directed surveillance or use of a CHIS likely to obtain confidential information or the deployment of a juvenile or vulnerable person (by virtue of mental or other condition) as a CHIS requires authorisation by the most senior local authority officer – Head of Paid Service or, in his/her absence, the acting Head of Paid Service.

15. If there is any doubt regarding sufficiency of rank you should contact your Local Authority Monitoring Officer who will be able to advise you.

TIME LIMITS

16. The current time limits for an authorisation or notice will continue[7]. That is: 3 months for directed surveillance and 12 months for a CHIS (1 month if the CHIS is 18). Authorisations and notices for CD will be valid for a maximum of one month from the date the JP has approved the grant. This means that the conduct authorised should have been commenced or the notice served within that month.

17. A renewal must be authorised prior to the expiry of the original authorisation, but it runs from the expiry date and time of that original authorisation. Authorisations may be renewed more than once if still considered necessary and proportionate and approved by the JP.

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

6 For CD RIPA applications, the Local Government Group and the Interception of Communications Commissioner's Office have advised that a Principal Trading Standards Officer is not considered to be of sufficient seniority to act as the Designated Person.

7 See section 43 RIPA.

3. DIRECTED SURVEILLANCE CRIME THRESHOLD

19. The crime threshold applies only to the authorisation of **directed surveillance** by local authorities under RIPA, not to the authorisation of local authority use of CHIS or their acquisition of CD. The threshold will come into effect on 1 November 2012.

20. The amendments to the 2010 Order have the following effect:

- Local authorities can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment **or** are related to the underage sale of alcohol and tobacco. The offences relating to the latter are in article 7A of the 2010 Order[8].
- Local authorities **cannot** authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.
- Local authorities may therefore continue to authorise use of directed surveillance in more serious cases as long as the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a JP has been granted. Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more could include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud.
- Local authorities may also continue to authorise the use of directed surveillance for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the necessity and proportionality test is met and prior approval from a JP has been granted.
- A local authority **may not authorise** the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low-level offences which may include, for example, littering, dog control and fly-posting.

21. The change will affect authorisations or renewals which are granted on of after 1 November. It will not affect authorisations or renewals granted before that date.

IMPACT ON INVESTIGATIONS

22. At the start of an investigation, council officers will need to satisfy themselves that what they are investigating is a criminal offence. Directed surveillance is an invasive technique and at the point it is decided whether or not to authorise its use it must be clear that the threshold is met and that it is necessary and proportionate to use it.

23. During the course of an investigation the type and seriousness of offences may change. The option of authorising directed surveillance is dependent on the offence under investigation attracting a sentence of a maximum six months imprisonment or more or being related to the underage sale of alcohol and tobacco. Providing the offence under investigation is one which appears on the statute book with at least a maximum six months term of imprisonment or is related to the specific offences listed in the order concerning the underage sale of alcohol and tobacco an application can be made. However, if during the investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold the use of directed surveillance should cease. If a directed surveillance authorisation is already in force it should be cancelled.

8 See section 5 for links to the relevant legislation

24. Directed surveillance will be authorised against a specific offence which meets the threshold, and the type and the timing of the deployment of the surveillance will always reflect this. There may be cases where it is possible, with the same evidence obtained by the same deployment, to substantiate a variety of different charges, some of which fall below the threshold, it will be for the courts to decide whether to admit – and what weight to attach to – the evidence obtained in the lesser charges.

25. Local authorities will no longer be able to use directed surveillance in some cases where it was previously authorised. But this does not mean that it will not be possible to investigate these areas with a view to stopping offending behaviour. The statutory RIPA Code of Practice on covert surveillance makes it clear that routine patrols, observation at trouble 'hotspots', immediate response to events and overt use of CCTV are all techniques which do not require RIPA authorisation.[9]

9 See paragraphs 2.21-2.29 of the Covert Surveillance and Property Interference Code of Practice.

4. JUDICIAL APPROVAL

WHAT THE CHANGES MEAN FOR LOCAL AUTHORITIES

26. From 1 November 2012, sections 37 and 38 of the Protection of Freedoms Act 2012 will commence. This will mean that a local authority who wishes to authorise the use of directed surveillance, acquisition of CD and use of a CHIS under RIPA will need to obtain an order approving the grant or renewal of an authorisation or notice from a JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

27. The new judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined in the Codes of Practice. The current local authority process of assessing necessity and proportionality, completing the RIPA authorisation/application form and seeking approval from an authorising officer/designated person will remain the same.

28. The inspection regimes of the independent RIPA oversight Commissioners will continue to apply to local authorities and the frequency and nature of their independent inspections of local authorities is not expected to change.

29. The judiciary is independent and it is not the role of the Commissioners to inspect the decision of the JP.[10] However the Commissioners will continue to have an important oversight role and will continue to inspect local authority use of RIPA. If the Commissioners identify an error in the authorisation process they will, as now, need to consider the best course of action. This may include asking the local authority to cancel the authorisation in question and, if appropriate, complete a new authorisation addressing their concerns which will need to be approved by the JP in the usual way. When an error is brought to the attention of a local authority they should cease the activity authorised.

30. The Commissioners will continue to advise local authorities of the procedures and training to adopt, on what is best practice and will continue to report to Parliament on relevant trends and findings.

PROCEDURE FOR APPLYING FOR JUDICIAL APPROVAL

Making the Application

31. The flowchart at Annex A outlines the procedure for applying for judicial approval. The application must be made by the public authority that has granted the authorisation[11]. Following approval by the authorising officer/designated person the first stage of the process is for the local authority to contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the magistrates' court to arrange a hearing.

10 See section 62(2A) RIPA.

11 Some local authorities may enter into arrangements to form a regional group with other local authorities but the group cannot itself make the application. Only local authority officers in local authorities described in SIs 2010 Nos.480 and 521 are able to authorise under RIPA.

32. The local authority will provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and **should contain all information that is relied upon**. For communications data requests the RIPA authorisation or notice may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assessed by the JP as part of his consideration (see Annex C for considerations relating to CD authorisations and notices).

33. The original RIPA authorisation or notice 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 court may wish to take a copy.

34. In addition, the local authority will provide the JP with a partially completed judicial application/order form (at Annex B).

35. Although the local authority is required 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.

36. The order section of this form will be completed by the JP and will be the official record of the JP's decision. The local authority will need to obtain judicial approval for all initial RIPA authorisations/ applications **and renewals** and the local authority will need to retain a copy of the judicial application/ order form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

Arranging a Hearing

37. It will be important for each local authority to establish contact with HMCTS administration at the magistrates' court. HMCTS administration will be the first point of contact for the local authority when seeking a JP approval. The local authority will inform HMCTS administration as soon as possible to request a hearing.

38. On the rare occasions where out of hours access to a JP is required then it will be for the local authority to make local arrangements with the relevant HMCTS legal staff. In these cases the local authority will need to provide two partially completed judicial application/order forms so that one can be retained by the JP. The local authority should provide the court with a copy of the signed judicial application/order form the next working day.

39. In most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior JP approval. No RIPA authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it (for instance when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening).

40. Where renewals are timetabled to fall outside of court hours, for example during a holiday period, it is the local authority's responsibility to ensure that the renewal is completed ahead of the deadline. Out of hours procedures are for emergencies and should not be used because a renewal has not been processed in time.

Attending a Hearing

41. The hearing is a 'legal proceeding' and therefore local authority officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the JP.

42. The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation or notice and the judicial application/order form. He/she may have questions to clarify points or require additional reassurance on particular matters.

43. Local authorities will want to consider who is best able to answer the JP's questions on the policy and practice of conducting covert operations and detail of the case itself. It is envisaged that the case investigator will be able to fulfil this role. The investigator will know the most about the investigation and will have determined that use of a covert technique is required in order to progress a particular case. The local authority may consider it appropriate for the SPoC (single point of contact) to attend for applications for CD RIPA authorisations or notices (see Annex C for considerations relating to CD authorisations and notices). This does not, however, remove or reduce in any way the duty of the authorising officer to determine whether the tests of necessity and proportionality have been met. Similarly, it does not remove or reduce the need for the forms and supporting papers that the authorising officer has considered and which are provided to the JP to make the case (see paragraphs 47-48).

44. The usual procedure would be for local authority Standing Orders to designate certain officers, including SPoCs, for the purpose of presenting RIPA cases to JPs under section 223 of the Local Government Act 1972. A pool of suitable officers could be designated at the start of the year when the Orders are examined and adjusted as appropriate throughout the year.

45. It is not envisaged that the skills of legally trained personnel will be required to make the case to the JP and this would be likely to, unnecessarily, increase the costs of local authority applications.

Decision

46. The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed or the notice was given or renewed, there were reasonable grounds for believing that the authorisation or notice 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.[12]

12 Further information on these restrictions can be found in the Regulation of Investigatory Powers Act 2000: Consolidating Orders and Codes of Practice, SI 2012 No.1500 (The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment), SI 2000 No.2793 (The Regulation of Investigatory Powers (Juveniles) Order 2000) and the OSC Procedures and guidance manual, available to public authorities on request from the Office of Surveillance Commissioners.

47. **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 may note on the form any additional information he or she has received during the course of the hearing but information fundamental to the case should not be submitted in this manner.

48. If more information is required to determine whether the authorisation or notice has met the tests then the JP will refuse the authorisation. If an application is refused the local authority 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.

49. The JP will record his/her decision on the order section of the judicial application/order form. HMCTS administration will retain a copy of the local authority RIPA authorisation or notice and the judicial application/order form. This information will be retained securely. Magistrates' courts are not public authorities for the purposes of the Freedom of Information Act 2000.

50. The local authority will need to provide a copy of the order to the communications the SPoC (Single Point of Contact) for all CD requests. SPoCs must not acquire the CD requested, either via the CSP or automated systems until the JP has signed the order approving the grant.

Outcomes

51. Following their consideration of the case the JP will complete the order section of the judicial application/order form (see form at Annex B) recording their decision. The various outcomes are detailed below and reflected on the flowchart at Annex A.

52. The JP may decide to[13] –

- **Approve the Grant or renewal of an authorisation or notice**

  The grant or renewal of the RIPA authorisation or notice will then take effect and the local authority may proceed to use the technique in that particular case.

  In relation to CD, the local authority will be responsible for providing a copy of the order to the SPoC.

- **Refuse to approve the grant or renewal of an authorisation or notice**

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

  Where an application has been refused the local authority may wish to consider the reasons for that refusal. For example, a technical error in the form may be remedied without the local authority going through the internal authorisation process again. The local authority may then wish to reapply for judicial approval once those steps have been taken.

13 See sections 23B(3) and 32B(3) of the Regulation of Investigatory Powers Act 2000.

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

  This applies where a magistrates' court refuses to approve the grant, giving or renewal of an authorisation or notice and decides to quash the original authorisation or notice.

  The court must not exercise its power to quash that authorisation or notice unless the applicant has had at least 2 business days from the date of the refusal in which to make representations.

Complaints/Judicial Review

53. There is no complaint route for a judicial decision unless it was made in bad faith. Any complaints should be addressed to the Magistrates' Advisory Committee.

54. A local authority may only appeal a JP decision on a point of law by juidical review. If such a concern arises, the local authority should consult their legal advisers.

55. The IPT will continue to investigate complaints by individuals about the use of RIPA techniques by public bodies, including local authorities. If, following a complaint to them, the IPT does find fault with a RIPA authorisation or notice it has the power to quash the JP's order which approved the grant or renewal of the authorisation or notice.

5. OTHER SOURCES OF REFERENCE

- The Regulation of Investigatory Powers Act 2000
  http://www.legislation.gov.uk/ukpga/2000/23/contents

- RIPA Explanatory Notes
  http://www.legislation.gov.uk/ukpga/2000/23/notes/contents

- RIPA statutory codes of practice

  – Covert Surveillance and Property Interference
  http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-covert
  – Covert Human Intelligence Sources
  http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-human-intel
  – Acquisition & Disclosure of Communications Data
  http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-acquisition

- SI 2000 No.2793 (The Regulation of Investigatory Powers (Juveniles) Order 2000
  http://www.legislation.gov.uk/uksi/2000/2793/made

- SI 2010 No.480 – Regulation of Investigatory Powers (Communications Data) Order 2010
  http://www.legislation.gov.uk/uksi/2010/480/contents/made

- SI 2010 N0.521 – Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010
  http://www.legislation.gov.uk/uksi/2010/9780111490365/contents

- SI 2010 No.461 (The Regulation of Investigatory Powers (Extension of Authorisation Provisions: Legal Consultations) Order 2010
  http://www.legislation.gov.uk/uksi/2010/461/contents/made

- SI 2012 No.1500 (The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012)
  http://www.legislation.gov.uk/uksi/1500/contents

6. HOME OFFICE POINT OF CONTACT

Further information is available on request from:

RIPA Team
Home Office
5th Floor Peel Building
2 Marsham Street
London SW1P 4DF
Email: commsdata@homeoffice.x.gsi.gov.uk

ANNEX A

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

Local authority investigator wants to use a RIPA technique (directed surveillance, CHIS (covert human intelligence source) or communications data).

Does investigator intend to use directed surveillance?

Yes

No

Is the local authority investigating an offence and does that offence attract a maximum custodial sentence of 6 month or more?

No

Yes

Is the offence being investigated either:
-Section 146/147/147A of the Licensing Act 2003, or
-Section 7 of the Children and Young Persons Act 1993.

No

Yes

Investigator may **not** use directed surveillance. The case should be investigated by other means. Continue to assess if threshold is met **if** further offences come to light as the case progresses.

- Complete RIPA authorisation/ notice form, and seek approval of authorising officer/designated person as per current arrangements.
- Complete application part of the judicial application/order form for JP.

Within Office Hours
Local authority investigator to contact Her Majesty's Courts & Tribunals Service (HMCTS) administration at the magistrates' court to arrange a hearing.

Attend court with:
- counter-signed RIPA authorisation/ or notice (for CD authorisations/ notices the signatures may be electronic signatures).
- the accompanying judicial application/order form.
- any other relevant reference or supporting material.

Outcome

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

This may be appropriate if the JP considers that an application is fundamentally flawed. The local authority must be given at least 2 business days in which to make representations before the authorisation is quashed. In these circumstances a local authority cannot use the technique and will need to seek fresh authorisation internally before reapplying.

Refuse to approve the grant or re-newal of an authorisation or notice.

The grant or renewal of the RIPA authorisation or notice will not take effect and the local authority may **not** use the covert technique. Local authority may wish to address, for example, a technical error and reapply.

Approve the grant or re-newal of an authorisation or notice.

Technique may be used in this case. Investigator to resubmit to the JP any renewal or authorisation for the use of a different technique in this case.

Outside usual office hours:

A JP may consider an authorisation out of hours in **exceptional** circumstances. If the authorisation is urgent and cannot be handled the next working day then you should:
- Phone the court's out of hours HMCTS legal staff contact. You will be asked about the basic facts and urgency of the authorisation. If the police are involved in the investigation you will need to address why they cannot make a RIPA authorisation.
- If urgency is agreed, then arrangements will be made for a suitable JP to consider the application. You will be told where to attend and give evidence.
- Attend hearing as directed with two copies of both the counter-signed RIPA authorisation form or notice and the accompanying judicial application/order form.

Obtain signed order and retain original RIPA authorisation/notice.
For CD authorisations or notices, local authority investigator to provide additional copy of judicial order to the SPoC.
If out of hours, a copy of the signed order to be provided to the court the next working day.

ANNEX B

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:.....

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:

ANNEX C

COMMUNICATIONS DATA (CD) RIPA AUTHORISATIONS OR NOTICES

Single Point of Contact (SPoC)

1. For CD requests, a Single Point of Contact (SPoC) undertakes the practical facilitation with the communications service provider (CSP) in order to obtain the CD requested. They will have received training specifically to facilitate lawful acquisition of CD and effective co-operation between the local authority and communications service providers.

2. Local authorities unable to call upon the services of an accredited SPoC should not undertake the acquisition of CD.

3. For CD requests the Home Office envisages that the local authority may also choose to authorise, under section 223 of the Local Government Act, their SPoC in order that they may appear in front of the JP. In cases where the type of CD or its retrieval is technically complex and the JP wants to satisfy him/herself that the CD sought meets the test, then the SPoC may be best placed to explain the technical aspects.

4. Following the hearing the SPoC may aquire the data. SPoCs must not acquire the data via a CSP or using automated systems until after the JP has signed the order approving the grant. The one month time limit will commence from the date of the JPs signature giving approval.

The National Anti Fraud Network (NAFN)

5. The National Anti-Fraud Network provides a SPoC service to local authorities, precluding each authority from the requirement to maintain their own trained staff and allowing NAFN to act as a source of expertise. Local authorities using the NAFN SPoC service will still be responsible for submitting any applications to the JP and a designated person in the local authority is still required to scrutinise and approve any applications. The accredited SPoCs at NAFN will examine the applications independently and provide advice to applicants and designated persons to ensure the local authority acts in an informed and lawful manner.

6. The local authority investigator (i.e. the applicant) will then submit the relevant judicial application/order form, the RIPA application (authorisation or notice) and any supporting material to the JP. As above, following a private hearing, the JP will complete the order section of the judicial application/order form, reflecting their decision. The local authority investigator will then upload a copy of this order to the NAFN SPOC.

7. The NAFN SPoC will then acquire the CD on behalf of the local authority in an efficient and effective manner.

Consequential Acquisition

8. Section 3.31 of the Code of Practice for the Acquisition and Disclosure of CD outlines that a designated person may, at the time of granting an authorisation or notice for service usage data, also authorise the consequential acquisition of specific subscriber information. The designated person may only do so to the extent where it is necessary and proportionate. The consequential acquisition may only be for subscriber data, not traffic data, which local authorities may not acquire nor service usage data. Where a SPoC has been authorised to engage in conduct to obtain details of a person to whom a service has been provided and concludes that data is held by a CSP from which it cannot be acquired directly, the SPoC may provide the CSP with details of the authorisation granted by the designated person in order to seek disclosure of the required data[14].

9. In cases where an authorisation or notice seeks to acquire consequential acquisition of specific subscriber information the JP will assess this as part of his/her consideration. The local authority investigator should be prepared to explain to the JP the reasoning behind the request for consequential acquisition and be able to show how it meets the necessity and proportionality tests.

10. In cases where consequential acquisition is approved, but where a notice is required (which must specify the name of the CSP to whom it is given, and be signed by the designated person), a further grant of a notice will be required. This is a new legal instrument and therefore will require further approval to the designated person and the JP, despite authority for the human rights interference having already been given.

14 Acquisition and Disclosure of Communications Data Code of Practice, Paragraph 3.30.

Home Office

ISBN: 978-1-78246-004-6

AGENDA ITEM NO. 11

Taunton Deane Borough Council

Corporate Governance Committee – 19 May 2014

Whistleblowing Policy

Report of the Strategic Finance Officer
(This matter is the responsibility of Executive Councillor Mrs Vivienne Stock-Williams)

1. Summary

1.1 This report includes the updated whistleblowing policy.

1.2 The Corporate Governance Committee is asked to approve the revised policy.

2. Background

2.1 Taunton Deane Borough Council has a Whistleblowing policy which is published on our website.

2.2 It was last updated in 2011 and is now due for a review.

3. Updated Policy

3.1 Following new legislation (The Enterprise and Regulatory Reform Act 2013) the policy needed to be revised to ensure it complied.

3.2 It is important that an up to date policy is maintained so that employees and members of the public know how to report any concerns and what protection they have. The main change from the previous policy is in the protection offered to a whistleblower. The previous legislation and policy stated that a person who raises a concern in **good faith** would be protected even if they were mistaken. This has changed so that any person raising a concern **where they reasonably believe that the disclosure they are making is in the public interest** even if they are mistaken will be protected.

3.3 The revised Whistleblowing policy is attached to this report.

4. Finance Comments

4.1 There are no financial implications of this report.

5. Legal Comments

5.1 The Whistleblowing policy is an important part of the authority's governance arrangements and thus need to be regularly reviewed to ensure they comply with all current legislation. The legal framework for Whistleblowing is contained within the Public Interest Disclosure Act 1998 as revised by the Enterprise and Regulatory Reform Act 2013.

.

6. Links to Corporate Aims

6.1 There are no Corporate Aim implications of this report.

7. Environmental and Community Safety Implications

7.1 There are no environmental and community safety implications of this report.

8. Equalities Impact

8.1 There are no equality impacts of this report.

9. Risk Management

9.1 Having a Whistleblowing policy reduces the risk that employees and members of the public do not feel able to raise concerns about the council.

10. Partnership Implications

10.1 The South West Audit Partnership is a contact point for members of the public to raise concerns. They have a confidential e-mail address and a telephone number for the public to use to report concerns.

11. Recommendations

11.1 That the Corporate Governance Committee approves the updated Whistleblowing policy.

Contact: Maggie Hammond
01823 358698
m.hammond@tauntondeane.gov.uk

Policy and Procedure for confidential reporting of concerns ("Whistleblowing")

Don't turn a blind eye
Stay calm
Know you are protected
Remember and note key details
Do not investigate the issue yourself
Follow the Council's Whistleblowing policy

Index

Revised date **May 2014**

Review date **May 2016**

1. Introduction to raising a concern with the Council

Taunton Deane Borough Council is committed to the highest possible standards of openness and accountability. In line with that commitment **we expect both employees and members of the public**, **who have serious concerns about any aspect of the Council's work to come forward and voice their concerns.**

Whether you are an employee or a member of the public, you might be the first to realise that there may be something seriously wrong within the Council.

This policy is intended to encourage and enable employees and members of the public to raise concerns within the Council rather than overlooking a problem.

This policy also explains how you can raise a concern without fear of victimisation, subsequent discrimination or disadvantage.

Who can use this policy?

- All members of the public
- All Employees (including Contractors, Agency and Temporary staff)
- External Contractors
- Suppliers
- Service providers

What is included in the policy?

There are existing procedures in place to enable staff to lodge a grievance relating to their own employment. This policy is intended to cover concerns that fall outside the scope of the grievance procedure. Thus any serious concern that a member of staff or a member of the public has about any aspect of service provision or the conduct of officers or members of the Council or others acting on behalf of the Council can and should be reported under this policy.

This concern may be about something that is:

- unlawful
- against the Council's Standing Orders, Financial Procedure Rules and policies
- against established standards of practice
- improper conduct
- amounts to malpractice
- posing a danger to the health and safety of individuals
- likely to cause damage to the environment
- other conduct that gives you cause for concern

Please note that this is not a comprehensive list but is intended to illustrate the range of issues which might be raised under this Code.

2. Safeguards

Harassment or Victimisation

The Council recognises that the decision to report a concern can be a difficult one to make, not least because of the fear of reprisals from those who may be guilty of malpractice or from the Council as a whole. The Council will not tolerate any harassment or victimisation (including informal pressures) and will take appropriate action in order to protect a person who raises a concern where they reasonably believe that the disclosure they are making is in public interest, even if they were mistaken. In addition employees have statutory protection against reprisals under the Public Interest Disclosure Act 1998 as revised by the Enterprise and Regulatory Reform Act 2013 and can refer their case to an Industrial Tribunal.

Confidentiality

As far as possible, the Council will protect the identity of any employee or member of the public who raises a concern and does not want his/her name to be disclosed but this confidentiality cannot be guaranteed. It must be appreciated that any investigation process may reveal the source of the information and a statement by the person reporting the concern may be required as part of the evidence. Where an employee or member of the public has requested that their identity not be revealed, the Council will discuss the matter with them before embarking on any course of action whereby their identity will need to be disclosed.

Anonymity

Concerns expressed anonymously will be considered at the discretion of the Council although it must be appreciated that it is inherently difficult to investigate concerns expressed this way. It is hoped that the guarantees contained in this policy will provide sufficient reassurance to staff to enable them to raise concerns in person. However in exercising the discretion, the factors to be taken into account would include:

- The likelihood of obtaining the necessary information;
- The seriousness of the issues raised;
- The specific nature of the complaint;
- The duty to the public.

False and Malicious Allegations

The Council will not tolerate the making of malicious or vexatious allegations. Acts of this nature will be treated as serious disciplinary offences. Disciplinary action, including summary dismissal for serious offences, will be taken against any employee found to have made malicious or vexatious claims.

In line with the TDBC Complaints Procedure examples of vexatious allegations are persistently complaining about a variety or number of different issues; persistently making the same complaint but not accepting the findings of any properly conducted investigation and/or seeking an unrealistic outcome.

In addition, a concern, which is genuinely believed, may prove to be unfounded on investigation – in which case no action will be taken against the person who raised the concern.

The Council will try to ensure that the negative impact of either a malicious or unfounded allegation about any person is minimised.

3. How to raise a concern

If you are a member of the Public

You can raise your concern(s) with any of the following officers;

- Section 151 Officer – Shirlene Adam (s.adam@tauntondeane.gov.uk)
- Human Resources Manager – Martin Griffin (m.griffin@tauntondeane.gov.uk)
- Monitoring Officer – Bruce Lang (bdlang@westsomerset.gov.uk)
- Director of Quality – Ian Baker (ian.baker@southwestaudit.co.uk)

The Council has set up an arrangement for a confidential answer phone service with the **South West Audit Partnership** (01935 462381).

You can also email them at; confidential@southwestaudit.co.uk

If you are an employee of the Council

You should normally raise your concern(s) with your immediate manager or their superior. This depends, however, on the seriousness and sensitivity of the issues involved and who is thought to be involved in the malpractice. If you prefer (for whatever reason) or if you believe that management is involved, you can contact one of the individuals listed above;

The Council has set up an arrangement for a confidential answer phone service with the **South West Audit Partnership** (01935 462381).

You can also email them at; confidential@southwestaudit.co.uk

Alternatively you can get confidential advice from your trade union or professional association. There is an independent charity called **Public Concern at Work (020 7404 6609) www.pcaw.co.uk** who have lawyers who can give independent advice at any stage about how to raise a concern about serious malpractice at work.

You can also invite your **trade union or professional association** to raise a matter on your behalf.

Members of the Public and Employees

Concerns can either be raised orally or in writing. Normally it is preferable to put your concern in writing.

What you need to include

It would be helpful to us if you could provide the following information

- **background**
- **the history**
- **reason for your concern**
- **names**
- **dates**
- **places**

See **Appendix A** Flowchart on 'How to Raise a Concern'

4. How the Council will respond

The action taken by the Council will depend on the nature of the concern. Where appropriate, the concern(s) raised will be;

- investigated by senior management, internal audit (SWAP) or through the disciplinary process;
- referred to the police;
- form the subject of an independent inquiry.

In order to protect the individual and the Council, an initial investigation will be carried out to decide whether a full investigation is appropriate and, if so, what form it should take. This investigation will be carried out by the most appropriate office. Concerns or allegations which fall within

the scope of specific procedures (for example fraud, theft and corruption) will normally be referred for consideration under those procedures.

It should be noted that some concerns may be resolved by agreed action without the need for investigation. If urgent action is required, this would be taken before any investigation is completed.

Within ten working days of a concern being raised, the Director of Quality will write to you;

- acknowledging that the concern; has been received,
- indicating how he/she proposes to deal with the matter; and
- giving an estimate of how long it will take to provide a final response.

If it is impossible for initial inquiries to be completed within ten working days, the situation will be explained in the letter of acknowledgement. Where a decision is made that no investigation will take place, the reasons for this will be provided.

The amount of contact between the officers considering the issues and you raising the concern will depend on the nature of the matters raised, the potential difficulties involved and the clarity of the information provided. If necessary, further information may be sought from the person raising the concern.

Where any meeting is arranged, you have the right, if you so wish, to be accompanied by a union or professional association representative, relative or a friend who is not involved in the area of work to which the concern relates.

The Council will take appropriate steps to minimise any difficulties, which you may experience as a result of raising a concern. For example, if as an employee you are required to give evidence in criminal or disciplinary proceedings, the Council will need to inform them and consider what steps are required to provide support.

The Council accepts that by raising a concern, you will need to be assured that the matter has been properly addressed. Thus, subject to legal constraints, you will receive as much information as possible about the outcomes of any investigation.

See **Appendix B** for flowchart on ‘How the Council will respond’

5. How the Concern can be taken further

This policy is intended to provide you with an avenue to raise concerns within the Council. The Council hopes you will be satisfied with any action taken. If you are not satisfied with the outcome of your confidential allegation you can write to the Chief Executive and ask for

the investigation and outcome to be reviewed. If you remain dissatisfied and you feel it is right to take the matter outside the Council, you may wish to take advice from your trade union, your local Citizens Advice Bureau, any of the external agencies listed in Appendix A, or your legal advisor on the options that are available to you.

Another option is that you may wish to rely on your rights under the Public Interest Disclosure Act 1998. This Act gives you protection from victimisation if you make certain disclosures of information in the public interest. The provisions are quite complex and include a list of prescribed persons outside of the Council who can be contacted in certain circumstances. You should seek advice on the effect of the Act from the Monitoring Officer.

If you do take the matter outside the Council, you need to ensure that you do not disclose information where you owe a duty of confidentiality to persons other than the Council (e.g. service users) or where you would commit an offence by making such disclosures. This is something that you would need to check with one of the officers mentioned in Section 3.

6. The Role of the Monitoring Officer

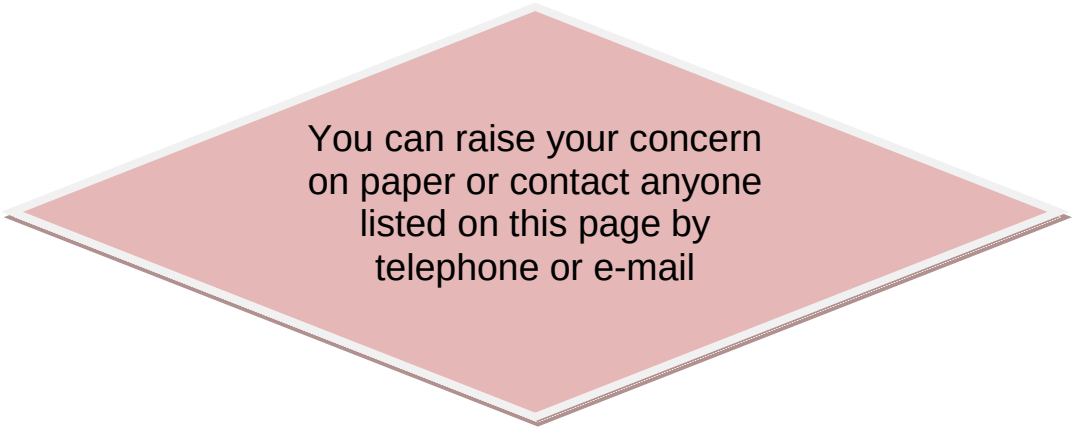
The Monitoring Officer is responsible for ensuring that the Council adheres to this Policy and the officer's contact details are documented in this policy should you have any concerns with it. The Monitoring Officer is also responsible for reporting to the Council on any findings of improper or unlawful conduct following an investigation.

7. Review of policy

This Policy will be regularly reviewed in line with future changes and developments and at least every two years. Next Review date planned: 1st May 2016.

APPENDIX A

How to raise your concern



Contact one of the following external contacts for support and advice:

Public Concern at Work (www.pcaw.co.uk tel 020 7404 6609)

The Audit Commission (www.audit-commission.gov.uk)

The Health & Safety Executive (www.hse.gov.uk)

Environment Agency (www.environment-agency.gov.uk)

Relevant professional bodies or regulatory organisations

A solicitor or legal advisor

The Police

The Local Government Ombudsmand

A trade Union

If you are an employee you can raise your concern with your immediate manager, or your manager's manager

You can arrange to have an informal conversation or raise your concern with the following contacts if you prefer:

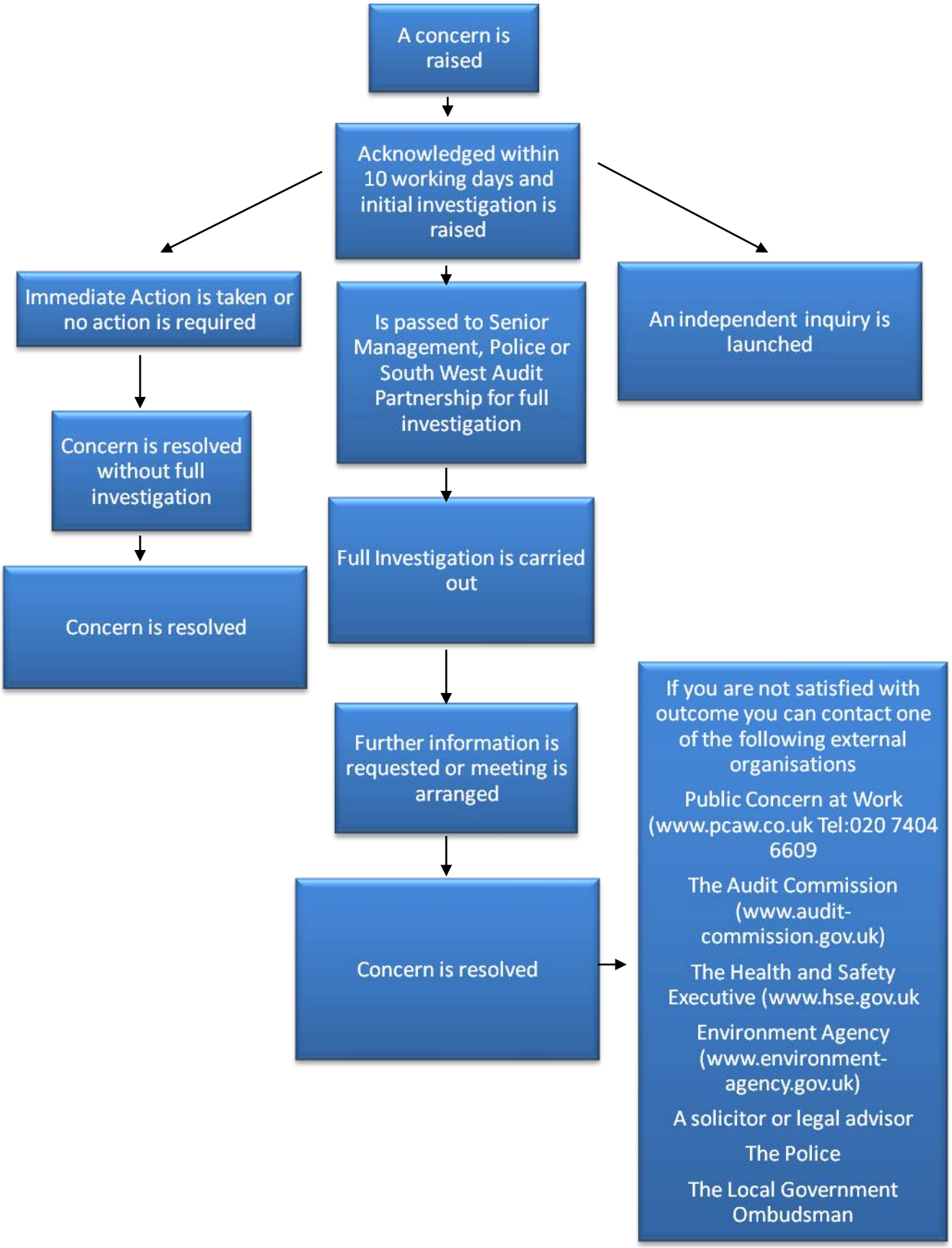
The Section 151 Officer

HR Manager – Martin Griffin

Monitoring Officer – Bruce Lang

Audit Manager – Alastair Woodland

APPENDIX B


A concern is raised
Acknowledged within 10 working days and initial investigation is raised
Immediate Action is taken or no action is required
Is passed to Senior Management, Police or South West Audit Partnership for full investigation
An independent inquiry is launched
Concern is resolved without full investigation
Concern is resolved
Full Investigation is carried out
Further information is requested or meeting is arranged
Concern is resolved
If you are not satisfied with outcome you can contact one of the following external organisations
Public Concern at Work (www.pcaw.co.uk Tel:020 7404 6609
The Audit Commission (www.audit-commission.gov.uk)
The Health and Safety Executive (www.hse.gov.uk
Environment Agency (www.environment-agency.gov.uk)
A solicitor or legal advisor
The Police
The Local Government Ombudsman

AGENDA ITEM NO. 12

Taunton Deane Borough Council

Corporate Governance Committee – 19 May 2014

Money Laundering Policy

Report of the Strategic Finance Officer
(This matter is the responsibility of Executive Councillor Vivienne Stock-Williams)

1. Executive Summary

- Money laundering is any attempt to use the proceeds of crime for legitimate purposes. The Council and its individual Members and employees have obligations under the Terrorism Act 2000 and certain sections of the Proceeds of Crime Act 2002 relating to money laundering. Public authorities are not legally obliged to implement the provisions of the Money Laundering Regulations 2007, but as a responsible public body, the Council should have a policy and procedures designed to reflect the essence of the UK's antiterrorist financing and anti money laundering regimes.

- The proposed policy ensures that the Council has appropriate and proportionate measures in place to comply with the legal requirements, to implement relevant regulatory provisions and to protect its staff and Members.

2. Background

2.1 Money laundering is any attempt to use the proceeds of crime for legitimate purposes and is generally defined as the process by which the proceeds of crime, and the true ownership of those proceeds, are changed so that the proceeds appear to come from a legitimate source. Anyone who becomes aware of an activity which they have reasonable grounds to suspect, is related to the proceeds of crime may be guilty of a money laundering offence.

2.2 The legal and regulatory framework for the UK's anti-terrorist financing and anti money laundering arrangements comprises:

- The Terrorism Act 2000 (TA);
- The Proceeds of Crime Act 2002 (POCA); and
- The Money Laundering Regulations 2007 (MLR).

2.3 The Chartered Institute of Public Finance and Accountancy (CIPFA) has published guidance on how the provisions of this framework apply to public authorities (CIPFA, 2009). The Policy accompanying this report is designed to ensure that the Council and its staff fulfil all legal obligations and regulatory requirements in accordance with this guidance.

2.4 The Council is not legally obliged to apply the provisions of the MLR because public authorities are neither 'relevant persons' (as defined in the MLR) nor part of the 'regulated sector' (as defined in POCA 2002). However, as a prudent and responsible public body, the Council's policy and procedures should be designed to reflect the essence of the UK's anti-terrorist financing and anti money laundering regimes.

3. Money Laundering Policy

3.1 Although the Council's risk of exposure to money laundering is relatively low and some of the provisions of the legal and regulatory framework do not apply, there is, as CIPFA observes, a reputational risk for any authority that does not have adequate policies and procedures in place. CIPFA's view is that, "it is prudent and responsible practice for public service organisations, including those outside the scope of the regulations, to put in place appropriate and proportionate anti-money laundering safeguards and reporting arrangements, designed to enable them to detect and avoid involvement in the crimes described in the legislation and regulations."

3.2 The risk is not only reputational. There is also a risk that individuals who, in the course of Council business, become aware that criminal property or funds could be involved may commit offences under the TA or POCA sections 327-329 if a reasonable suspicion is not reported.

3.3 It is therefore important that appropriate and proportionate arrangements are established to ensure that the Council, its staff and Members are protected as far as practicable, notably by having in place a reporting mechanism, arrangements for publicising the responsibilities of individuals and provisions for appropriate training and education.

3.4 The policy needs to be clear, succinct and practical to ensure maximum accessibility to staff and Members.

3.5 This Policy applies to all employees of the Council and aims to maintain the high standards of conduct which currently exist within the Council by preventing criminal

activity through money laundering. The Policy sets out the procedures which must be followed (for example, the reporting of suspicions of money laundering activity) to enable the Council to comply with its legal obligations.

3.6 The policy and staff guide are attached to this report.

4. Finance Comments

4.1 There are no financial implications of this policy

5. Legal Comments

5.1 Even though Taunton Deane Borough Council is not a “relevant person” or part of the regulated sector it is good practice to have a clear Money Laundering Policy and also to ensure that employees are aware of this policy.

6. Links to Corporate Aims

6.1 There are no links to specific corporate aims of this policy.

7. Environmental Implications

7.1 There are no environmental implications of this report

8. Community Safety Implications

8.1 There are no community safety implications of this report

9. Equalities Impact

9.1 All Acts and guidance are applicable equally to all and no one protected group is adversely impacted by this policy.

10. Risk Management

10.1 The risk of exposure to money laundering is relatively low.

11. Partnership Implications

11.1 Cash payments are processed by Southwest One. Southwest One will be made aware of our policy on money laundering .

12. Recommendations

12.1 That Corporate Governance Committee approves the Money Laundering policy.

Contact: Maggie Hammond
(01823) 358698
m.hammond@tauntondeane.gov.uk

TAUNTON DEANE BOROUGH COUNCIL
ANTI-MONEY LAUNDERING POLICY

1. INTRODUCTION

1.1 Money laundering can be defines as “a process that makes money with an illegal origin appear legal so that it may be used.”

1.2 There have been significant changes to the legislation concerning money laundering (the Proceeds of Crime Act 2002, the Money Laundering Regulations 2003/2007 and the Terrorism Acts 2000 and 2006), which have broadened the definition of money laundering and increased the range of activities caught by the statutory framework. It is prudent and responsible practice for all public service organisations to put in place appropriate and proportionate anti-money laundering safeguards and reporting arrangements, designed to enable them to detect and avoid involvement in money-laundering related crimes.

2. SCOPE OF THE POLICY

2.1 This policy applies to all employees of the Council and aims to maintain the high standards of conduct which currently exist within the Council by preventing criminal activity through money laundering. The Policy sets out the procedures which must be followed (for example the reporting of suspicions of money laundering activity) to enable the Council to comply with its legal obligations. Within this policy the term employee refers to all employees as well as elected Members.

2.2 Anti money laundering legislation places responsibility upon Council employees to combat money laundering and covers a very wide area of financial transactions, including possessing, or in any way dealing with, or concealing the proceeds of any crime. It applies to all employees involved with monetary transactions.
.

2.3 Under the legislation it is a criminal offence to:

- Assist a money launderer:
- ***Inform*** a person suspected to be involved in money laundering that they are suspected or that they are the subject of police investigations;
- ***Fail to report a suspicion of money laundering and;***
- Acquire, use or possess criminal property

3. PURPOSE

3.1 The legislative requirements concerning anti-money laundering procedures are extensive and complex. This Policy has been written to enable the Council to meet the legal requirements in a way that is proportionate to the risk to the Council of contravening this legislation.

3.2 The object of this policy is to make all employees aware of their responsibilities and the consequences of non-compliance with this policy.

3.3 An employee could potentially be caught within the money laundering provisions of they suspect money laundering and either become involved with it in some way and/or do nothing about it.

3.4 Whilst the risk to the Council of contravening the legislation is relatively low, it is extremely important that all employees are familiar with their legal responsibilities
Employees contravening the regulations can be faced with imprisonment (up to 14 years), a fine or both.

4. MONEY LAUNDERING REQUIREMENT, FROM THIS COUNCIL'S POINT OF VIEW

4.1 Provision of training to relevant officers and staff (or contractors' staff) on the requirements of the legislation, including the identification of suspicions transactions, identity verification and reporting procedures.

4.2 Establishment of procedures for employees to report any suspicions to the Money Laundering Officer ("MLRO").

4.3 Designation of an officer as the Money Laundering Reporting Officer, who will receive any report, keep records and if considered appropriate, make reports to the National Crime Agency (who have replaced the Serious and Organised Crime Agency)

5. PROCEEDURES

When do I need to identify the person I am dealing with?

When the Council is carrying out relevant business and: -

a) Forming a business relationship: or

b) Considering undertaking a one off transaction

And: -

a) Suspect a transaction involves money laundering: -

b) A payment is to be made for a series of linked one off transactions involving total payment of £10,000

Not all the Council's business is "relevant" for the purposes of the legislation regarding client identification. Relevant services as defined by the legislation

include investments, accountancy and audit services and the financial, company and property transactions undertaken by the council.

What Procedures do I use to identify the person?

5.1 Any employee involved in a relevant business should ensure the client provides satisfactory evidence of their identity personally, through passport/photo driving licences plus one other document with their name and address e.g utility bill (not mobile) mortgage/building society/bank documents, card documents, pension/benefit book. Or corporate identity, this can be through company formation documents or business rates.

5.2 In circumstances where the client cannot be physically identified the employee should be aware: -.

a) That there is greater potential for money laundering where the client is not physically present when being identified;

b) If satisfactory evidence is not obtained the relationship or transaction should not proceed;

c) If the client acts, or appears to act for another person, reasonable measures must be taken for the purpose of identifying that person.

6 RECORD KEEPING PROCEDURES

6.1 Each Service of the Council and contractors working for the Council conducting relevant business must maintain records of:-

a) Client identification evidence obtained; which must be kept for five years.

b) Details of all relevant business transactions carried out for clients for at least five years from completion of the transaction. This is so that they can be used as evidence in any subsequent investigation by the authorities into money laundering. The AD Resources must be informed of the existence and location of such records.

6.2 The precise nature of the records are not prescribed by law, however, they must provide an audit trail during any subsequent investigation, e.g. distinguishing the client and the relevant transaction and recording in what form any funds were received or paid.

7. THE MONEY LAUNDERING REPORTING OFFICER

7.1 The Officer nominated to receive disclosures about money laundering activity within the Council is the Assistant Director Resources. i.e. The Money Laundering Officer (MLRO).

7.2 The Deputy Money Laundering Reporting Officer is the Finance Manager

8. INTERNAL REPORTING PROCEDURE

8.1 Where an employee is aware that money laundering may have taken place (or may be taking place), he or she must contact the MLRO for guidance as soon as possible regardless of the amount being offered. In such circumstances, no money may be taken from anyone until this has been done.

8.2 Any person knowing or suspecting money laundering, fraud or use of the proceeds of crime must report this to the MLRO on the form(s) attached.

8.3 Upon receiving the report the MLRO will consider all of the admissible information in order to determine whether there are grounds to suspect money laundering.

8.4 If the MLRO determines that the information or matter should be disclosed it would be reported to the National Crime Agency (who have replaced the Serious and Organised Crime Agency).

8.5 At no time and under no circumstances should an employee voice any suspicions to the person(s) suspected of money laundering even if the National Crime Agency has given consent to a particular transaction proceeding, otherwise the employee may be committing a criminal offence of ***informing***. Therefore, no reference should be made on a client file to a report having been made to the MLRO. Should the client exercise their right to see the file, then such a note will obviously tip them off to the report having been made and may render the employee liable to prosecution. The MLRO will keep the appropriate records in a confidential manner.

9 OTHER PROCEDURES

9.1 The Council will establish other procedures of internal control and communication as may be appropriate for the purpose of forestalling and preventing money laundering:-

9.2 **Regular receipts-** The Council in the normal operation of its services accepts payments form individuals and organisations e.g. in relation to council tax, rent, sundry debtors etc. For all transactions under £2,000

the Money Laundering regulations do not apply but if an employee has reasonable grounds to suspect money laundering activities or proceeds of crime or is simply suspicious, the matter should still be reported to the MLRO.

9.3 **Cash receipts-** if the money offered in cash is £10,000 or more, then payment must not be accepted until the employee has received guidance from the MLRO or Finance Manager.

9.4 **Refunds-** Care will need to be taken especially with the procedures for refunds. For instance, a significant overpayment that results in a repayment will need to be properly investigated and authorised before payment. **Note – all refunds should be made only to the source of the payment and not a different account.** In the event of ant suspicious transactions, the MLRO will be contacted to investigate the case. The possible perpetrator should not be informed.

9.5 **Training-** The Council will take, or require its contractor to take appropriate measures to ensure that relevant employees are:

a) Made aware of the provisions of these regulations, (under the Proceeds of Crime Act 2002, and the Money Laundering Regulations 2003):
b) Given training in how to recognise and deal with transactions that may be related to money laundering

10 GLOSSARY OF TERMS

AML	Anti money laundering
MLRO	Money Laundering Reporting Officer as defined in the Money Laundering Regulations 2003 and the FSA (Financial Services Act)

11 MONEY LAUNDERING WARNING SIGNS

11.1 The following examples could indicate that money laundering is taking place:

- Transactions or trade that appear to make no commercial or economic sense from the perspective of the other party – a money launderer's objective is to disguise the origin of criminal funds and not necessarily to make a profit. A launderer may therefore enter into transactions at a financial loss if it will assist in disguising the source of the funds and allow the funds to enter the financial system.

- Large volume/large cash transactions – all large cash payments should be the subject of extra care and before accepting cash the reasons for such payments should be fully understood. Payments should be encouraged through the banking system to avoid problems.

- Payments received from third parties – money launderers will often look to legitimate business activity in order to assist in ‘cleaning’ criminal funds and making payments on behalf of a legitimate company can be attractive to both parties. For the legitimate company it can be useful source of funding and for the launderer the funds can be repaid though a banking system.

11.2 Examples of tell tale signs of organised money laundering:

1. Use of cash where other means of payment are normal
2. Unusual transactions or ways of conducting business
3. Unwillingness to answer questions/secretiveness generally
4. Use of overseas companies
5. New companies
6. Overpayment of Council Tax where refunds are needed

Disclosure Form to MLRO

Please complete and return to the Assistant Director Resources

Date of disclosure:

Date of event:

Officer making disclosure:

Job title of officer:

Telephone details:

SUBJECT DETAILS

Title:

Surname:

Forename:

DoB:

IN THE CASE OF A LEGAL ENTITY (COMPANY)

Name:

Address:

Company Number (if known):

Type of Business:

VAT no (if known):

REASON FOR DISCLOSURE

Please provide an explanation of the activity and amounts. If you know or suspect what the offence behind the reported activity may be please provide details.

RECEIVED BY MLRO

Reference:

Date:

Signature:

AGENDA ITEM NO. 13

Taunton Deane Borough Council

Corporate Governance Committee – 19 May 2014

Update on Internal Audit Plan 2013/14 actions from Corporate Governance Meeting 10 Mar 2014

Report of the Assistant Director Corporate Services and Strategic Finance Officer
(This matter is the responsibility of Executive Councillor Stock-Williams)

1. Summary

1.1 This report provides Corporate Governance Committee with an update on issues raised at the meeting of 10th March 2014 in relation to Procurement Cards audit and the delay in progressing various ICT audits.

2. Background

2.1 At its meeting on 10th March 2014 the Corporate Governance Committee considered the Internal Audit Plan 2013/14 – Progress Report. This report updated the committee on any audits undertaken by SWAP since the previous report where only a partial assurance opinion had been given.

2.2 There was only one audit that had received a partial assurance which was the Procurement Cards audit. A number of management actions have been agreed by the Strategic Finance Officer with SWAP to rectify the issues identified.

2.3 Alastair Woodland from SWAP also outlined to the committee concerns around delays in being able to progress various ICT related audits. The Assistant Director – Corporate Services, Richard Sealy, explained that these concerns were being raised with the ICT service.

2.4 Members requested on 10th March 2014 'a progress update on the partial audit of procurement cards as well as an update of the ICT audit progress'.

3. Update on Procurement Cards

3.1 The procurement card audit had six recommendations that have been agreed by the Strategic Finance Officer. Five of which were due to be completed by 31st March 2014

3.2 Due to work load the Strategic Finance Officer missed the 31st March deadline. .

3.3 A policy has been written and agreed by the assistant Director Finance. This was shared with all the holders of Procurement Cards on 28th April 2014. Procurement Card holders have been asked to confirm that they have read the policy and understand their responsibility as a Procurement Card holder.

3.4 At the point of writing this report 9 of the 12 Procurement Card holders have signed the acceptance form.

4 SWAP ICT Audits

4.1 Alastair Woodland from SWAP reported delays in SWAP being able to progress ICT audits at the Corporate Governance meeting on 10 March 2014. Specifically these delays resulted from the auditors not being provided with the appropriate access to the SAP system, which is required in order for them to undertake the audit.

4.2 The issues have now been resolved and satisfactory progress is being made on the audits in question. The specific audit affected are the Data Centre Facilities Management; System Development Life Cycle and IT Financial Controls. Data Centre Facilities Management is now finalised, System Development Life Cycle will be finalised by the 16th May 2014 and SAP IT Financial Controls will be by the 20th June 2014.

5. Finance Comments

5.1 The correct use of Procurement Cards enables TDBC to reduce costs and secure efficiencies in dealing with low value ad hoc purchases. The policy will ensure that Procurement Card holders understand their responsibilities.

6. Legal Comments

6.1 There are no legal implications of this report.

7. Links to Corporate Aims

7.1 There are no direct links to the Corporate Aims.

8. Environmental and Community Safety Implications

8.1 There are no environmental and community safety implications of this report.

9. Equalities Impact

9.1 There are no equality impacts of this report.

10. Risk Management

10.1 Staff who hold Procurement cards have now been advised in writing of their responsibilities and also security measures that they should take, helping to reduce the risk of fraud.

11. Partnership Implications

11.1 There are no partnership implications of this report.

12. Recommendations

12.1 Corporate Governance Committee are asked to note the progress on both the Procurement Card Audit Recommendation and the ICT Audits.

Contact: SAP Access update
Richard Sealy
01823 356310
r.sealy@tauntondeane.gov.uk

Procurement Card Policy update
Maggie Hammond
01823 358698
m.hammond@tauntondeane.gov.uk

19/05/2014, Report:Whistleblowing Policy Refresh
Reporting Officers:Maggie Hammond

19/05/2014, Report:Money Laundering Policy Refresh
Reporting Officers:Maggie Hammond

19/05/2014, Report:External Audit - Fees Report 14/15
Reporting Officers:Richard Sealy

19/05/2014, Report:External Audit Plan 2013/14
Reporting Officers:Peter Lappin

19/05/2014, Report:Regulation of Investigatory Powers Act (RIPA) - Policy and Porcedures Update
Reporting Officers:Richard Bryant

19/05/2014, Report:Update on Internal Audit Plan 2013/14 actions from Corporate Governance Meeting 10 March 2014
Reporting Officers:Maggie Hammond,Richard Sealy

23/06/2014, Report:Health and Safety Update Report
Reporting Officers:Catrin Brown

23/06/2014, Report:Draft Annual Governance Statement 2012/13
Reporting Officers:Dan Webb

23/06/2014, Report:Corporate Governance Action Plan
Reporting Officers:Dan Webb

23/06/2014, Report:Annual Report of SWAP
Reporting Officers:Alastair Woodland

23/06/2014, Report:Internal Audit - Review of Effectiveness
Reporting Officers:Shirlene Adam

23/06/2014, Report:Overview of Technical Changes to Statement of Accounts 13/14
Reporting Officers:Peter Barber,Paul Fitzgerald

23/06/2014, Report:Verbal Update on Approach to Corporate Fraud
Reporting Officers:Paul Fitzgerald

22/09/2014, Report:HRA Self-Financing Code Self Assessment Outcome
Reporting Officers:James Barrah

22/09/2014, Report:Pensions Deficit Presentation
Reporting Officers:Anton Sweet

22/09/2014, Report:Health and Safety Update Report
Reporting Officers:Catrin Brown

22/09/2014, Report:Grant Thornton - Financial Resilience
Reporting Officers:Peter Barber

22/09/2014, Report:Grant Thornton - Audit Findings
Reporting Officers:Peter Barber

22/09/2014, Report:Grant Thornton - Certification Plan
Reporting Officers:Peter Barber

22/09/2014, Report:Approval of Statement of Accounts 2013/14
Reporting Officers:Paul Fitzgerald

22/09/2014, Report:Internal Audit Plan 14/15 - Progress Report
Reporting Officers:Alastair Woodland

22/09/2014, Report:Update on Approach to Corporate Fraud
Reporting Officers:Paul Fitzgerald

08/12/2014, Report:Health and Safety Update Report
Reporting Officers:Catrin Brown

08/12/2014, Report:Grant Thornton - Annual Audit Letter 2012/13
Reporting Officers:Peter Barber

08/12/2014, Report:Grant Thornton - External Audit Update
Reporting Officers:Peter Barber

08/12/2014, Report:Internal Audit Plan - Progress Report
Reporting Officers:Alastair Woodland

08/12/2014, Report:Corporate Governance Action Plan Update
Reporting Officers:Dan Webb

Corporate Governance Committee – 19 May 2014

Present:

Councillors Allgrove, Beaven, Coles, Denington, Gaines, Hall, Hunt, S Lees, D Reed, Mrs Stock-Williams, Miss Smith, Tooze, D Wedderkopp and A Wedderkopp.

Officers: Richard Sealy (Assistant Director Corporate Services), Bruce Lang (Assistant Chief Executive and Monitoring Officer), Maggie Hammond (Strategic Finance Officer), Shirlene Adam (Director of Operations) and Emma Hill (Corporate Support Officer).

Also Present: Ashley Allen (Audit Manager, Grant Thornton)
Peter Barber (Appointed Auditor, Grant Thornton)

(The meeting commenced at 6.15 pm)

14. Appointment of Chairman

Resolved that Councillor D Reed be appointed Chairman of the Corporate Governance Committee for the remainder of the Municipal Year.

15. Appointment of Vice-Chairman

Resolved that Councillor Coles be appointed Vice-Chairman of the Corporate Governance Committee for the remainder of the Municipal Year.

16. Apologies/Substitutions

Apologies: Councillors A Govier, Horsley, R Lees and Mrs Waymouth.
Substitutions: Councillor Miss F Smith for Councillor Horsley
Councillor S Lees for Councillor R Lees
Councillor Allgrove for Councillor Mrs Waymouth

17. Minutes

The minutes of the meeting held on 10 March 2014 were taken as read and were signed.

18. Declaration of Interests

Councillors Coles, Hunt, D Wedderkopp and A Wedderkopp declared personal interests as Members of Somerset County Council. Councillor Tooze declared a personal interest as an employee of UK Hydrographic Office.

19. External Audit Plan 2013/2014

Considered report previously circulated, which introduced the External Audit Plan for 2013/2014.

Each year the Council's external auditors, Grant Thornton, provided a plan which detailed their approach to the audit work required in respect of the preceding

financial year (2013/2014). Specifically this audit work focussed on the provision of an audit opinion in relation to the accounts, value for money (VFM) and associated key risks.

During the discussion of this item, Members made comments and statements and asked questions which included:- (Responses are shown in italics)

- Concerns were raised over the cost of the service to the Council. What was the percentage of work / cost?
  Currently about 15% of work had been completed but the majority of the remaining work would be completed by late June.
- Why the level of detail and cost?
  As a public body with public money, the Council needed to be seen to be transparent. The Council was a £70 million body and the cost of the audit to the Council was 0.01% of our revenue.
- How much would Grant Thornton have to do with the West Somerset audit in connection with the current shared services project?
  This would be looked into as part of the projected savings related to sharing of services with West Somerset.

Resolved that the report be noted.

20. External Audit Update

Considered report previously circulated, which provided a progress update from the Council's external auditors, Grant Thornton, in respect of the 2013/2014 audit work for Taunton Deane and on emerging national issues, which might be relevant to the Council.

Each year Grant Thornton were required to carry out "set" audit work and the report provided a useful progress update in relation to that work.

Additionally, the report shared the headlines on emerging national issues and developments, which might have a bearing on the Council. Specifically the 2013/2014 Code for valuing property and assets and changes to the Local Government Pension Scheme were highlighted.

During the discussion of this item, Members made comments and statements and asked questions which included:- (Responses are shown in italics)

- Was the Council on track to meet the deadline of 30 June 2014? *Yes.*
- Was Taunton Deane amongst those with concerns over assets and accounts?
  Grant Thornton was working with the Director of Operations on procedures as to the presenting of the draft accounts as well as looking at the Council's principles.

Resolved that the report be noted.

21. External Audit – Fees Report

Considered report previously circulated, on the fee position for external audit services for 2014/2015.

The external audit function for Taunton Deane transferred from the Audit Commission to Grant Thornton during 2012. This change was part of a national programme of "outsourcing" the external audit work and had resulted in significant savings for local authorities.

The letter also set out details of the process and timetable for completing the external audit work for 2014/2015 together with details of the team who would lead the work. However, since receiving the letter the Council had been notified of a change to the team – Peter Lappin would be replaced by Ashley Allen as Engagement Manager.

Any additional audit work, outside of the planned audit and grant fee work, would be billed separately and in addition to the fee quoted.

The indicative audit fee for 2014/2015 was £76,955. This was split between the fee for the main audit of £66,605 (which remained the same as the previous year) and the grant certification work of £10,350 (which represented a reduction of £7,210 from the previous year).

The fee was within the Council's budget allocation for 2014/2015.

Resolved that the Grant Thornton report be noted.

22. Regulation of Investigatory Powers Act (RIPA) – Policy and Procedure Update

Considered report previously circulated, concerning the Policy amendments made to the Regulation of Investigatory Powers Act 2000 (RIPA) by The Protection of Freedoms Act 2012.

The Council had had a corporate policy dealing with the Regulation of Investigatory Powers Act 2000 since July 2008.

The Policy detailed various aspects of the legislation and guided officers and the relevant processes and procedures that needed to be followed. In addition, it also set out details of the relevant authorising officers for the Council.

The Protection of Freedoms Act had made amendments to RIPA to provide that following authorisation to use the Act, no surveillance could be conducted until that authorisation had been approved by a Justice of the Peace. Therefore the Council's policy needed to be updated to reflect this change in process.

In addition, following the changes to the Council's management structure new officers were required to be authorising officers and the policy had been updated to reflect these changes.

During the discussion of this item, Members made comments and statements and asked questions included: - (Responses were shown in italics)

- *Could the missing information from the RIPA document be included before the next inspection which was due later this year?*
- Members asked to see the document once the amendments had been included.
  The policy document could be approved as a Draft version subject to the required additional amendments being included. The document could then be re-submitted for final approval at a meeting later in the year.
- Could a notification system for surveillance requests be included in the document? Perhaps to the Chairman and Vice-Chairman of the Committee, or to all Members?
- Outside agencies and contractors used surveillance as well. Was this covered in the policy?
  Outside agencies would have their own procedures in place for requests for surveillance.

Resolved that:-

1. The report be noted;
2. The appointment of the Assistant Chief Executive and Monitoring Officer as the Senior Responsible Officer for the Regulation of Investigatory Powers Act process be approved; and
3. The Council's draft updated Policy and Procedures in relation to the Regulation of Investigatory Powers Act as set out within the report be approved, with the Monitoring Officer being requested to bring any further changes back to a future meeting of the Committee.

23. Whistle Blowing Policy Refresh

Considered report previously circulated, concerning the refresh of the Council's Whistleblowing Policy.

Following new legislation -The Enterprise and Regulatory Reform Act 2013 - the policy needed to be revised to ensure it complied.

It was important that an up to date policy was maintained so that employees and members of the public knew how to report any concerns and what protection they had. The main change from the previous policy was in the protection offered to a whistleblower. This had been changed so that any person raising a concern where they reasonably believed that the disclosure they were making was in the public interest, even if they were mistaken, would be protected.

The Whistleblowing policy was an important part of the authority's governance arrangements and thus need to be regularly reviewed to ensure it complied with all current legislation.

Resolved that the updated Whistleblowing Policy for Taunton Deane Borough Council be approved.

24. Money Laundering Policy Refresh

Considered report previously circulated, concerning the proposed Money Laundering Policy.

The proposed policy ensured that the Council had appropriate and proportionate measures in place to comply with the legal requirements, to implement relevant regulatory provisions and to protect its staff and Members.

The Council and its individual Members and employees had obligations under the Terrorism Act 2000 and certain sections of the Proceeds of Crime Act 2002 relating to money laundering. Public authorities were not legally obliged to implement the provisions of the Money Laundering Regulations 2007 because public authorities were neither 'relevant persons' nor part of the 'regulated sector'.

However, as a prudent and responsible public body, the Council's policy and procedures should be designed to reflect the essence of the UK's anti-terrorist financing and anti-money laundering regimes.

Money laundering was any attempt to use the proceeds of crime for legitimate purposes and was generally defined as the process by which the proceeds of crime, and the true ownership of those proceeds, were changed so that the proceeds appeared to come from a legitimate source. Anyone who became aware of an activity which they had reasonable grounds to suspect, was related to the proceeds of crime might be guilty of a money laundering offence.

The Chartered Institute of Public Finance and Accountancy (CIPFA) had published guidance on how the provisions of this framework apply to public authorities (CIPFA, 2009). The Policy which had accompanied the report had been designed to ensure that the Council and its staff fulfilled all legal obligations and regulatory requirements in accordance with this guidance.

Resolved that the Money Laundering Policy be approved.

25. Update on Internal Audit Plan 2013/2014

Considered report previously circulated, concerning an update on issues raised at the previous meeting in relation to the Procurement Cards Audit and the delay in progressing various ICT Audits.

The Procurement Card Audit had contained six recommendations that had been agreed by the Strategic Finance Officer. Although five of these were due to be completed by 31 March 2014, unfortunately this deadline had been missed.

A policy had now been written and agreed by the Assistant Director - Resources. This had been shared with all the holders of Procurement Cards who had been asked to confirm that they had read the policy and understood their responsibility as a Procurement Card holder.

Further reported that the delays with the ICT audits had resulted from the auditors not being provided with the appropriate access to the SAP system, which was required in order for them to undertake the audit.

The issues had now been resolved and satisfactory progress had now been made on the audits in question. The Data Centre Facilities Management audit had now been finalised. The System Development Life Cycle would be finalised by the 16 May 2014 and SAP IT Financial Controls would be finalised by the 20 June 2014

During the discussion of this item, Members made comments and statements and asked questions included: - (Responses were shown in italics)

- Pleased to hear that certain elements would be blocked on Procurement Cards.
- Had there been any issues with Procurement Cards and using them?
  There had been no issues with staff using Procurement Cards. Getting people set up and instructed on how to use the cards was straight forward.

Resolved that the progress with both the Procurement Card Audit Recommendations and the ICT Audits be noted.

26. Corporate Governance Committee Forward Plan

Submitted for information the proposed Forward Plan of the Corporate Governance Committee.

Resolved that the Corporate Governance Committee Forward plan be noted.

(The meeting ended at 7.40pm).