COTSWOLD
DISTRICT COUNCIL

# AUDIT COMMITTEE AGENDA

Thursday 14 November 2019, 4.00 p.m.

Council Chamber, Trinity Road, Cirencester

Trinity Road, Cirencester, Gloucestershire, GL7 1PX Tel: 01285 623000 www.cotswold.gov.uk

# NOTES

(i) Questions Arising on the Agenda

If any Member has any questions regarding either (a) an update/progress report on a specific item contained in the Minutes of the previous Meeting or (b) a report contained within the Agenda, he/she is requested to give advance notice of such question to the Director/Officer originating the report or to an Officer of the Democratic Services Section so that a full response can be made available either prior to, or at, the Meeting. If no such advance notification is given, a full response to any question cannot be guaranteed at the Meeting.

With specific regard to the Minutes of previous Meetings, Members' attention is drawn to Council Procedure Rule 17.1 which provides that, once the Minutes have been signed, Members may ask questions to ascertain what progress has been made on a particular matter referred to in the Minutes, but may not make any other statement or generate discussion on the Minutes.

(ii) Mobile Phones/Pagers

All mobile phones/pagers should be **SWITCHED OFF OR SET TO SILENT MODE BEFORE** the start of the Meeting.

(iii) Recording of Proceedings

The public proceedings of Council, Cabinet, and Committee Meetings may be recorded, which includes filming as well as audio-recording. Photography is also permitted.

As a matter of courtesy, if you intend to record any part of the proceedings please let the Committee Administrator know before the start of the Meeting.

Recording/filming should not be disruptive or distracting to the good order and conduct of the Meeting. To assist with this, an area of the Meeting venue will be designated from which proceedings can be recorded/filmed, and 'roaming' around the venue while recording is not permitted. The Chair will exclude anyone whose behaviour is disruptive.

Recording/filming should only be of Members and Council Officers, and not any members of the public (unless they are formally addressing the Meeting or unless specific permission has been given by those individuals).

For further information, please read the Notices displayed inside and outside the Meeting venue and/or speak with the Committee Administrator.

(iv) Committee Administrator

If any Member has any general questions about the Meeting or the associated agenda papers, or is unable to attend, he/she is asked to contact Democratic Services.

Distribution:

All Members of the Audit Committee
(Councillors Patrick Coleman, Roly Hughes, Nick Maunder, Richard Morgan, Ray Theodoulou)

All other Councillors for information

**Nigel Adams**
Head of Paid Service 6 November 2019

# AUDIT COMMITTEE : 14 NOVEMBER 2019

# AGENDA

(1) **Apologies**

(2) **Substitute Members** - To note details of any substitution arrangements in place for the Meeting.

Note:

The procedures in respect of substitution arrangements are principally set out in Council Procedure Rule 29. Particular attention is drawn to the fact that the Head of Democratic Services must be notified of any intended substitution **by 5.00 p.m. on the working day prior to the day of the Meeting.** Please note that neither a Member of the Cabinet, nor the Chair of the Council, may substitute.

(3) **Declarations of Interest** - To receive any declarations of interest from Members under:-

(i) the Code of Conduct for Members; and/or

(ii) Section 106 of the Local Government Finance Act 1992 (any Councillor who has Council Tax payments remaining unpaid for at least two months must declare an interest and not participate in any matter affecting the level of Council tax or arrangements for administering the Council Tax).

(4) **Minutes**

To confirm the Minutes of the Meeting of the Committee held on 26 September 2019 (attached).

(5) **Chair's Announcements** (if any)

(6) **Public Questions** - Council Procedure Rule 10 - Not more than fifteen minutes allowed for written questions to be put by Local Government electors within the Cotswold District on any matter in relation to which the Council has any power or duties or which affects the district, and which falls within the Terms of Reference of the Committee.

(7) **Member Questions** - Council Procedure Rule 11 - Not more than fifteen minutes allowed for written questions to be put by Members on any matter in relation to which the Council has any power or duties or which affects the district, and which falls within the Terms of Reference of the Committee.

# Items for Consideration and Decision

(8) **Meeting times**

For Members to consider whether the meeting times should be changed to increase public involvement and engagement at the meeting.

(9) **Grant Thornton Reports – (Reports to follow)**
**(Chief Finance Officer)**

For Members to receive and discuss details of the Annual Audit Letter for 2018/19 and an update report from the Council's external auditors (Grant Thornton).

*Officer Recommendation*

*That the Committee discuss and note the Annual Audit Letter and update report from Grant Thornton.*

Officer Ref: Jenny Poole (01285 623313)

(10) **Treasury Management Mid-Year Performance Report 2019-20**
**(Chief Finance Officer)**

To receive and discuss the Council's Treasury Management performance for the period 1 April to 30 September 2019.

*Officer Recommendation*

*That the Treasury Management mid-year performance be considered and recommended to Council for approval.*

Officer Ref: Jenny Poole (01285 623313)

(11) **Internal Audit Plan Progress Report 2019-20**
**(Chief Finance Officer)**

To present Members with a summary of the activity undertaken by Internal Audit since Committee on 25 July 2019.

*Officer Recommendation*

*That the report be noted.*

Officer Ref: Jenny Poole (01285 623313)

(12) **Counter Fraud Unit Report**
**(Counter Fraud Manager)**

To provide the Audit Committee with assurance over the counter fraud activities of the Council.

*Officer Recommendation*

*a) That the Committee notes the report and the work plan and makes comment as necessary.*

b) *That the Committee considers the Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy to comment thereon to Cabinet, to aid its deliberations and decision making.*

c) *That the Committee considers the Investigatory Powers Act 2016 Acquisition of Communications Data Policy to comment thereon to Cabinet, to aid its deliberations and decision making.*

Officer Ref: Jenny Poole (01285 623313) and Emma Cathcart (01285 623356)

(13) **Corporate Risk Register Updates**
**(Head of Paid Service)**

To update the Committee on the changes to the Council's Corporate Risk Register at the end of Quarter 2.

*Officer Recommendation*

*That the Committee notes the updates to the Council's Corporate Risk Register.*

Officer Ref: Nigel Adams (01285 623202)

(14) **Work Plan 2019/20**

To consider the Work Plan for 2019/20.

# Other Matters

(15) **Date of Next Meeting** - The next Meeting of the Committee will be held in the Council Chamber, Trinity Road, Cirencester on Thursday 30 January 2020 at 10.00 a.m.

(16) **Other Business** - Such other business which, in the opinion of the Chair, is urgent.

(END)

COTSWOLD DISTRICT COUNCIL

AUDIT COMMITTEE

26 SEPTEMBER 2019

Present:

Councillors

Patrick Coleman — Chair

Stephen Andrews
Nick Maunder
Richard Morgan (left at 11.30am)

Substitutes:

Stephen Andrews

Apologies:

Ray Theodoulou and Roly Hughes.

AUD.16 SUBSTITUTION ARRANGEMENTS

Councillor Stephen Andrews substituted for Councillor Ray Theodoulou.

AUD.17 DECLARATIONS OF INTEREST

There were no declarations of interest under the Code of Conduct for Members or Section 106 of the Local Government Finance Act 1992.

There were no declarations of interest under the Code of Conduct for Officers.

AUD.18 MINUTES

**RESOLVED that the Minutes of the Meeting of the Committee held on 25th July 2019 be confirmed.**

**Record of Voting - for 4, against 0, abstention 0, absent 1.**

AUD.19 CHAIR'S ANNOUNCEMENTS

The Chair announced he would be attending the Local Audit Quality Forum to be held on 25 November 2019 at Transport House, LGA Headquarters.

AUD.20 PUBLIC QUESTIONS

No public questions had been received.

AUD.21 MEMBER QUESTIONS

No Member questions had been received.

AUD.22 PRIVATE WATER SUPPLIES

The Service Leader (Operational, Technical and Pollution Services) and Environmental & Regulatory Services Senior Officer attended Committee to give and update on the changes made following the internal audit report on private water supplies.

There is a duty on Local Authorities to regulate private water supplies such as boreholes, wells, springs, rivers, lakes and land drains. Requirements are that the supply should be wholesome for customers to use.

The team look after 234 private supplies within the district. From the samples being taken 32% of these would fail the test, if this happens recommendations are given to the customer to correct the situation. Samples will be sent to the lab at South East Water and can take anything from five days to three months for the results to be returned. If any fail the Council has a legal obligation to provide technical advice and if there is a clear danger to the water supply the Council would then issue a notice to restrict the supply, the customer would then have 28 days to resolve the issue.

One of the Audit recommendations was to undertake cleansing work on the data which is used to submit information to the Water Inspectorate. This had been done by; prioritising the work on the Uniform computer system and be consistent with data entry which means invoicing can be carried out correctly; updating outdated records and access databases which in turn updates the annual return for the drinking water inspectorate. All members of staff are now entering data consistently and procedures are now in place with quality assurance being carried out to ensure consistency. There is always room for human error.

Work on the sampling procedures had been carried out, updating procedure notes and identifying missing data. A monthly report is run to match every supply to visits and cross that information with historic data.

Risk Assessment which is a legal obligation has to be carried out and the risk assessed as a minimum once every five years. Work plans are issued to each member of staff and put on the forward plan for the next 12 months which is being monitored on a monthly basis.

A new procedure for invoicing is in place with monthly reports being produced to ensure invoicing to customers is taking place. Officers are update to date with invoices to the end of July 2019.

This is a complex service which needs a high level of expertise, improvements have been introduced and Uniform helps with a consistent approach. Issues highlighted in the 2017/18 audit plan are being addressed, with regards to sampling, risk assessment and investigations, costs that are able to be recovered are done so.

Officers responded to Member questions:

(i) Most enforcement cases comply if served a notice, there is a process for monitoring compliance/non compliance, if the case is considered for prosecution there would be independent scrutiny before this happened.

(ii) Waste water which is privately cleansed would have private treatment plants if the customers are intending to drink the water. Legislation covers this issue and the environment agency and other organisations would be involved to ensure safety.

(iii) RAF Fairford have their own borehole and they have to carry out their own assessments on the supply of drinking water which is then presented to the water inspectorate. The Council does not have jurisdiction on the base.

The Chair thanked the officers and noted the high level of assurance which they were able to provide, which is an example of the benefits of having a proactive internal audit service.

**RESOLVED that the report and comments made be noted.**

**Record of Voting - for 4, against 0, abstentions 0, absent 1.**

AUD.23 STATEMENT OF ACCOUNTS 2018/19

The accounts were presented to Committee for approval. Thanks were expressed to Council Officers and Grant Thornton for their work on producing the accounts. One of the reasons for the lateness of the final Statement of Accounts was because the Government had changed the dates for final accounts to be produced throughout local authorities and for this reason Grant Thornton had difficulty resourcing local authority audits. Local authorities are lobbying the Government to move the deadline dates for audits back to the end of September. The statutory deadline for publishing the accounts is current end of July.

The Chief Finance Officer commented that the audit fee had been increased by £4,500 because of extra work needed to be carried out. The Council would be writing to the PSAA for them to consider whether they feel this is necessary.

Officers explained that the Statement of Accounts had been prepared for dispatch of papers and some small changes had been made following the dispatch, these were circulated to Committee and had been highlighted in the accounts. The following changes were highlighted:

(i) The difference in debtors and creditors balances were highlighted to Members, in relation to the collection of council tax business rates, extracting all payments to other organisations such as the County Council, Parish/Town Council, Police and Crime Commissioner, leaving the balance for the Council.

(ii) Figures had been revised following the McCloud judgement on the pension fund.

(iii) Some items of income had switched category, although the final figure remained the same.

(iv) All of 2010 business rates valuations appeals had been resolved. MHCLG were considering the business rates retention scheme.

Officers responded to Member questions:

(i) Clarification was given to Members in relation to the collection of council tax. The Council collecting the tax, payments go out to Parish/Town Councils,

County Council and Police. Some payments are paid in twelve monthly instalments, some every six monthly instalments. The monies left would be invested. If there is late collection of council tax and the Council has a surplus, this would be distributed to the relevant organisations. One exemption of collection of business rates was the flooding in Gloucestershire in 2007.

(ii) The implications around McCloud ruling on the pension fund are being monitored by officers, with Actuaries calculating the investment returns.

(iii) Journal entries have been corrected, within income and expenditure.

(iv) Categorisation of items such as investment income, fees and charges have been put under headings to explain the income, categorisation should be clearer and there is a mapping process to these items.

(v) Reserves are working for the Council in the financial markets. The capital strategy sets out plans on spending.

Grant Thornton were invited to speak to Committee. They explained that there are two opinions, the first for financial statements and second for a value for money conclusion on whether the Council is delivering what it is meant to deliver. They did anticipate offering an unqualified opinion although a few adjustments were made to conclude the Audit. They were in receipt of a signed variation. The opinions set out areas of work and value for money arrangements, medium term financial planning and governance arrangements in relation to Publica. The concept of materiality is used so every pound is not being audited.

A risk which had been identified was around journals, although an improvement had been made on last year, it is still a high risk area and controls need to be in place.

The Chief Financial Officer explained that there are financial challenges ahead and decisions will need to be made in the future whether the Council call on reserves or discover ways of income generation, such as reviewing fees and charges, review of car parking charges. Substantial savings were made through sharing services and setting up Publica.

The Chair thanked Grant Thornton and Officers for the thorough approach to the audit and the impending unqualified opinion.

**RESOLVED that:**

**(a) the Grant Thornton findings report for the Council be noted;**
**(b) the Statement of Accounts be approved;**
**(c) the Chief Finance Officer and the Chairman of the Audit Committee be authorised to write a letter of representation on behalf of the Committee and Council the Grant Thornton to enable an opinion to be issued.**

**Record of Voting - for 4, against 0, abstentions 0, absent 1.**

AUD.24 TREASURY INVESTMENT OPPORTUNITY WITH A HOUSING REIT (REAL ESTATE INVESTMENT TRUST)

The report presented a treasury investment opportunity for the Council to invest in available long term funds in a Social Housing REIT

Officers explained that Fundamentum Property are looking to raise £150m. To do this they would go through the international stock exchange, for the purchase of properties for vulnerable people and people with disabilities. Arlingclose Limited, the Council's treasury advisors had identified this opportunity to invest. The amount which was considered appropriate to invest would be £1m. Officers and Arlingclose would be doing further due diligence. The money could be earning an additional £40,000. The risk of investing in an investment trust is of the rise and fall of the investment in line with the valuation of the housing assets

Officers responded to Member questions:

(i) Fundamentum Property owned the Castel Fund which was sold and they are now looking to set up a new fund;
(ii) 25% of the UK REIT's are already listed on the International Stock Exchange;
(iii) There are three directors listed on the REIT, the auditors are KPMG. They would be working alongside local authorities, the management fees would be 0.6% and ongoing charges.
(iv) A fixed fee is being received for the launch.
(v) Officers would ascertain whether there would be an entry fee for the launch.
(vi) Members required assurance at Arlingclose were doing due diligence
(vii) 5% inflation linked.
(viii) The money invested in the REIT would be invested for the long term, Members were concerned about liquidity and the market price if they were to sell shares, and how the estimate of the shares could change, the return on investments, the gearing seems quite high.
(ix) There is a large exposure on that fund, how much borrowing on top, investing in residential property and there is a risk of the property market falling.
(x) There would be a need to ensure that this would be an ethical type of investment as the Council had passed a motion on the climate change emergency.

A proposal was put forward by Councillor Maunder to half the investment to £500,000.

Members were concerned to be investing in the REIT and wanted more information and reassurances, as the launch was to be in the Channel Islands and run from the Isle of Man. There were also concerns over why the Castel Fund run by Fundamentum Properties was sold and did the investors make money by selling the fund. Officers were asked to consult with Arlingclose and do more due diligence on what consequences of the future investment would be if Fundamentum did sell the portfolio.

Grant Thornton highlighted that there would be audit regulations in relation to investing in the REIT and they would appoint a review partner to deal with the investments and questioned whether the Council would be dealing with an investment or a company.

**RESOLVED to note the reports and comments made**

**Record of Voting - for 3, against 0, abstentions 0, absent 2.**

AUD.25 DATE OF NEXT MEETING

The date of the next meeting to be held in the Council Chamber at the Council offices, Trinity Road, Cirencester, 14 November 2019 at 4.00 pm.

AUD.26 OTHER BUSINESS

There was no other business that was urgent.

The Meeting commenced at 10.00 a.m. and closed at 1.20pm

Chair

(END)

COTSWOLD DISTRICT COUNCIL

| | |
|---|---|
| Council name | **COTSWOLD DISTRICT COUNCIL** |
| Name and date of Committee | **AUDIT COMMITTEE – 14 NOVEMBER 2019** |
| Report Number | **AGENDA ITEM 9** |
| Subject | **GRANT THORNTON REPORTS** |
| Wards affected | All |
| Accountable member | Cllr. Mike Evemy, Deputy Leader and Cabinet Member for Finance<br>Mike.evemy@cotswold.gov.uk |
| Accountable officer | Jenny Poole, Chief Finance Officer<br>Jenny.Poole@cotswold.gov.uk<br>01285 623313 |
| Summary/Purpose | For Members to receive and discuss details of the Annual Audit Letter for 2018/19 and an update report from the Council's external auditors (Grant Thornton). |
| Annexes | Annex A – Grant Thornton report – "The Annual Audit Letter for Cotswold District Council"<br>Annex B – Grant Thornton report – "Audit Progress Report and Sector Update" |
| Recommendation/s | *That the Committee discuss and note the Annual Audit Letter and update report from Grant Thornton.* |
| Corporate priorities | Ensure that all services delivered by the Council are delivered to the highest standard. |
| Key Decision | No |
| Exempt | No |
| Consultees/ Consultation | N/A |

## 1. BACKGROUND

**1.1.** The Council's external auditor (Grant Thornton) has provided the Annual Audit Letter for 2018/19 (see Annex A) and an update report for Members to consider (see Annex B).

**1.2.** The Annual Audit Letter summarises the key findings arising from the work carried out by Grant Thornton at the Council for the year ended 31 March 2019. Detailed findings from the audit work were reported to the Council's Audit Committee (as those charged with governance) in Grant Thornton's Audit Findings Report on 26 September 2019. The key points from the Letter are summarised below:

### Financial statements opinion

**1.3.** An unqualified opinion on the Council's financial statements was issued on 15 October 2019.

### Value for money conclusion

**1.4.** The auditor was satisfied that the Council put in place proper arrangements to ensure economy, efficiency and effectiveness in its use of resources during the year ended 31 March 2019. This was reflected in the audit opinion on 15 October 2019.

### Certificate

**1.5.** The auditor certified the completion of the audit of the accounts of Cotswold District Council in accordance with the requirements of the Code on 15 October 2019.

### Audit Progress Report and Sector Update

**1.6.** The update report includes an update of progress on the audit deliverables for 2018/19 and 2019/20 and highlights emerging issues and developments.

**1.7.** Representatives from Grant Thornton have been invited to the meeting and will be available to answer any questions on either document.

Grant Thornton

# The Annual Audit Letter for Cotswold District Council

**Year ended 31 March 2019**

**5 November 2019**

# Contents

**Your key Grant Thornton team members are:**

Julie Masci
Key Audit Partner
T: 029 2034 7506
E: julie.masci@uk.gt.com

Michelle Burge
Manager
T: 0117 305 7886
E: michelle.burge@uk.gt.com

Courtney Aylott
In Charge Auditor
T: 0117 305 7809
E: courtney.j.aylott@uk.gt.com

| Section | | Page |
|---|---|---|
| 1. | Executive Summary | 3 |
| 2. | Audit of the Financial Statements | 5 |
| 3. | Value for Money conclusion | 12 |

**Appendices**

A Reports issued and fees

# Executive Summary

## Purpose

Our Annual Audit Letter (Letter) summarises the key findings arising from the work that we have carried out at Cotswold District Council (the Council) for the year ended 31 March 2019.

This Letter is intended to provide a commentary on the results of our work to the Council and external stakeholders, and to highlight issues that we wish to draw to the attention of the public. In preparing this Letter, we have followed the National Audit Office (NAO)'s Code of Audit Practice and Auditor Guidance Note (AGN) 07 – 'Auditor Reporting'. We reported the detailed findings from our audit work to the Council's Audit Committee as those charged with governance in our Audit Findings Report on 26 September 2019.

## Respective responsibilities

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

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

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

## Our work

| | |
|---|---|
| **Materiality** | We determined materiality for the audit of the Council's financial statements to be £812,900, which was 2% of the Council's gross revenue expenditure. |
| **Financial Statements opinion** | We gave an unqualified opinion on the Council's financial statements on 15 October 2019. |
| **Whole of Government Accounts (WGA)** | We completed work on the Council's consolidation return following guidance issued by the NAO.<br><br>We carried out work on the Council's Data Collection Tool in line with instructions provided by the NAO . We issued an assurance statement which confirmed the Council was below the audit threshold. |
| **Use of statutory powers** | We did not identify any matters which required us to exercise our additional statutory powers. |
| **Value for Money arrangements** | We were satisfied that the Council put in place proper arrangements to ensure economy, efficiency and effectiveness in its use of resources. We reflected this in our audit report to the Council on 15 October 2019. |
| **Certificate** | We certified that we have completed the audit of the financial statements of Cotswold District Council in accordance with the requirements of the Code of Audit Practice on 15 October 2019. |

# Executive Summary

## Working with the Council

During the year we have delivered a number of successful outcomes with you:

- Sharing our insight – we provided regular audit committee updates covering best practice.
- We shared our thought leadership reports, providing insight on topical issues in the sector including
- Providing training – we provided your teams with training on financial statements
- We held quarterly liaison meeting with the Chief Finance Officer to discuss emerging issues.

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

**Grant Thornton UK LLP**
**November 2019**

# Audit of the Financial Statements

## Our audit approach

### Materiality

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

We determined materiality for the audit of the Council's financial statements to be £812,900, which is 2% of the Council's gross revenue expenditure. We used this benchmark as, in our view, users of the Council's financial statements are most interested in where the Council has spent its revenue in the year.

We also set a lower level of specific materiality for senior officer remuneration of £20,000.

We set a lower threshold of £40,645, above which we reported errors to the Audit Committee in our Audit Findings Report.

### The scope of our audit

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

- the accounting policies are appropriate, have been consistently applied and adequately disclosed;
- the significant accounting estimates made by management are reasonable; and
- the overall presentation of the financial statements gives a true and fair view.

We also read the remainder of the financial statements to check it is consistent with our understanding of the Council.

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

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

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

# Audit of the Financial Statements

## Significant Audit Risks

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

| Risks identified in our audit plan | How we responded to the risk | Findings and conclusions |
|---|---|---|
| **Valuation of land and buildings**<br><br>The Authority revalues its land and buildings on a rolling five year basis. This valuation represents a significant estimate by management in the financial statements due to the size of the numbers involved and the sensitivity of this estimate to changes in key assumptions. Additionally, management need to ensure the carrying value in the Authority financial statements is not materially different from the current value or fair value (for surplus assets) at the financial statements date, where a rolling programme is used.<br><br>We therefore identified valuation of land and buildings, particularly revaluations, as a significant risk, as one of the most significant assessed risks of material misstatement. | We part of our audit work we have:<br>• evaluated management's processes and assumptions for the calculation of the estimate, the instructions issued to the valuation experts and the scope of their work<br>• evaluated the competence, capabilities and objectivity of the valuation expert<br>• communicated with the valuer to confirm the basis on which the valuations were carried out<br>• challenged the information and assumptions used by the valuer to assess completeness and consistency with our understanding<br>• tested revaluations made during the year to ensure they have been input correctly into the Council's asset register<br>• evaluated the assumptions made by management for any assets not revalued during the year and how management has satisfied themselves that these are not materially different to current value. | Our audit work has not identified any issues in respect of valuation of property, plant and equipment |

# Audit of the Financial Statements

## Significant Audit Risks

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

| Risks identified in our audit plan | How we responded to the risk | Findings and conclusions |
|---|---|---|
| **Valuation of investment property**<br>The Authority revalues its investment properties on an annual basis to ensure that the carrying value is not materially different from the fair value at the financial statement date. This valuation represents a significant estimate by management in the financial statements due to the size of the numbers involved (£4.8m) and the sensitivity of this estimate to changes in key assumptions.<br>Management engaged the services of a external valuer to estimate the current value as at 31 March 2019.<br>We therefore identified valuation of investment properties, particularly revaluations as a significant risk, which was one of the most significant assessed risks of material misstatement. | We part of our audit work we have:<br>• evaluated management's processes and assumptions for the calculation of the estimate, the instructions issued to the valuation experts and the scope of their work<br>• evaluated the competence, capabilities and objectivity of the valuation expert<br>• communicated with the valuer to confirm the basis on which the valuations were carried out<br>• challenged the information and assumptions used by the valuer to assess completeness and consistency with our understanding<br>• tested revaluations made during the year to ensure they have been input correctly into the Council's asset register | Our audit work has not identified any issues in respect of valuation of investment properties. |

# Audit of the Financial Statements

## Significant Audit Risks

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

| Risks identified in our audit plan | How we responded to the risk | Findings and conclusions |
|---|---|---|
| **Valuation of net pension liability**<br><br>The Council's pension fund asset and liability as reflected in its balance sheet represent a significant estimate in the financial statements.<br><br>We identified the valuation of the Authority's pension fund net liability as a significant risk, which was one of the most significant assessed risks of material misstatement. | As part of our audit work we have:<br>• updated our understanding of the processes and controls put in place by management to ensure that the Authority's pension fund net liability is not materially misstated and evaluate the design of the associated controls;<br>• evaluated the instructions issued by management to their management expert (an actuary) for this estimate and the scope of the actuary's work;<br>• assessed the competence, capabilities and objectivity of the actuary who carried out the Authority's pension fund valuation;<br>• assessed the accuracy and completeness of the information provided by the Authority to the actuary to estimate the liability;<br>• tested the consistency of the pension fund asset and liability and disclosures in the notes to the core financial statements with the actuarial report from the actuary;<br>• undertook procedures to confirm the reasonableness of the actuarial assumptions made by reviewing the report of the consulting actuary (as auditor's expert) and performing any additional procedures suggested within the report;<br>• obtained assurances from the auditor of the Pension Fund as to the controls surrounding the validity and accuracy of membership data; contributions data; and benefits data sent to the actuary by the pension fund and the fund assets valuation in the pension fund financial statements. | The Council requested an estimate from its actuary of the potential impact of the 'McCloud' ruling and GMP equalisation changes. The actuary's estimate was of a increase in pension liabilities of £310,000 (£237,000 and £73,000 respectively). A revised IAS 19 report was issued in July which also included actual rather than estimated return on investment value resulting in an overall increase of net pension liabilities of £750,000.The Council has adjusted for this in the final version of the statement of accounts. We assessed the reasonableness of the adjustment and are satisfied that the approach and assumptions used by the actuary in the calculation of the estimate are reasonable |

# Audit of the Financial Statements

## Significant Audit Risks

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

| Risks identified in our audit plan (continued) | How we responded to the risk | Findings and conclusions (continued) |
|---|---|---|
| **Valuation of net pension liability (continued)**<br><br>The Council's pension fund asset and liability as reflected in its balance sheet represent a significant estimate in the financial statements.<br><br>We identified the valuation of the Authority's pension fund net liability as a significant risk, which was one of the most significant assessed risks of material misstatement. | | We recommended in 2017/18 that In order to support the Council's position that it retains liabilities in relation to staff transferred to controlled companies, it should ensure that the tripartite admission agreements between the Council, its controlled entities and Gloucestershire Pension Fund are clarified to more clearly emphasise that that the Council bears the risks in relation to changes in actuarial assumptions. We highlighted that the Council should review its tripartite agreements to ensure that its controlled entities are not unintendedly exposed to any actuarial or financial risks in relation to pensions obligations of staff transferred under TUPE arrangements. The Council was unable to amend the tripartite agreement. An alternative legal agreement was finalised between the Council, Publica and Gloucestershire Pension Fund which agrees that a fixed LGPS contribution rate is in place with Publica and that the impact of triennial valuations will be the responsibility of the Council. We received a signed copy of the agreement on the 25 September 2019.<br><br>Our audit work has not identified any issues in respect of the Pension Fund net liability. |

# Audit of the Financial Statements

## Significant Audit Risks

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

| Risks identified in our audit plan | How we responded to the risk | Findings and conclusions |
|---|---|---|
| **Management override of internal controls**<br>Under ISA (UK) 240 there is a non-rebuttable presumed risk that the risk of management over-ride of controls is present in all entities. The Council faces external scrutiny of its spending, and this could potentially place management under undue pressure in terms of how they report performance.<br><br>We therefore identified management override of controls as a risk requiring special audit consideration. | As part of our audit work we:<br>• evaluated the design effectiveness of management controls over journals<br>• analysed the journals listing and determine the criteria for selecting high risk unusual journals<br>• tested unusual journals recorded during the year and after the draft accounts stage for appropriateness and corroboration<br>• gained an understanding of the accounting estimates and critical judgements applied made by management and consider their reasonableness with regard to corroborative evidence<br>• evaluated the rationale for any changes in accounting policies, estimates or significant unusual transactions. | Following a recommendation raised in 2017/18, our testing of journals identified that journals raised by the Deputy S.151 Officer should be subject to review and approval by the Chief Finance Officer. Our testing identified that although the majority of journals raised by the Deputy S.151 officer were reviewed by the Chief Finance Officer, 2/15 had not been subject to review and evidence of approval could not be located for one.<br><br>We recommended in our audit findings report that all journals posted by the Deputy Section 151 Officer, including accruals should be subject to review and approval by the Chief Finance Officer.<br><br>Our audit work has not identified any other issues in respect of management override of controls.<br><br>**Management response**<br>The process for identifying journals processed by the Deputy S.151 Officer is manual and onerous. Therefore, we will comply with this recommendation as far as is reasonably practicable. |

# Audit of the Financial Statements

### Audit opinion
We gave an unqualified opinion on the Council's financial statements on 15 October 2019.

### Preparation of the financial statements
The Council presented us with draft financial statements in accordance with the national deadline, and overall provided us with a good set of working papers to support them.

### Issues arising from the audit of the financial statements
We reported the key issues from our audit to the Council's Audit Committee on 26 September 2019.

### Annual Governance Statement and Narrative Report
We are required to review the Council's Annual Governance Statement and Narrative Report. It published them on its website in the Statement of Accounts in line with the statutory requirements.

Both documents were prepared in line with the CIPFA Code and relevant supporting guidance. We confirmed that both documents were consistent with the financial statements prepared by the Council and with our knowledge of the Council.

### Whole of Government Accounts (WGA)
We carried out work on the Council's Data Collection Tool in line with instructions provided by the NAO . We issued an assurance statement which confirmed the Council was below the audit threshold.

### Other statutory powers
We also have additional powers and duties under the Act, including powers to issue a public interest report, make written recommendations, apply to the Court for a declaration that an item of account is contrary to law, and to give electors the opportunity to raise questions about the Council's accounts and to raise objections received in relation to the accounts. No additional statutory powers were exercised.

### Certificate of closure of the audit
We certified that we have completed the audit of the financial statements of Cotswold District Council in accordance with the requirements of the Code of Audit Practice on 15 October 2019.

# Value for Money conclusion

## Background

We carried out our review in accordance with the NAO Code of Audit Practice, following the guidance issued by the NAO in November 2017 which specified the criterion for auditors to evaluate:

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

## Key findings

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

The risks we identified and the work we performed are set out overleaf.

As part of our Audit Findings report agreed with the Council in September 2019, we agreed a recommendations to address our findings.

## Overall Value for Money conclusion

We are satisfied that in all significant respects the Council put in place proper arrangements to secure economy, efficiency and effectiveness in its use of resources for the year ending 31 March 2019.

# Value for Money conclusion

## Value for Money Risks

| Risks identified in our audit plan | Findings and conclusions |
|---|---|
| **Medium Term Financial Strategy (MTFS)**<br><br>The Authority has been required to deliver substantial savings since 2010/11 and forecast continued significant savings requirements going forward. The current MTFS indicates that the Authority has identified that it needs to find savings of £2.1m between 2019/20 and 2021/22. The Authority may need to use the General Fund Working Balance in order to balance the budget from 2020/21 onwards unless further savings of £1.5m can be identified. | As part of our work we:<br>• Reviewed the MTFS, including the robustness of the assumptions underpinning the strategy.<br>• Understood how savings were identified and monitored to ensure they supported the delivery of budgets<br>• Considered 2018/19 performance against savings plans<br>• Considered the use of reserves in 2019/20 to reach the balanced budget.<br>We concluded that the risk was sufficiently mitigated and the Council has proper arrangements for planning finances effectively to support the sustainable delivery of strategic priorities.<br>We recommend that Members and Officers should work together as part of the 2020/21 Budget and MTFS planning process to identify and develop further plans to resolve the funding gap.<br>**Management response**<br>Work is already taking place with the new Administration to develop both a contingency plan to address likely reductions to central government funding, which will now take effect from 2021/22, and to increase income to fund activity to support the priorities of the new Administration. The Council will consider the contingency plans and income generation plans as part of the updated MTFS and detailed budgets for 2020/21 in February 2020. |

# Value for Money conclusion

## Value for Money Risks

| Risks identified in our audit plan | Findings and conclusions |
|---|---|
| **Publica Group (Support) Ltd**<br>Publica is a Council owned employment company which delivers shared services between Cotswold, West Oxfordshire, Forest of Dean and Cheltenham Borough Council. 2018/19 is the first full year of operation for Publica. The success of Publica is critical to the medium term financial strategy of the Authority. | As part of our work we:<br>• Reviewed the contract monitoring processes in place to ensure performance and quality standards are delivered in line with the original Business Plan<br>• Reviewed the arrangements in place at the Council to ensure Publica is delivering required financial savings while maintaining agreed service standards<br>• Reviewed the Council's Governance arrangements to provide appropriate oversight as one of the partnering organisations, including how members of the Council are kept informed of any issues and the outcomes of remedial action required to address any issues identified.<br><br>We concluded that the Council has appropriate arrangements in place. |

# A. Reports issued and fees

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

## Reports issued

| Report | Date issued |
|---|---|
| Audit Plan | January 2019 |
| Audit Findings Report | September 2019 |
| Annual Audit Letter | November 2019 |

## Fees

| | Planned £ | Actual fees £ | 2017/18 fees £ |
|---|---|---|---|
| Statutory audit | 34,557 | 34,557 | 44,879 |
| Additional Audit Fee* | | 4,500 | 8,000 |
| **Total fees** | **34,557** | **39,057** | **52,879** |

* Fee variations are subject to PSAA approval.

## Audit fee variation

As outlined in our audit plan, the 2018-19 scale fee published by PSAA of £34,557 assumes that the scope of the audit does not significantly change. There are a number of areas where the scope of the audit has changed, which has led to additional work. These are set out in the table on the next page.

## Fees for non-audit services

| Service | Fees £ |
|---|---|
| **Audit related services**<br>- None | Nil |
| **Non-Audit related services**<br>- CFO Insights subscription | 3,750 |

## Non- audit services

- For the purposes of our audit we have made enquiries of all Grant Thornton UK LLP teams providing services to the Council. The table above summarises all non-audit services which were identified.

- We have considered whether non-audit services might be perceived as a threat to our independence as the Council's auditor and have ensured that appropriate safeguards are put in place.

The above non-audit services are consistent with the Council's policy on the allotment of non-audit work to your auditor.

# A. Reports issued and fees (continued)

## Audit fee variation

As outlined in our audit plan, the 2018-19 scale fee published by PSAA of £34,557 assumes that the scope of the audit does not significantly change. There are a number of areas where the scope of the audit has changed, which has led to additional work. These are set out in the table below.

| Area | Reason | Fee proposed |
|---|---|---|
| **Assessing the impact of the McCloud ruling** | The Government's transitional arrangements for pensions were ruled discriminatory by the Court of Appeal last December. The Supreme Court refused the Government's application for permission to appeal this ruling. As part of our audit we considered the impact on the financial statements along with any audit reporting requirements. This included consultation with our own internal actuary in their capacity as an auditor expert. | 1,500 |
| **Pensions – IAS 19** | The Financial Reporting Council has highlighted that the quality of work by audit firms in respect of IAS 19 needs to improve across local government audits. Accordingly, we increased the level of scope and coverage in respect of IAS 19 this year to reflect this.<br>This additional work involved areas including:<br>- Additional testing of data provided to the actuary and Gloucestershire pension fund to inform the IAS 19 valuation<br>- Further scrutiny and review of the assumptions used by the Council's actuary to determine its valuation for reasonableness and changes to previous years. | 1,500 |
| **PPE Valuation – work of experts** | As above, the Financial Reporting Council has highlighted that auditors need to improve the quality of work on PPE valuations across the sector. We have increased the volume and scope of our audit work to reflect this.<br>This additional work involved areas including:<br>- Additional sample testing of valuations carried out during the year to understand reasons for valuation changes and key assumptions informing these valuations<br>- Additional review and testing of information and finance and asset data provided to the valuer used to inform their valuation exercise<br>- Enhanced scrutiny and challenge around those assets not subject to formal valuation during the period to support management's view that these are materially stated within the financial statements | 1,500 |
| **Total** | | 4,500 |

Grant Thornton
An instinct for growth™



# Audit Progress Report and Sector Update

Cotswold District Council
Year ending 31 March 2020

**5 November 2019**

# Contents


| Section | Page |
|---|---|
| Introduction | 3 |
| Progress at November 2019 | 4 |
| Audit Deliverables | 6 |
| Sector Update | 7 |

# Introduction

**Julie Masci**

**Engagement Lead**

T 029 2034 7506
M 07730 677623
E Julie.masci@uk.gt.com

**Michelle Burge**

**Engagement Manager**

T 0117 305 7886
M 07825 028771
E michelle.burge@uk.gt.com

## This paper provides the Audit 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 local authority; and
- includes a number of challenge questions in respect of these emerging issues which the Committee may wish to consider (these are a tool to use, if helpful, rather than formal questions requiring responses for audit purposes)

Members of the Audit Committee can find further useful material on our website, where we have a section dedicated to our work in the public sector. Here you can download copies of our publications www.grantthornton.co.uk

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

# Progress at November 2019

## Financial Statements Audit

We issued our opinion on your 2018/19 Statement of Accounts on 15 October 2019. We will begin our planning for the 2019/20 audit in December and will issue a detailed audit plan, setting out our proposed approach to the audit of the Council's 2019/20 financial statements in early 2020.

We will begin our interim audit in January 2020. Our interim fieldwork includes:

- Updated review of the Council's control environment
- Updated understanding of financial systems
- Review of Internal Audit reports on core financial systems
- Early work on emerging accounting issues
- Early substantive testing

## Value for Money

The scope of our work is set out in the guidance issued by the National Audit Office. The Code requires auditors to satisfy themselves that; "the Council has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources".

The guidance confirmed the overall criterion as: "in all significant respects, the audited body had proper arrangements to ensure it took properly informed decisions and deployed resources to achieve planned and sustainable outcomes for taxpayers and local people".

The three sub criteria for assessment to be able to give a conclusion overall are:

- Informed decision making
- Sustainable resource deployment
- Working with partners and other third parties

Details of our initial risk assessment to determine our approach will be included in our Audit Plan.

We will report our work in the Audit Findings Report and aim to give our Value For Money Conclusion by the statutory accounts publication date of 31 July 2020.

# Progress at November 2019 (Cont.)

## Other areas

### Meetings

We met with your Chief Finance Officer and finance team in September as part of our quarterly liaison meetings and continue to be in discussions with finance staff regarding emerging developments and to ensure the audit process is smooth and effective.

### Events

We provide a range of workshops, along with network events for members and publications to support the Council.

Further details of the publications that may be of interest to the Council are set out in our Sector Update section of this report.

## Audit Fees

During 2017, PSAA awarded contracts for audit for a five year period beginning on 1 April 2018. 2019/20 is the second year of that contract. Since that time, there have been a number of developments within the accounting and audit profession. Across all sectors and firms, the Financial Reporting Council (FRC) has set out its expectation of improved financial reporting from organisations and the need for auditors to demonstrate increased scepticism and challenge and to undertake additional and more robust testing.

Our work in the Local Government sector in 2018/19 has highlighted areas where financial reporting, in particular, property, plant and equipment and pensions, needs to improve. There is also an increase in the complexity of Local Government financial transactions and financial reporting. This combined with the FRC requirement that all Local Government audits are at or above the “few improvements needed” (2A) rating means that additional audit work is required.

We are currently reviewing the impact of these changes on both the cost and timing of audits. We will discuss this with your s151 Officer including any proposed variations to the Scale Fee set by PSAA Limited, before communicating fully with the Audit Committee.

As a firm, we are absolutely committed to meeting the expectations of the FRC with regard to audit quality and local government financial reporting.

# Audit Deliverables

| 2018/19 Deliverables | Planned Date | Status |
|---|---|---|
| **Audit Findings Report**<br>The Audit Findings Report was reported to the September Audit Committee. | September 2019 | Complete |
| **Auditors Report**<br>This is the opinion on your financial statements, annual governance statement and value for money conclusion. | October 2019 | Complete |
| **Annual Audit Letter**<br>This letter communicates the key issues arising from our work. | November 2019 | Complete |

| 2019/20 Deliverables | Planned Date | Status |
|---|---|---|
| **Fee Letter**<br>Confirming audit fee for 2019/20. | April 2019 | Complete |
| **Accounts Audit Plan**<br>We are required to issue a detailed accounts audit plan to the Audit Committee setting out our proposed approach in order to give an opinion on the Council's 2019-20 financial statements. | January 2020 | Not yet due |

# Sector Update

Councils are tackling a continuing drive to achieve greater efficiency in the delivery of public services, whilst facing the challenges to address rising demand, ongoing budget pressures and social inequality.

Our sector update provides you with an up to date summary of emerging national issues and developments to support you. We cover areas which may have an impact on your organisation, the wider LG and the public sector as a whole. Links are provided to the detailed report/briefing to allow you to delve further and find out more.

Our public sector team at Grant Thornton also undertake research on service and technical issues. We will bring you the latest research publications in this update. We also include areas of potential interest to start conversations within the organisation and with audit committee members, as well as any accounting and regulatory updates.

- **Insights from local government sector specialists**
- **Reports of interest**
- **Accounting and regulatory updates**

More information can be found on our dedicated public sector and local government sections on the Grant Thornton website by clicking on the logos below:

Public Sector

Local government

# CIPFA – CFO confidence survey

## In July, the Chartered Institute of Public Finance and Accountancy (CIPFA) reported the results of their annual confidence survey.

The survey found that the majority of local government finance officers have lost confidence in their future financial positions over the last year.

Seventy per cent of respondents said they were either slightly less or much less confident in their financial position this year compared to 2018-19.

The survey also found that 68% said they were either slightly less or much less confident in their ability to deliver services in 2020-21. Sixty-two per cent expressed equal confidence in their financial position for 2019-20 as they had last year.

CIPFA found that the area of greatest pressure for top tier authorities was children's social care, with the number of authorities rating it as the biggest pressure rising by six percentage points.

For districts the greatest pressures were housing, cultural services and environmental services.

Rob Whiteman, CIPFA chief executive, said: "Local government is facing greater demand pressures than ever before, with particularly pressures in adults' and children's social care and housing. Local authorities also lack certainty about their future financial positions, so it's unsurprising to see confidence on the decline.

"We have repeatedly pointed out that local government is in need of a sustainable funding solution, but meeting this demand requires more than pennies and pounds. The sector as a whole must come together to address the challenges of effective service delivery."

CIPFA's survey received a total of 119 responses from authorities in the UK - 56 top tier authorities, 47 English districts, 12 Scottish authorities, and 4 Welsh authorities.

CIPFA The Chartered Institute of Public Finance & Accountancy

On the same theme, a Local Government Association (LGA) survey, also reported in July, found that almost two-thirds of councils believe cash for services like adult social care, child protection and preventing homelessness will dry up by 2024-25.

The survey got responses from 141 of the 339 LGA member councils in England and Wales.

It also found that 17% of councils were not confident of realising all of the savings they had identified this year (2019-20).

The LGA said that councils needed a guarantee they will have enough money to meet growing demand pressures in particular in adult social care, children's services, special educational needs, homelessness support and public health.

Local Government Association

### Financial confidence

**Challenge question:**

How confident over its' financial position is your Authority? Has this changed from previous years?

# Local Government Association – Profit with a purpose – delivering social value through commercial activity

## The Local Government Association (LGA) report 'Profit with a purpose' focuses on some of the practicalities of how councils can deliver social value through their commercial activity.

Through 'key questions' to ask, the guidance supports councils to face the challenge of how to undertake commercial activity and achieve greater value for the public purse in ways that better meet society's needs and outcomes for people and communities.

In addition, the publication features a number of short case studies highlighting some of the innovative commercial practice already achieving results for communities.

The LGA comments that the best approaches ensure the generation of social value is the primary factor driving commercial activity; from the initial decision to develop a commercial vision to how the approach is developed, and implemented, councils which are pulling ahead ensure social value is placed centre stage.

The guidance starts with an overview of what the LGA understands by 'profit with a purpose', the guidance explores different types of social value and the role of councils in driving social value alongside their commercial ambition.

The guidance then looks at how consideration and delivery of social value should be practically considered when deciding on whether to embark on commercial activity, the need for social value to be prioritised alongside financial return and the key questions councils should consider when embarking on a commercial initiative.

Following on from this, there are specific chapters on; embedding social value in governance of alternative service delivery vehicles, the role of procurement in contracting services that deliver social value and finally how to contract and performance manage social value through your service providers.

Each chapter outlines the factors that need to be considered and the 'key questions' councils should be asking themselves.

In addition, a number of short case studies are provided to highlight some of the innovative commercial practice already achieving results for communities.

The report can be downloaded from the LGA website:

https://www.local.gov.uk/profit-purpose-delivering-social-value-through-commercial-activity

Local Government Association

### Profit with a purpose

**Challenge question:**

If your Authority is looking at commercial activity, have you considered the LGA report?

# MHCLG – Brexit preparations

## Councils should be fully prepared to leave the European Union by the end of October, the Communities and Local Government Secretary announced on 3 August as he ramped up preparations.

Mr Jenrick thanked councils for all the work they have already done, but said they must step up vital preparations and committed £20 million for councils across England to prepare for delivering Brexit on 31 October, whatever the circumstances.

He has asked each council to designate a Brexit lead to work with central government and oversee teams in every community who will work with stakeholders in their area to plan intensively for Brexit.

The new funding comes in recognition of the central role councils will play to make sure their residents are ready for Brexit, and is expected to support a range of activity including communications, training and the recruitment of staff.

Ministry of Housing, Communities & Local Government

The Secretary of State said:

"From Whitehall to town halls – everyone needs to be ready to fulfil our democratic mandate to leave the European Union by the end of October.

Local government has a vital role in helping to make Brexit a success and it is absolutely right that together we intensify preparations in every community.

And to do this successfully I have asked every council to appoint a Brexit lead to work with government. We'll be providing £20 million for councils to support the major step up in preparations.

I want all of us – central and local government – to be fully prepared for leaving the EU on 31 October whatever the circumstances. I know that we can achieve this, by continuing to work side by side with renewed national focus and intensity."

### Brexit preparations

**Challenge question:**

Who is your Brexit lead and how is your authority supporting Brexit preparations?

# Public Accounts Committee – Local Government Governance and Accountability

## The Public Accounts Committee has found that the Government has not done enough to ensure that, at a time when local authority budgets are under extreme pressure, governance systems are improved.

The Ministry of Housing, Communities & Local Government (the Department) is responsible for: ensuring that this framework contains the right checks and balances, and changing the system if necessary. The Secretary of State also has powers to intervene in cases of perceived governance failure. The framework includes: officers with statutory powers and responsibilities; internal checks and balances such as audit committees and internal audit; and external checks and balances such as external audit and sector-led improvement overseen by the Local Government Association. These arrangements represent a significant reduction in the level of central oversight in recent years following the government's decision to abolish the Audit Commission and the Standards Board for England as part of a broader reform of local audit, inspection and reporting.

The Public Accounts Committee report summary notes "Local authorities have a good overall track record with governance arrangements generally robust across the sector, and there is evidence that local authority governance compares favourably to that of the health sector. However, this is not universal and in some authorities governance is under strain, as funding reduces and responsibilities and exposure to commercial pressures change. We are worried to hear about audit committees that do not provide sufficient assurance, ineffective internal audit, weak arrangements for the management of risk in local authorities' commercial investments, and inadequate oversight and scrutiny. This is not acceptable in the more risky, complex and fast-moving environment in which local authorities now operate.

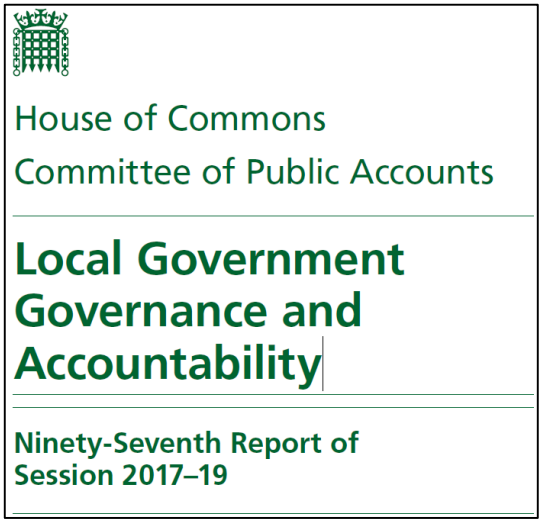
The Department has been reactive and ill-informed in its approach to oversight of the local governance system. However, the Department has now recognised that the network of bodies with responsibility for the local governance framework is fragmented and lacking the leadership needed to drive change. Encouragingly, the Department has now committed to enhancing its oversight role and producing a proactive work programme to deliver this change. We urge the Department to ensure that this activity leads to concrete actions and outcomes on a timely basis. When a local authority fails this has a significant impact on local people and the Department has a responsibility to work with local government to ensure that problems are caught early and that it can pinpoint at-risk councils. Since the abolition of the Audit Commission and other changes culminating in the Local Audit and Accountability Act 2014 there is no central assessment of value for the money, which means the Department's work is fundamental."

The report makes five conclusions, with associated recommendations:

1) The Department is not yet providing effective leadership of the local governance system.
2) The Department does not know why some local authorities are raising concerns that external audit is not meeting their needs.
3) The Department lacks reliable information on key governance risks, or relies on weak sources of information, meaning it has no way of pinpointing the at-risk councils.
4) The Department's monitoring is not focused on long-term risks to council finances and therefore to services.
5) There is a complete lack of transparency over both the Department's informal interventions in local authorities with financial or governance problems and the results of its formal interventions.

The Government response is available on the website below:

https://www.parliament.uk/documents/commons-committees/public-accounts/Gov-response-to-Public-Accounts-on-the-93-98-reports.pdf



# MHCLG – Independent probe into local government audit

## In July, the then Communities secretary, James Brokenshire, announced the government is to examine local authority financial reporting and auditing.

At the CIPFA conference he told delegates the independent review will be headed up by Sir Tony Redmond, a former CIPFA president.

The government was “working towards improving its approach to local government oversight and support”, Brokenshire promised.

“A robust local audit system is absolutely pivotal to work on oversight, not just because it reinforces confidence in financial reporting but because it reinforces service delivery and, ultimately, our faith in local democracy,” he said.

“There are potentially far-reaching consequences when audits aren’t carried out properly and fail to detect significant problems.”

The review will look at the quality of local authority audits and whether they are highlighting when an organisation is in financial trouble early enough.

It will also look at whether the public has lost faith in auditors and whether the current audit arrangements for councils are still “fit for purpose”.

On the appointment of Redmond, CIPFA chief executive Rob Whiteman said: “Tony Redmond is uniquely placed to lead this vital review, which will be critical for determining future regulatory requirements.

“Local audit is crucial in providing assurance and accountability to the public, while helping to prevent financial and governance failure.”

He added: “This work will allow us to identify what is needed to make local audit as robust as possible, and how the audit function can meet the assurance needs, both now and in the future, of the sector as a whole.”

In the question and answer session following his speech, Brokenshire said he was not looking to bring back the Audit Commission, which appointed auditors to local bodies and was abolished in 2015. MHCLG note that auditing of local authorities was then taken over by the private, voluntary and not-for-profit sectors.

He explained he was “open minded”, but believed the Audit Commission was “of its time”.

Local authorities in England are responsible for 22% of total UK public sector expenditure so their accounts “must be of the highest level of transparency and quality”, the Ministry of Housing, Local Government and Communities said. The review will also look at how local authorities publish their annual accounts and if the financial reporting system is robust enough.

Redmond, who has also been a local authority treasurer and chief executive, is expected to report to the communities secretary with his initial recommendations in December 2019, with a final report published in March 2020. Redmond has also worked as a local government boundary commissioner and held the post of local government ombudsman.

Ministry of Housing, Communities & Local Government

# National Audit Office – Code of Audit Practice

The Code of Audit Practice sets out what local auditors of relevant local public bodies are required to do to fulfill their statutory responsibilities under the Local Audit and Accountability Act 2014. 'Relevant authorities' are set out in Schedule 2 of the Act and include local councils, fire authorities, police and NHS bodies.

Local auditors must comply with the Code of Audit Practice.

### Consultation – New Code of Audit Practice from 2020

Schedule 6 of the Act requires that the Code be reviewed, and revisions considered at least every five years. The current Code came into force on 1 April 2015, and the maximum five-year lifespan of the Code means it now needs to be reviewed and a new Code laid in Parliament in time for it to come in to force no later than 1 April 2020.

In order to determine what changes might be appropriate, the NAO is consulting on potential changes to the Code in two stages:

**Stage 1** involves engagement with key stakeholders and public consultation on the issues that are considered to be relevant to the development of the Code.

**This stage of the consultation is now closed.** The NAO received a total of 41 responses to the consultation which included positive feedback on the two-stage approach to developing the Code that has been adopted. The NAO state that they have considered carefully the views of respondents in respect of the points drawn out from the Issues paper and this will inform the development of the draft Code. A summary of the responses received to the questions set out in the Issues paper can be found below.

Local audit in England Code of Audit Practice – Consultation Response (pdf – 256KB)

**Stage 2** of the consultation involves consulting on the draft text of the new Code. To support stage 2, the NAO has published a consultation document, which highlights the key changes to each chapter of the draft Code. The most significant changes are in relation to the Value for Money arrangements. Rather than require auditors to focus on delivering an overall, binary, conclusion about whether or not proper arrangements were in place during the previous financial year, the draft Code requires auditors to issue a commentary on each of the criteria. This will allow auditors to tailor their commentaries to local circumstances. The Code proposes three specific criteria:

a) Financial sustainability: how the body plans and manages its resources to ensure it can continue to deliver its services;

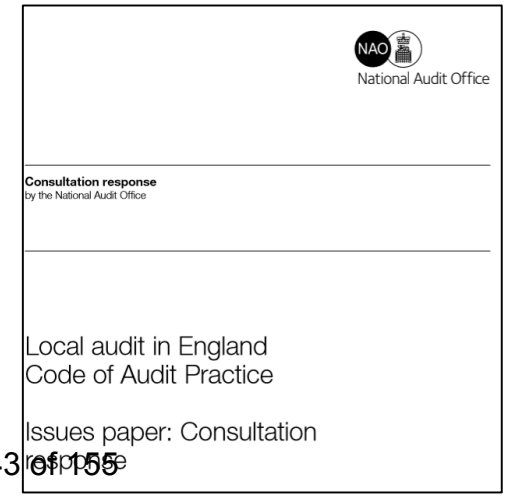
b) Governance: how the body ensures that it makes informed decisions and properly manages its risks; and

c) Improving economy, efficiency and effectiveness: how the body uses information about its costs and performance to improve the way it manages and delivers its services.

The consultation document and a copy of the draft Code can be found on the NAO website. The consultation is open until 22 November 2019. The new Code will apply from audits of local bodies' 2020-21 financial statements onwards.

Link to NAO webpage for the Code consultation:

https://www.nao.org.uk/code-audit-practice/code-of-audit-practice-consultation/



COTSWOLD DISTRICT COUNCIL

| | |
|---|---|
| Council Name | **COTSWOLD DISTRICT COUNCIL** |
| Name and date of Committee | **AUDIT COMMITTEE – 14 NOVEMBER 2019** |
| Report Number | **AGENDA ITEM 10** |
| Subject | **TREASURY MANAGEMENT MID-YEAR PERFORMANCE REPORT 2019-20** |
| Wards affected | ALL |
| Accountable member | Cllr Mike Evemy, Deputy Leader and Cabinet Member for Finance.<br>Email: mike.evemy@cotswold.gov.uk |
| Accountable officer | Jenny Poole, Chief Finance Officer<br>Tel: (01285) 623313 Email: jenny.poole@cotswold.gov.uk |
| Summary/Purpose | To receive and discuss the Council's Treasury Management performance for the period 1 April to 30 September 2019. |
| Annexes | None. |
| Recommendation | *That the Treasury Management mid-year performance be considered and recommended to Council for approval.* |
| Corporate priorities | |
| Key Decision | No |
| Exempt | No |
| Consultees/ Consultation | None |

## 1. BACKGROUND

1.1 In February 2011 the Authority adopted the Chartered Institute of Public Finance and Accountancy's Treasury Management in the Public Services: Code of Practice (the CIPFA Code). The Code requires Members of the Council to approve the treasury management strategy annually and receive a mid-year update on activity.

1.2 This report covers the treasury management activity and performance of Cotswold District Council for the period 1st April to 30th September 2019.

1.3 The Council's treasury management strategy for 2019/20 was approved at a meeting on 26th February 2019. The Council has invested substantial sums of money and is therefore exposed to financial risks including the loss of invested funds and the revenue effect of changing interest rates. The successful identification, monitoring and control of risk are therefore central to the council's treasury management strategy.

1.4 The 2017 Prudential Code includes a requirement for local authorities to provide a Capital Strategy, which is to be a summary document approved by full council covering capital expenditure and financing, treasury management and non-treasury investments. The authority's Capital Strategy, complying with CIPFA's requirement, was approved by full Council on 26th February 2019.

## 2. ECONOMIC UPDATE FOR THE PERIOD 1ST APRIL TO 30TH SEPTEMBER

2.1. UK Consumer Price Inflation (CPIH) fell to 1.7% year/year in August 2019 from 2.0% in July, weaker than the consensus forecast of 1.9% and below the Bank of England's target. The most recent labour market data for the three months to July 2019 showed the unemployment rate edged back down to 3.8% while the employment rate remained at 76.1%, the joint highest since records began in 1971. Nominal annual wage growth measured by the 3-month average excluding bonuses was 3.8% and 4.0% including bonuses. Adjusting for inflation, real wages were up 1.9% excluding bonuses (and 2.1% including).

2.2. The Quarterly National Accounts for Q2 GDP confirmed the UK economy contracted by 0.2% following the 0.5% gain in Q1 which was distorted by stockpiling ahead of Brexit. Only the services sector registered an increase in growth, a very modest 0.1%, with both production and construction falling and the former registering its largest drop since Q4 2012. Business investment fell by 0.4% (revised from -0.5% in the first estimate) as Brexit uncertainties impacted on business planning and decision-making.

2.3. Politics both home and abroad, continued to be a big driver of financial markets over the last quarter. Boris Johnson won the Conservative Party leadership contest and committed the Country to leaving the EU.

2.4. Tensions continued between the US and China with no trade agreement in sight and both countries imposing further tariffs on each other's goods. The US Federal Reserve cut its target Federal Funds rates by 0.25% in September to a range of 1.75% - 2%, a pre-emptive move to maintain economic growth amid escalating concerns over the trade war and a weaker economic environment leading to more

pronounced global slowdown. The euro area Purchasing Manager Indices (PMIs) pointed to a deepening slowdown in the Eurozone. These elevated concerns have caused key government yield curves to invert, something seen by many commentators as a predictor of a global recession. Market expectations are for further interest rate cuts from the Fed and in September the European Central Bank reduced its deposit rate to -0.5% and announced the recommencement of quantitative easing from 1st November

2.5. The Bank of England maintained Bank Rate at 0.75% and in its August Inflation Report noted the deterioration in global activity and sentiment and confirmed that monetary policy decisions related to Brexit could be in either direction depending on when a deal is ultimately reached.

**FINANCIAL MARKETS**

2.6. After rallying early in 2019, financial markets have been adopting a more risk-off approach in the following period as equities saw greater volatility and bonds rallied (prices up, yields down) in a flight to quality and anticipation of more monetary stimulus from central banks. The Dow Jones, FTSE 100 and FTSE 250 are broadly back at the same levels seen in March/April.

2.7. Gilt yields remained volatile over the period on the back of ongoing economic and political uncertainty. From a yield of 0.63% at the end of June, the 5-year benchmark gilt yield fell to 0.32% by the end of September. There were falls in the 10-year and 20-year gilts over the same period, with the former dropping from 0.83% to 0.55% and the latter falling from 1.35% to 0.88%. 1-month, 3-month and 12-month LIBID (London Interbank Bid) rates averaged 0.65%, 0.75% and 1.00% respectively over the period.

2.8. Recent activity in the bond markets and PWLB interest rates highlight that weaker economic growth remains a global risk. The US yield curve remains inverted with 10-year Treasury yields lower than US 3-month bills. History has shown that a recession hasn't been far behind a yield curve inversion. Following the sale of 10-year Bunds at -0.24% in June, yields on German government securities continue to remain negative in the secondary market with 2 and 5-year securities currently both trading around -0.77%.

2.9. Credit Default Swap (CDS) spreads rose and then fell again during the quarter, continuing to remain low in historical terms. After rising to almost 120bps in May, the spread on non-ringfenced bank NatWest Markets plc fell back to around 80bps by the end of September, while for the ringfenced entity, National Westminster Bank plc, the spread remained around 40bps. The other main UK banks, as yet not separated into ringfenced and non-ringfenced from a CDS perspective, traded between 34 and 76bps at the end of the period.

2.10. There were minimal credit rating changes during the period. Moody's upgraded The Co-operative Bank's long-term rating to B3 and Fitch upgraded Clydesdale Bank and Virgin Money to A-.

## 3. TREASURY MANAGEMENT - SUMMARY POSITION 1/4/2019 TO 30/9/2019

3.1 On the 31st March 2019, the Council had net lending of £32.203m arising from its revenue and capital income and expenditure. The underlying need to borrow for capital purposes is measured by the Capital Financing Requirement (CFR), while usable reserves and working capital are the underlying resources available for investment. These factors are summarised in Table 1 below:

Table 1: Balance Sheet Summary

| | **31.3.19 Actual £m** |
|---|---|
| General Fund – Capital Financing Requirement (CFR) | 0 |
| Less: External borrowing | 0 |
| Less: Usable reserves | (27.890) |
| Less: Working capital | (4.313) |
| **Net lending** | **(32.203)** |

3.2 The Council's current strategy is to maintain investments below their underlying levels, known as internal borrowing, in order to reduce risk and keep interest costs low.

Table 2: Treasury Management Summary

| | **31.3.19 Balance £m** | **Movement £m** | **30.9.19 Balance £m** | **30.9.19 Return %** |
|---|---|---|---|---|
| Long-term investments | 12.301 | 0.199 | 12.500 | 4.06 |
| Short-term investments | 13.190 | 2.810 | 16.000 | 0.83 |
| Cash and cash equivalents | 6.712 | (0.766) | 5.946 | 0.73 |
| **Net Lending** | **32.203** | **2.243** | **32.446** | **2.01** |

3.3 At 30th September 2019 the Authority was debt free and has no immediate plans to borrow.

### INVESTMENT PERFORMANCE AND PROJECTIONS

3.4 The Council holds invested funds, representing income balances and reserves. During the six month period the council's investment balance ranged between £26.4m and £42.00m due to timing differences between income and expenditure. The investment position, across investment type, as at the 30th September is shown below:

Table 3: Treasury Investment Position

| | 31.3.19 Balance £m | Net Movement £m | 30.9.19 Balance £m | 30.9.19 Return % |
|---|---|---|---|---|
| Banks & Building Societies (unsecured) | 8.033 | 7.967 | 16.000 | 0.94 |
| Local Authorities | 5.010 | (3.010) | 2.000 | 1.00 |
| Money Market Funds/ Call Accounts | 6.712 | (2.766) | 3.946 | 0.73 |
| Pooled Funds | 12.448 | 0.052 | 12.500 | 4.64 |
| **Total Investments** | **32.203** | **2.243** | **34.446** | **2.01** |

3.5 Both the CIPFA Code and government guidance require the Council to invest its funds prudently, and to have regard to the security and liquidity of its treasury investments before seeking optimum rate of return, or yield. All investments made to date have been in line with the approved lending list, as set in February 2019.

3.6 In March 2019 the Council's Investment income for 2019/20 was budgeted to be £575,668. The average cash balances available for investment, representing the council's reserves and working balances, was £33.582m during the period this report covers.

3.7 Based upon current performance and returns the Council is on target to achieve in the region of £650,000 (at an average rate of return of 1.94%) for this financial year, generating a budget surplus in the region of £74,000.

**POOLED FUNDS**

3.8 Table 4 below shows the current valuations of the Pooled Funds portfolio at 30th September 2019, compared with the opening balances of 1st April 2019.

Table 4: Pooled Funds

| FUND NAME | Initial Investment | 1 April Fund Value | 30th Sept Fund Value | Dividends in 2019/20 (as at 30 Sept) | Gain / (Loss) for 2019/20 | Gain / (Loss) to Initial Principal |
|---|---|---|---|---|---|---|
| | £ | £ | £ | £ | £ | £ |
| CCLA Property Fund | 500,000 | 511,537 | 506,759 | 11,168 | (4,778) | 6,759 |
| CCLA Property Fund | 2,000,000 | 1,872,848 | 1,855,357 | 40,889 | (17,491) | (144,643) |
| Schroders Income Maximiser Fund | 1,000,000 | 930,978 | 860,863 | 48,279 | (70,115) | (139,137) |
| CCLA Diversified Income Fund | 1,000,000 | 998,850 | 1,032,740 | 9,651 | 33,890 | 32,740 |
| M&G UK Income Fund | 2,000,000 | 1,932,672 | 1,948,542 | 62,622 | 15,870 | (51,458) |
| Investec Diversified Fund | 2,000,000 | 2,027,051 | 1,994,511 | 38,189 | (32,540) | (5,489) |
| Columbia Threadneedle Bond Fund | 2,000,000 | 2,026,591 | 2,075,104 | 30,577 | 48,513 | 75,104 |
| **Total** | **10,500,000** | **10,300,527** | **10,273,876** | **241,375** | **(26,651)** | **(226,124)** |

## 4. OUTLOOK FOR THE REMAINDER OF 2019/20

4.1 Having raised policy rates in August 2018 to 0.75%, the Bank of England's Monetary Policy Committee (MPC) has maintained expectations of a slow rise in interest rates over the forecast horizon.

4.2 The global economy is entering a period of slower growth in response to political issues, primarily the trade policy stance of the US. The UK economy has displayed a marked slowdown in growth due to both Brexit uncertainty and the downturn in global activity. In response, global and UK interest rate expectations have eased dramatically.

4.3 There appears no near-term resolution to the trade dispute between China and the US, a dispute that the US appears comfortable exacerbating further. With the 2020 presidential election a year away, Donald Trump is unlikely to change his stance.

4.4 The probability of a no-deal EU exit in the immediate term has decreased, although a no-deal Brexit cannot be entirely ruled out and the risk of this event remains for 2020. The upcoming general election may change the political landscape too.

4.5 The view is that the Bank Rate is to remain at 0.75% for the foreseeable future but there remain substantial risks to this forecast, dependant on Brexit outcomes and the evolution of the global economy. The Council's treasury advisors, Arlingclose, expect gilt yields to remain at low levels for the foreseeable future and judge the risks to be weighted to the downside and that volatility will continue to offer longer-term borrowing opportunities.

| | Dec-19 | Mar-20 | Jun-20 | Sep-20 | Dec-20 | Mar-21 | Jun-21 | Sep-21 | Dec-21 | Mar-22 | Jun-22 | Sep-22 | Dec-22 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Official Bank Rate | | | | | | | | | | | | | |
| Upside risk | 0.00 | 0.00 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 |
| Arlingclose Central Cas | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 |
| Downside risk | 0.50 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 | 0.75 |

## 5. COMPLIANCE

The Chief Finance Officer reports that all treasury management activities undertaken during the first six months complied fully with the CIPFA Code of Practice and the Authority's approved Treasury Management Strategy. Compliance with specific investment limits is demonstrated in table 6 below.

Table 6: Debt Limits

| | 30.9.19 Actual £m | 2019/20 Operational Boundary £m | 2019/20 Authorised Limit £m | Complied? |
|---|---|---|---|---|
| Borrowing | 0.0 | 7.8 | 10.8 | Yes |
| **Total debt** | **0.0** | **0.0** | **0.0** | |

COTSWOLD DISTRICT COUNCIL

| | |
|---|---|
| Council name | **COTSWOLD DISTRICT COUNCIL** |
| Name and date of Committee | **AUDIT COMMITTEE – 14 NOVEMBER 2019** |
| Report Number | **AGENDA ITEM 11** |
| Subject | **INTERNAL AUDIT PLAN PROGRESS REPORT 2019/20** |
| Wards affected | N/A |
| Accountable member | Cllr Mike Evemy, Deputy Leader and Cabinet Member for Finance<br>Email: mike.evemy@cotswold.gov.uk |
| Accountable officer | Jenny Poole, Chief Finance Officer<br>Tel: 01285 623313 Email: jenny.poole@cotswold.gov.uk |
| Summary/Purpose | To present the Audit Committee with a summary of the activity undertaken by Internal Audit since the last meeting of this Committee |
| Annexes | **ANNEX A – REPORT OF INTERNAL AUDIT ACTIVITY – PLAN PROGRESS 2019/20** |
| Recommendation/s | Please write recommendations using letters and italics as below.<br>*a) To note the report* |
| Corporate priorities | Ensure that all services delivered by the Council are delivered to the highest standard. |
| Key Decision | NO |
| Exempt | NO |
| Consultees/ Consultation | N/A |

## 1. BACKGROUND

The Internal Audit Service is provided to this Council by SWAP Internal Audit Services (SWAP). SWAP is a local authority-controlled company.

The report attached at **Annex A** sets out the work undertaken by SWAP for the Council since the last meeting of this Committee. It follows the risk-based auditing principles and, therefore, this is an opportunity for the Committee to be aware of emerging issues which have resulted in SWAP involvement.

Officers from SWAP will be in attendance at the Committee meeting and will be available to address Members' questions.

## 2. MAIN POINTS

**2.1.** The progress report enables the Audit Committee to monitor the work of the Internal Audit Service and ensure that it remains effective. It also provides the Committee with assurance opinions over areas reviewed within the reporting period, details of audit recommendations and the outcome of follow-up reviews conducted on previous audit recommendations.

## 3. FINANCIAL IMPLICATIONS

**3.1.** The Internal Audit Service is operating within the contract sum.

## 4. LEGAL IMPLICATIONS

**4.1.** None directly from this report. Internal Audit reviews consider compliance with legislation relevant to the service area under review.

## 5. RISK ASSESSMENT

**5.1.** The weaknesses in the control framework, identified by the Internal Audit activity, continues to threaten organisational objectives if recommendations are not implemented.

## 6. BACKGROUND PAPERS

**6.1.** Internal Audit Reports

# Cotswold District Council

## Report of Internal Audit Activity

### Plan Progress 2019/2020
### October 2019

**Internal Audit ▪ Risk ▪ Special Investigations ▪ Consultancy**

# Contents

**The contacts at SWAP in connection with this report are:**

**David Hill**
Chief Executive
Tel: 01935 848540
david.hill@swapaudit.co.uk

**Ian Baker**
Executive Director
Tel: 07917628774
ian.baker@swapaudit.co.uk

**Lucy Cater**
Assistant Director
Tel: 01285 623340
lucy.cater@swapaudit.co.uk

- Role of Internal Audit — Page 1
- Internal Audit Work — Page 2
- Approved Changes to the Audit Plan — Page 3
- Appendices:
  - Appendix A – Internal Audit Definitions — Page 4 – 5
  - Appendix B – Internal Audit Work Plan Progress — Page 6 – 10
  - Appendix C – Executive Summary of Finalised Audit Assignments — Page 11 – 20
  - Appendix D – High Priority Recommendation Follow-Up — Page 20 – 29
  - Appendix E – Summary of All Recommendations — Page 30

# Internal Audit Plan Progress 2018/2019

**Our audit activity is split between:**

- **Governance Audit**
- **Operational Audit**
- **Key Control Audit**
- **IT Audit**
- **Other Reviews**

## Role of Internal Audit

The Internal Audit service for Cotswold District Council is provided by SWAP Internal Audit Services (SWAP). SWAP is a Local Authority controlled Company. SWAP has adopted and works to the Standards of the Institute of Internal Auditors, further guided by interpretation provided by the Public Sector Internal Audit Standards (PSIAS), and also follows the CIPFA Code of Practice for Internal Audit. The Partnership is also guided by the Internal Audit Charter.

Internal Audit provides an independent and objective opinion on the Authority's control environment by evaluating its effectiveness. Primarily the work includes:

- Governance Audits
- Operational Audits
- Key Financial System Controls
- IT Audits
- Other Special or Unplanned Review

Internal Audit work is largely driven by an Annual Audit Plan. This is recommended to the Audit Committee by the Chief Finance Officer, following consultation with the Council's Management Team. The 2019/20 Audit Plan was reported to, and approved by, Audit Committee at its meeting in April 2019.

Audit assignments are undertaken in accordance with this Plan to assess current levels of governance, control and risk.

**Outturn to Date:**

**We rank our recommendations on a scale of 1 to 3, with 1 being a major area of concern requiring immediate corrective action and 3 being a minor or administrative concern**

- Internal Audit Work

Each completed assignment includes its respective "assurance opinion" rating together with the number and relative ranking of recommendations that have been raised with management. In such cases, the Committee can take assurance that improvement actions have been agreed with management to address these. The assurance opinion ratings have been determined in accordance with the Internal Audit "Audit Framework Definitions" as detailed in **Appendix A** of this document.

The schedule provided at **Appendix B** contains a list of all audits as agreed in the Internal Audit Annual Plan 2019/20. It is important that Members are aware of the status of all audits and that this information helps them place reliance on the work of Internal Audit and its ability to complete the plan as agreed.

As agreed with this Committee where a review has a status of 'Final' we will provide a summary of the work and further details to inform Members of any key issues, if any, identified.

Further information on all the finalised reviews can be found within **Appendix C**.

At **Appendix D** we have included a schedule of the high priority recommendations (priority 1s and 2s) that have been identified during our audit reviews. These will be updated when the follow-up audit has been completed.

**Appendix E** summarises all recommendations made and the progress that has been made against these.

**We keep our audit plans under regular review to ensure that we audit the right things at the right time.**

## Approved Changes to the Audit Plan

The audit plan for 2019/20 is detailed in **Appendix B.** Inevitably changes to the plan will be required during the year to reflect changing risks and ensure the audit plan remains relevant to Cotswold District Council. Members will note that where necessary any changes to the plan throughout the year will have been subject to agreement with the appropriate Service Manager and the Audit Client Officer (Chief Finance Officer).

The following changes have been made to the plan:

The audit on Business Rates Reset has been deferred at this time due to the slow progress at national level on the new Business Rates Scheme (due to come into effect April 2021).

We were asked to defer the audit on Civil Contingencies to later in the year by the client due to changes in the service.

We have been requested to undertake a review on Cash Handling procedures at our Partner Councils to ensure they are appropriate and adhered to.

The planned audit of Management and Monitoring of Contracts has been removed, days have been allocated to the review on Ubico – Waste and Recycling Contract. The audit, as originally planned, will be included in the 2020/21 audit plan.

We have been asked to undertake a small review by the CFO in respect of the Corinium Museum Project Management arrangements.

**At the conclusion of audit assignment work each review is awarded a "Control Assurance Definition";**

- **No Assurance**
- **Partial**
- **Reasonable**
- **Substantial**

## Audit Framework Definitions

**Control Assurance Definitions**

| | |
|---|---|
| **No Assurance** | The areas reviewed were found to be inadequately controlled. Risks are not well managed, and systems require the introduction or improvement of internal controls to ensure the achievement of objectives. |
| **Partial** | In relation to the areas reviewed and the controls found to be in place, some key risks are not well managed, and systems require the introduction or improvement of internal controls to ensure the achievement of objectives. |
| **Reasonable** | Most of the areas reviewed were found to be adequately controlled. Generally, risks are well managed, but some systems require the introduction or improvement of internal controls to ensure the achievement of objectives. |
| **Substantial** | The areas reviewed were found to be adequately controlled. Internal controls are in place and operating effectively and risks against the achievement of objectives are well managed. |

Non-Opinion – In addition to our opinion based work we will provide consultancy services. The "advice" offered by Internal Audit in its consultancy role may include risk analysis and evaluation, developing potential solutions to problems and providing controls assurance. Consultancy services from Internal Audit offer management the added benefit of being delivered by people with a good understanding of the overall risk, control and governance concerns and priorities of the organisation.

**Recommendations are prioritised from 1 to 3 on how important they are to the service/area audited. These are not necessarily how important they are to the organisation at a corporate level.**

**Each audit covers key risks. For each audit a risk assessment is undertaken whereby with management risks for the review are assessed at the Corporate inherent level (the risk of exposure with no controls in place) and then once the audit is complete the Auditors assessment of the risk exposure at Corporate level after the control environment has been tested. All assessments are made against the risk appetite agreed by the SWAP Management Board.**

## Audit Framework Definitions

**Categorisation of Recommendations**

When making recommendations to Management it is important that they know how important the recommendation is to their service. There should be a clear distinction between how we evaluate the risks identified for the service but scored at a corporate level and the priority assigned to the recommendation. No timeframes have been applied to each Priority as implementation will depend on several factors; however, the definitions imply the importance.

| | **Categorisation of Recommendations** |
|---|---|
| **Priority 1** | Findings that are fundamental to the integrity of the service's business processes and require the immediate attention of management. |
| **Priority 2** | Important findings that need to be resolved by management |
| **Priority 3** | Finding that requires attention. |

**Definitions of Risk**

| **Risk** | **Reporting Implications** |
|---|---|
| **High** | Issues that we consider need to be brought to the attention of both senior management and the Audit Committee. |
| **Medium** | Issues which should be addressed by management in their areas of responsibility. |
| **Low** | Issues of a minor nature or best practice where some improvement can be made. |

| Audit Type | Audit Area | Quarter | Status | Opinion | No of Rec | Priority | | | Comments |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | 1 | 2 | 3 | |
| **2018/19 Audits in Draft / In Progress at Annual Opinion** | | | | | | | | | |
| ICT | Data Protection Act (GDPR) | | Final Report | Substantial | 1 | | | 1 | See Appendices C & E |
| Operational | Procurement & Contact Management | | Final Report | Partial | 2 | | 1 | 1 | See Appendices C & E |
| Key Financial Control | Systems Admin | | Final Report | Reasonable | 7 | | 2 | 5 | See Appendices C & E |
| Key Financial Control | Human Resources | | Final Report | Reasonable | 2 | | 1 | 1 | See Appendices C & E |
| Key Financial Control | Procurement | | Draft Report | | | | | | |
| Governance | Risk Management | | Final Report | Substantial | - | | | | See Appendix C |
| ICT | Cybersecurity | | Draft Report | | | | | | |
| Advice and Consultancy | Benefits Realisation | | Position Statement | | | | | | |
| | | | | | | | | | |

| Audit Type | Audit Area | Quarter | Status | Opinion | No of Rec | Priority | | | Comments |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | 1 | 2 | 3 | |
| **2019/20 Audit Plan** | | | | | | | | | |
| Governance | Annual Governance Statement | 1 | Draft Report | | | | | | |
| Operational | Asset Management | 1 | Draft Report | | | | | | |
| Operational | Commercial Property / Investment Property | 1 | Draft Report | | | | | | |
| Operational | Management and Monitoring of Contracts | 1 | Deferred | | | | | | See note on page 3 |
| Operational | Use of Volunteers | 1 | In Progress | | | | | | |
| Advice and Consultancy | Cemetery Services Fees Process | 1 | Complete | | | | | | |
| ICT | Software as a Service – Cloud Provision | 1 | ToE Issued | | | | | | |
| ICT | Software as a Service – Dataset Management | 1 | ToE Issued | | | | | | |
| Advice and Consultancy | Ubico – Waste and Recycling Collection Contract | 1 | Draft Report | | | | | | Draft Report Issued – Waiting for Response(s) |
| | | | | | | | | | |
| Operational | Affordable Housing | 2 | Draft Report | | | | | | |
| Operational | Business Rates Reset | 2 | Deferred | | | | | | See note on page 3 |
| Operational | Internal Enforcement Agency | 2 | | | | | | | |

# Internal Audit Work Plan Progress 2019/2020 APPENDIX B

| Audit Type | Audit Area | Quarter | Status | Opinion | No of Rec | Priority | | | Comments |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | 1 | 2 | 3 | |
| Operational | Civil Contingencies | 2 | Deferred | | | | | | See note on page 3 |
| Operational | Grants | 2 | In Progress | | | | | | |
| Operational | Waste and Recycling Assets | 2 | | | | | | | |
| Operational | (NEW) Cash Handling | 2 | ToE Issued | | | | | | See note on page 3 |
| Grant Certification | Disabled Facilities Grants | 2 | Complete | | | | | | |
| ICT | Cyber Security – Incident Management | 2 | | | | | | | |
| ICT | Cyber Security – High Risk Area (defined from 2018/19 audit) | 2 | | | | | | | |
| | | | | | | | | | |
| Key Financial Control | Revenues and Benefits | 3 | | | | | | | |
| | • National Non-Domestic Rates | | In Progress | | | | | | |
| | • Council Tax | | | | | | | | |
| | • Council Tax Benefit | | In Progress | | | | | | |
| Key Financial Control | Core Financials | 3 | | | | | | | |
| | • Accounts Payable | | In Progress | | | | | | |
| | • Accounts Receivable | | | | | | | | |

| Audit Type | Audit Area | Quarter | Status | Opinion | No of Rec | Priority | | | Comments |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | 1 | 2 | 3 | |
| | • Main Accounting | | | | | | | | |
| | • Payroll | | | | | | | | |
| | • Treasury Management and Bank Reconciliation | | | | | | | | |
| Key Financial Control | Systems Administration | 3 | | | | | | | |
| Key Financial Control | Human Resources | 3 | In Progress | | | | | | |
| Key Financial Control | Other Support Service provided by Publica<br>• Health and Safety | 3 | | | | | | | |
| ICT | Management of Service Provision | 3 | | | | | | | |
| ICT | ICT Business Continuity | 3 | | | | | | | |
| Grant Certification | Disabled Facilities Grant Certification – Additional Grant | 3 | | | | | | | |
| Advice and Consultancy | (NEW) Corinium Museum – Project Management Arrangements | 3 | In Progress | | | | | | See note on page 3 |
| | | | | | | | | | |
| Governance | Risk Management | 4 | | | | | | | |
| Governance | Performance Management | 4 | | | | | | | |

| Audit Type | Audit Area | Quarter | Status | Opinion | No of Rec | Priority | | | Comments |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | 1 | 2 | 3 | |
| Operational | Publica Transformation Benefits Realisation | 4 | | | | | | | |
| Operational | Corporate Culture | 4 | | | | | | | |
| | | | | | | | | | |
| Follow-Up | Follow-Ups of Recommendations made in Substantial and Reasonable Audits | 1 – 4 | On Going | | | | | | |
| Follow-Up | Follow-Up of Control Weaknesses identified by the Counter Fraud Unit | 3 – 4 | | | | | | | |
| | | | | | | | | | |
| Advice and Consultancy | Workforce Strategy | 1 – 4 | | | | | | | |
| Advice and Consultancy | Support to the Publica Transformation Programme | 1 – 4 | On Going | | | | | | |
| Advice and Consultancy | Assurance to the Partner Councils in respect of the Publica Transformation Programme | 1 – 4 | | | | | | | |
| | | | | | | | | | |
| Other Audit Involvement | Working with the Counter Fraud Unit | 1 – 4 | On Going | | | | | | |
| Other Audit Involvement | Management of the IA Function and Client Support | 1 – 4 | On Going | | | | | | |

| Audit Type | Audit Area | Quarter | Status | Opinion | No of Rec | Priority | | | Comments |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | 1 | 2 | 3 | |
| Other Audit Involvement | Contingency – Provision for New Work based on emerging risks | | | | | | | | |
| | | | | | | | | | |

**Audit Assignments finalised since the last Audit Committee**:

- Summary of Audit Findings and High Priority Recommendations

The following information provides a brief summary of each audit review finalised since the last Committee update.

**2018/19 – Data Protection Act 2018 – Substantial Assurance**

**Background**

The new General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA) came into effect on 25 May 2018. Together they form the new Data Protection Legislation and replace the Data Protection Act 1998.

The DPA 2018 controls how personal information is used by organisations and increases the rights of the individual whose data is used. Most of the main principals of the previous data protection act are still the same, however accountability has been enhanced, and tighter time controls introduced in relation to the reporting of data breach incidents. In addition, fines and penalties for non-compliance with the new regulations have been increased.

The DPA also distinguishes between data controllers and data processors, and it applies to both. A controller determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of a controller.

The DPA places specific legal obligations on processors; for example, they are required to maintain records of personal data and processing activities. They will have legal liability if they are responsible for a breach. However, controllers are not relieved of DPA obligations where a processor is involved. The DPA places further obligations on them to ensure contracts with processors comply with the GDPR.

Publica Group is a council owned employment company which delivers shared services between Cotswold, West Oxfordshire, and Forest of Dean District Councils and Cheltenham Borough Council and could be considered as the data processor.

**Audit Conclusion / Findings**

In line with the Data Protection Act 2018 (DPA) requirements Publica have appointed a Data Protection Officer. Details of this post together with contact information is publicly available on the Publica Group's website.

Publica have an up to date and approved Data Protection Policy in place which is available to staff, and detailed information regarding Publica's data collection and usage is clear and can be found on the website. Publica employees have also received training on the DPA's requirements.

In the event of a potential data breach, Publica have a sound incident reporting procedure in place. Incidents are investigated thoroughly and assessed in line with the DPA to determine if they should be reported to the Information Commissioners Office (ICO). A register of incidents with supporting documents is maintained. We can confirm that no incidents have had to be reported to the ICO.

A recommendation was made in the 2017/18 EU General Data Protection Regulations advisory audit report to consider providing periodic, formal reporting on the progress of GDPR preparations including identified project and business risks and issues, to key Council and Publica risk owners, stakeholders, and Members. We can confirm that this reporting is now in place and provided by the Data Protection Officer on a quarterly basis.

Internal audit will include DPA 2018 compliance testing in individual service area audits during 2019/20 to provide additional assurance in this area.

In certain circumstances, such as enforcement, delegated statutory powers can be used when necessary to make requests for certain information from other public bodies. A recommendation is made to review all the roles where this is necessary to determine that if required, all employees hold a dual contract with the relevant Council to ensure compliance with these powers.

**2018/19 Risk Management – Substantial Assurance**

**Background**

The Risk Management audit is undertaken using a modular approach with one third of the process being examined and tested each year.

The modules are as follows:

- Risk Framework - Policy and Process
- Risk Identification and Assessment
- Risk Control Environment.

The module covered for this year's review is the Risk Control Environment. At October 2018 there were 25 risks identified in the Corporate Risk Register (CRR); 2 high scoring, 20 medium scoring and 3 low scoring risks. The 2 high scoring risks relate to the potential of an adverse local government financial settlement and the risk of poor service delivery by Publica.

Publica is responsible for service delivery for most of the Council's services and therefore risk management activity is undertaken by Publica officers as well as the Council's Statutory officers.

**Audit Conclusion / Findings**
The outcome of the review is as follows:

• There is a good system of risk review. Risks are reviewed and reported to the Shared Risk Management Group on a quarterly basis.
• The likelihood assessment of risks in the Corporate Risk Register (CRR) is fair.
• High Impact risks are closely monitored and managed appropriately.
• Appropriate controls have been identified although on occasion there was limited evidence to support how control effectiveness is assessed. Discussions with relevant officers confirmed processes were in place.

We can confirm that 3 recommendations from our previous audit undertaken in June 2018 have been implemented. A Business Manager – Corporate Responsibility has recently been appointed who we have been advised will oversee the implementation of the other 2 recommendations which relate to officer and member training provision. The officer will aim to implement consistent review and reporting across the partner councils.

Our review has found little change since services transferred to Publica. Although, we did note that the Q3 review of the CRR was not reported to the Audit Committee until April 2019. The previous report (Q2) was presented in October 2018. We were advised the delay was because the cycle of committee meetings had changed to meet the requirements of reporting the financial statements in line with statutory requirements. It is important that timely reports are presented on a quarterly basis so that Members charged with governance can be assured that risks are being managed effectively and if needed appropriate challenge can be made.

We have not made any recommendations in this report.

**2018/19 Systems Administration – Reasonable Assurance**

**Background**

Publica Group provide ICT infrastructure and support services on behalf of Cheltenham Borough Council (CBC), Cotswold District Council (CDC), Forest of Dean District Council (FoDDC) and West Oxford District Council (WODC).

As part of this service, Publica have written the ICT and Security Policies in place across Publica, CBC, CDC, FoDDC and WODC. The Security Policy framework incorporates an Access Control Policy which defines the required security controls for the provision of access and permissions to the councils' network and applications. Robust identity and access management processes and access controls are fundamental to help ensure the confidentiality, integrity and availability of an organisation's systems and data.

The Publica ICT team are responsible for the administration of the ICT estate however for certain applications, systems admin duties including access control fall within the service areas themselves and are not the sole responsibility of the ICT team.

Business World, the main financial system in use across the authorities, is managed by a dedicated systems admin team within Publica ICT. The Civica Cash Receipting system at CDC, FoDDC and WODC has a dedicated ICT system administrator who is also able to support CBC.

**Audit Conclusion / Findings**

Overall, the systems admin user access controls and processes reviewed for the business applications used by Publica and the Councils were found to be adequately controlled. The recommendations made within this report apply to processes across all business systems to improve internal controls and management of risks.

Those employees with systems admin responsibilities that were interviewed, are knowledgeable and understand their responsibilities and systems well.

A Security Policy framework is in place and incorporates an access control policy. An end to end access control process should be closely aligned to the Policy, fully documented and communicated widely. Whilst a process is generally followed by most teams, a recommendation has been made to document, align and ensure coverage of an Identity and Access Management process across all systems and for local procedures to be documented or updated to align with the

overarching policy and process.

Application settings should reflect the requirements stipulated in the Security Policy. A recommendation is made for the Policy to be issued to and reviewed by the system administrators so that any discrepancies are captured, remediated or risk managed.

Regular access reviews are not currently performed and a review of system access levels highlighted a need for this secondary control. In line with the Policy, a recommendation is made to undertake and document regular reviews of all access across all systems to ensure employees access is current, required and accurate according to job role and responsibility.

We were advised that the recommendations from the external auditor, Grant Thornton's ICT audit of 2018 are in progress.

| Priority | Recommendation | Management Response | Due Date |
|---|---|---|---|
| 2 | We recommend a principal Identity and Access Management process detailing requirements for 'Joiners, Movers and Leavers' is developed and documented and that complies with the requirements set out in the Information Security and Access Control Policy. The overarching process should apply to and embrace all systems that may not be included within the standard ICT team scope and should be available for all employees to view and follow.<br>System administrators should then document or update local processes and procedures that should be in alignment with the overarching policy and process requirements. and documented on a quarterly basis as per the requirements of the Risk Management | Our team ICT Administrators are now updating and documenting our Access Management system process for joiners, Movers and Leavers. A change control process will be introduced that will document significant changes to the ICT infrastructure which will also align to our ICT User Policies and guidances. | 31st March 2020 |

| | | | |
|---|---|---|---|
| | Policy | | |
| 2 | We recommend that officers with systems administration responsibilities are requested to review the Security Policy and its requirements, perform a gap analysis on their current system settings and processes and devise a plan to implement those changes to ensure continued compliance with the Policy. Should it not be possible to make changes for any reason, they should be risk assessed and documented on the ICT risk register or policy exception register.<br>Priority | We agree with the password setting findings and risks with on systems Business World and Civica applications. However at present these risks are mitigated by the Active Directory (AD) password settings. Both Business world and Civica systems users only access these systems via the AD. We also comply with the HMG National Cyber Security Centre (NCSC) password guidance on our network. However, we will seek to review all passwords policy setting on both applications. Our ICT Risk register will be updated to reflect these security risks and mitigations. | 31st December 2019 |

**2018/19 Procurement and Contact Management – Partial Assurance**

**Background**

The Publica Procurement Service provides a collaborative approach to procurement work, information and guidance to all of the Publica Partner Councils – Cotswold District Council (CDC), West Oxfordshire District Council (WODC), Forest of Dean District Council (FoDDC) and Cheltenham Borough Council (CBC) as well as Ubico and Cheltenham Borough Homes (CBH). The objective of the service is to improve the way the Council and partners procure services, goods and works and manage contracts to deliver improved quality services and make sure our spending is value for money.

Contracts and relationship management refers to the effective management and control of all contracts from their planned inception until their completion by the appointed contractor(s). It covers the supporting policies, procedures and systems needed to undertake it, together with broader issues from the identification and minimisation of risk, successful and timely delivery of outcomes and performance, effective control of cost and variations and the maintenance of clear communications and operational relationships with contractors.

Once a contract is in place, contract management is the responsibility of the contract owner or another delegated

contract manager. The TUPE transfer of most Council staff (from CDC, WODC and FoDDC) into Publica in November 2017 means that in the majority of cases, Publica officers are responsible for the management of contracts on the Councils' behalf.

The responsibility to manage contract and supplier risk is part of contract management activities once the contract is in place. Improvement of the contract management process is required and should also include enhancement of management of supplier risk.

The Council's Procurement and Contract Management Strategy sets out contract management guidance and requirements. The In-Tend Portal can be used by contract managers to prompt contract management activities, with an enhanced Contract Management Wizard module in the process of being purchased and set up as an add-on to the In-Tend Portal.

**Audit Conclusion / Findings**

We are able to offer a Partial assurance over the Procurement and Contract Management processes and related controls at Cotswold District Council (CDC). This opinion is based on the partial assurance issued to Publica Group (Support) Ltd (Publica) in an equivalent audit, who provide procurement services to CDC.

Evidence was obtained to confirm some sound procurement and due diligence processes during the tender stages. Relevant evidence and information is requested of potential suppliers at various stages, including as part of pre-procurement considerations and tender questionnaires. Proportionate and adequate supplier checks are made by Procurement Officers in line with the value and nature of the prospective contract.

Opportunity for improvement was found in relation to contract management processes. Although there is a Procurement and Contract Strategy in place for the Partner Councils, it is out of date and in need of review and update. Tools available to contract owners through the In-Tend Procurement Portal to monitor and manage contracts are not widely used, and training to encourage use of contract management modules on the portal has been delayed due to limited staffing resource within the Procurement Service.

According to the National Procurement Strategy 2018, research by the International Association for Contract and Commercial Management (IACCM) shows that contracts exceed their expected costs by 9.4 per cent on average over their lifetime. Poor contractor performance could seriously damage the Council's reputation and its ability to deliver

effective services and support to local communities. The absence of ongoing due diligence and contract management by contract owners throughout the life of the contract could also expose the Council to unnecessary risk in multiple areas, such as financial, legal, compliance and operational risk.

It is also noted that procedures to embed whistleblowing arrangements into contracts are weak, increasing the likelihood that fraud and misconduct will go undetected or unreported. In turn, this could expose the Council to financial and reputational risk.

Two recommendations are made within this report. The focus of recommendations made to the Council surround the need to gain assurance from Publica Group Ltd that contract management processes and controls are robust and effective.

The Publica Procurement and Contract Management audit includes a recommendation to implement a mandatory requirement that whistleblowing arrangements are drafted into contracts and are included within supporting procurement process guidance and training.

Based on the findings reported from this review, we will conduct a further audit on Management and Monitoring of Contracts as part of our 2019/20 Audit Plan.

**Publica Management Response to the Audit Findings**

In response to the Procurement and the Procurement and Contract Management audit reports issued, we plan to carry out a fundamental review of the Procurement Service. This review will include an evaluation of how the Procurement Service will integrate or work alongside the new Commissioning and Contract Management teams introduced as part of the recent service review.

| Priority | Recommendation | Management Response | Due Date |
|---|---|---|---|
| 2 | We recommend that assurance is sought from Publica that contracts held and managed on behalf of the Council are monitored and managed effectively.<br>Priority | The Joint Management Team, which includes the Publica Executive Directors and the Council's Chief Executive, Monitoring Officer and Chief Finance Officer, will monitor the implementation of internal audit recommendations made to Publica in the "Procurement and Contract Management Governance 2018/19" report and the "Procurement 2018/19" report. Implementation of the internal audit recommendations will strengthen the internal control environment. Assurance will also be sought from the follow up work to be carried out by the internal audit team during 2019/20. | 30th September 2020 |

**2018/19 Human Resources (Sickness Absence) – Reasonable Assurance**

**Background**

HR and Payroll services are a centralised function provided by Publica Group (Support) Ltd (Publica), a Council owned company to the four partner Councils Cotswold District Council (CDC), West Oxfordshire District Council (WODC), Forest of Dean District Council (FoDDC) and Cheltenham Borough Council (CBC), as well as, Ubico Ltd, Cheltenham Borough Homes (CBH) and the Cheltenham Trust.

CDC use Business World Self Service functionality for payroll related processes including sickness recording.

Testing samples were taken from Agresso Business World (ABW) from the following date range: 1st November 2017 – 31st October 2018. During this time, the sickness recorded for CDC was 212 FTE sickness days.

**Audit Conclusion / Findings**

We are pleased to offer reasonable assurance over the following processes within the HR and Payroll Service:

- Existence of a Sickness Absence Policies.
- Appropriate action following periods of sickness absence.
- Sickness absence payment and calculations.
- Sickness payments accuracy checks.

No significant risks were identified during the review, although there are areas where there is opportunity for improvement. These areas are highlighted within the report and recommendations made to improve processes have been made in the areas as described below.

A Sickness absence policy exist for the Council; however, it was noted that it had not been reviewed and updated recently. The policy should be reviewed and updated, to ensure it is in line with relevant legislation and is appropriate to the officers retained by the Council. For Publica officers based at the Council, an up to date Sickness Absence Policy is in place.

Line managers are responsible for monitoring and the reporting of sickness absence to Payroll, by way of the self-service element of the Business World system. Managers are also responsible for holding a return to work interview, completing a form to be signed by both employee and manager to be returned to HR for checking and filing. Testing found that not all forms were found on file or fully completed, and we have therefore recommended refresher training and guidance is provided following the review and update of then policy.

Controls are in place for Payroll Advisors to monitor long-term sickness absence, ensuring any amendments to pay are made in accordance with terms and conditions are captured and actioned at the correct time. Different methods are used across the team during this process; therefore, we recommend standardising the process for consistency.

Sickness variation reports are produced from the Business World System and checked by Payroll Advisors during each payroll run. The checking of these reports highlights if there is a discrepancy in pay caused by a system anomaly and enables personnel to correct the anomaly to ensure the correct payment prior to payroll authorisation and release.

| Priority | Recommendation | Management Response | Due Date |
|---|---|---|---|
| 2 | The Council's Sickness and Absence Policy should be reviewed and updated to ensure it meets the ongoing needs of the Councils | We will review the Council policy. It will be brought in line with the new Publica policy if and when the partner Council adopts the | 30th November 2019 |

| | | | |
|---|---|---|---|
| | retained staff. | new Publica terms and conditions. | |

# High Priority Recommendation Follow-Up APPENDIX D

| Audit Name | Priority | Recommendation | Management Response | Due Date | Update September 2019 |
|---|---|---|---|---|---|
| 2017/18 – Licensing | 2 | We recommend that the procedure for debt recovery for premises and club premises licences is amended to be in accordance with relevant legislation. | In accordance with the legislation the current procedure for debt recovery will be amended to ensure that Premises and Club Licences are suspended after 21 days of an invoice becoming due. ERS will request the assistance of Accounts Receivable to assist with this task. | 28/02/19 | The Service Leader (Licensing) advised that a process has put in place to monitor debt more frequently and action any suspension of licences necessary. A Technical Officer has been allocated to be responsible for this process. She reviews a debt report which is sent through to Licensing every month by Accounts Receivable. From this, she highlights to any licensing officers where payment is overdue. Officers will then complete necessary actions to retrieve the debt or investigate the issue. If no payment is forthcoming the license is suspended on the Uniform system and a letter is sent to the licence holder. Evidence of this process was provided to support this.<br><br>Recommendation has been closed |

# High Priority Recommendation Follow-Up APPENDIX D

| Audit Name | Priority | Recommendation | Management Response | Due Date | Update September 2019 |
|---|---|---|---|---|---|
| 2017/18 - Safeguarding | 2 | A process should be put in place to ensure that the Safeguarding Policy is embedded into all contracted services or to ensure that contractors have a sufficient regard for Safeguarding which is equivalent to the requirements of the authority's Safeguarding Policy. This process should include a method of gaining continued assurance that a supplier is abiding by the Safeguarding requirements of the Council. | This is a matter that can be discussed with the procurement team. It will also need to be part of discussions as part of the new contractual arrangements between CDC and Publica." | 01/04/18 | There will be a standard clause which is inserted into applicable contracts about safeguarding and would be referenced in the tendering pack. As part of the vetting process, if a contractor didn't meet the clause then they wouldn't qualify to be taken through to the next stage, where the bids are reviewed, scored, and the contract is awarded<br><br>Recommendation has been closed |

# High Priority Recommendation Follow-Up APPENDIX D

| Audit Name | Priority | Recommendation | Management Response | Due Date | Update September 2019 |
|---|---|---|---|---|---|
| 2017/18 - Safeguarding | 2 | "The 'Lead Designated Safeguarding Officer', who is accountable for the effective delivery of the Safeguarding Policy, must obtain assurance that the training requirements of the policy are met. In order to gain such assurance, it is recommended that a full review of the approach to training is undertaken for all 'employees' and Members. Focus should be given to the following:<br>- The introduction of Safeguarding into the Corporate Induction process<br>- Development of a plan for Safeguarding training for staff and Members and to include a timeframe for completing the training requirements<br>- Introduction of a method of recording staff training and understanding of training content" | The LSO, together with the Community Safety Officer, now attend induction sessions to give a presentation in respect of safeguarding and PREVENT.<br><br>A training plan/strategy is being developed that will outline training requirements for staff and councillors and how this will be delivered.<br><br>Safeguarding of children and vulnerable adults is now included on the new online training system and other courses will be added as appropriate. Details of completion of the courses will be recorded on the system." | 31/10/19 | The Corporate Lead (Claire Hughes) advised that she is in the process of developing an updated policy and training strategy and hopes this will be concluded by the end of October 2019. |

| Audit Name | Priority | Recommendation | Management Response | Due Date | Update September 2019 |
|---|---|---|---|---|---|

# High Priority Recommendation Follow-Up APPENDIX D

| Audit Name | Priority | Recommendation | Management Response | Due Date | Update September 2019 |
|---|---|---|---|---|---|
| 2018/19 Disabled Facilities Grants | 2 | The Councils should ensure all planned work is approved by an Occupational Therapist or suitably qualified substitute (if appropriate) prior to any work commencing to ensure its suitability. In addition, consideration should be given to ensuring all major adaptations are checked on completion by an Occupational Therapist or qualified surveyor, and applicant satisfaction recorded, prior to payment being approved. | The new HIA system to be implemented (for WODC) in April 2019 has a requirement for proposed and completed work to be approved built into it. It has been agreed by Foundations that provided it is written into the Regulatory Reform Order, basic works do not require OT involvement. We are researching courses and costs for Trusted Assessor Training for Officers to assist them with this decision-making process. This will speed up the process for applicants and reduce the backlog of works, thus better meeting clients' needs.<br><br>Gloucestershire County Council has deemed the completion of satisfaction questionnaires unnecessary as all customers were satisfied due to the nature of the work and therefore was creating work with no real outcomes. Satisfaction surveys are therefore not undertaken at CDC. Officers have been reminded to ensure that satisfaction certifications are obtained after completion. | 30/04/19 | Follow-up response from Commercial manager:<br>•HIA system went live w/c 06.05.19 due to delay in signing contract<br>•Trusted Assessor Level 4 training booked for 3 Officers 20/21 May 2019<br>•Meeting held with Senior Gloucestershire OT 09.05.19 to discuss future way of working with follow up meeting scheduled for 04.06.19 |

# High Priority Recommendation Follow-Up APPENDIX D

| Audit Name | Priority | Recommendation | Management Response | Due Date | Update September 2019 |
|---|---|---|---|---|---|
| 2018/19 Internal Enforcement Agency | 2 | Publica must ensure the Councils are consulted prior to any further stages of enforcement being internalised to ensure all risks can be considered by them. | Head of Revs and Bens and Business service managers are meeting to discuss a cabinet report with a view to adopting further enforcement methods. This will happen in late November/December. | 28/06/19 | This is still in draft, trying to increase to include FOD too. |
| 2018/19 Accounts Receivable | 2 | A review of all active subscriptions should be carried out, on behalf of each client, to identify any other duplicate subscriptions and these should all be corrected.<br>Priority | Agreed. This will be carried out. Additional training will also be provided to AR officers to prevent this occurring again in the future. | 31/03/19 | Will be followed up during the 2019/20 audit of Accounts Receivable |
| 2018/19 Private Water Supplies | 2 | All existing data within Uniform should be reviewed and cleansed to ensure Uniform is an accurate reflection of all Private Water Supplies registered, and that data can be easily extracted for the annual Drinking Water Inspectorate Data Return. | The Private Water Supplies data cleanse is currently underway. This involves resolving anomalies, identifying causes of missed risk assessments and sampling and ensuring all Reg 8/9/10 supplies contain accurate data and sampling triggers. | 30/06/19 | This work has been completed. As part of this project all records that were maintained outside of uniform have now been migrated.<br>Access reports have been written that allows officers to monitor the progress of RAs & sampling at each authority within a single report.<br><br>Recommendation has been closed |

# High Priority Recommendation Follow-Up APPENDIX D

| Audit Name | Priority | Recommendation | Management Response | Due Date | Update September 2019 |
|---|---|---|---|---|---|
| 2018/19 Private Water Supplies | 2 | As part of the data cleanse the service should agree a consistent approach to entering Private Water Supplies data and produce guidance documentation to assist officers | Following the data cleanse, a procedure will be written to ensure data entry is consistent allowing for a simplified Drinking Water Inspectorate extract. | 31/07/19 | Procedure notes have been produced to guide all officers entering data into Uniform. These are live documents that are discussed and reviewed as part of weekly team meetings where issues arise, or efficiencies are realised.<br><br>Recommendation has been closed |
| 2018/19 Private Water Supplies | 2 | Following the project to cleanse private water supply data within Uniform, an accurate schedule to complete all overdue and upcoming risk assessments, including realistic timeframes, should be developed that prioritises supplies based on perceived level of risk to users of those supplies. | Following the data cleanse, the Senior Officer will work with the ERS Data Analyst to produce this list to ensure work is effectively prioritised based upon risk to public health. | 30/06/19 | Reports of due/overdue RAs are produced monthly and assigned to senior officers according to their current workload.<br><br>The service has approval to employ a contractor in November to concentrate on completing RAs<br><br>Recommendation has been closed |

# High Priority Recommendation Follow-Up APPENDIX D

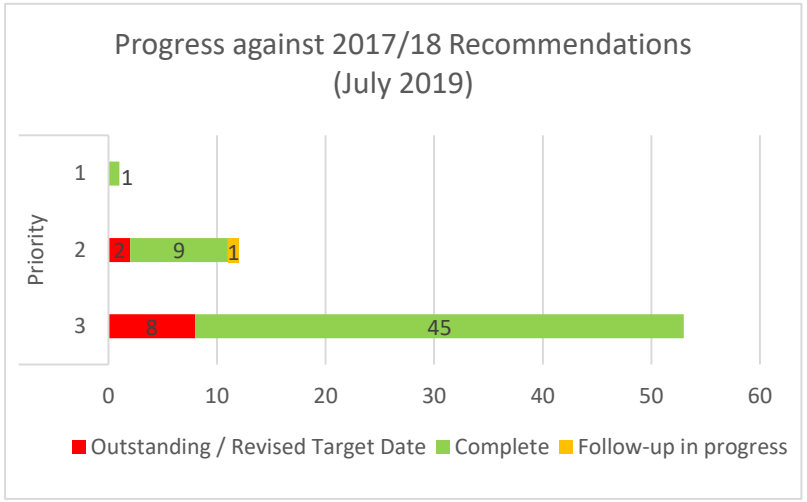
| Audit Name | Priority | Recommendation | Management Response | Due Date | Update September 2019 |
|---|---|---|---|---|---|
| 2018/19 Private Water Supplies | 2 | A review of all active private water supply entries on Uniform should be undertaken to ensure sufficient sampling visits are scheduled, according to the most resent risk assessment, for the next two years. | This action will be completed as part of the overall data cleanse plan. | 30/06/19 | This has been completed for a 12-month period. 2 years was requested as part of the audit to allow the service sufficient time to complete overdue RAs. The Senior officer gave verbal assurance this would be completed within 12 months.<br><br>Recommendation has been closed |
| 2018/19 Section 106 Agreements and Funds | 2 | All relevant internal Service areas must be involved as appropriate, at either pre-application and/or application stage to ensure evidence, impact and need are generated regarding the proposed development. Consideration should be given to creating a reference document that states when the specific Service areas / officers should be involved in the S106 consultation process and who will maintain this document. | Historically, internal Services were not invited to submit claims as the Council did not have an approved policy to support their involvement. The Local Plan was approved in December 2018. Planning Managers will continue to raise awareness of recent policy changes and apply the Development Team Approach at the earliest stage, which will ensure all interested parties are included. Furthermore, regular meetings will be held with relevant Service areas to gain feedback from consultees over the consultation process. | 31/07/19 | Officers responsible for agreeing, recording and monitoring S106 at FoDDC, CDC & WODC met 23/09/19 to discuss strategies for aligning best practice across the partner councils.<br><br>Audit are due to follow-up the outcomes of this meeting in October 2019. |

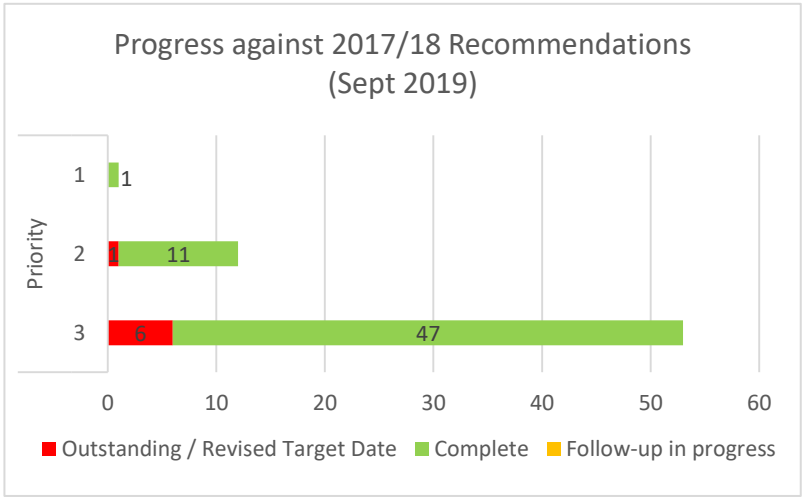
# High Priority Recommendation Follow-Up APPENDIX D

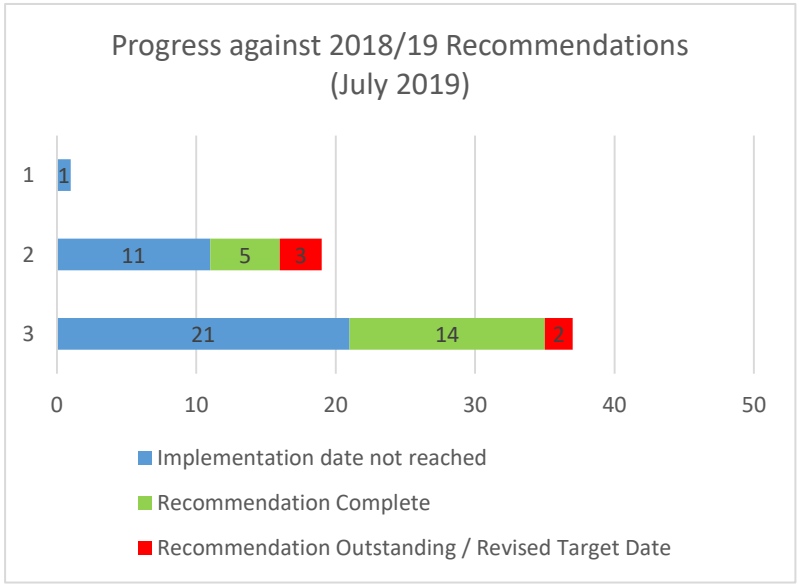
| Audit Name | Priority | Recommendation | Management Response | Due Date | Update September 2019 |
|---|---|---|---|---|---|
| 2018/19 Section 106 Agreements and Funds | 1 | To ensure all S106 Agreements and financial contributions can be monitored, an overarching S106 record should be maintained, to include: covenants, clauses, triggers and payments. The use of the tick box in Uniform should also be reviewed to assess whether this adds value to the Service and the records it maintains. | We will ensure the implementation of CIL includes a system for monitoring S106s. Prior to this being implemented, quarterly S106 monitoring meetings will be held with the S106 Development team. The Governance arrangements of this team will be developed following the conclusion of the audit. | 31/07/19 | As above |
| 2018/19 Section 106 Agreements and Funds | 2 | To ensure there is a full audit trail and financial contributions are consistently managed, developers should be invoiced for financial contributions once the relevant trigger has been reached. In addition, evidence that 3rd parties spend contributions in accordance with the agreement, or an itemised invoice, should be obtained prior to issuing payments to 3rd parties. | Officers will liaise with officers at WODC and FODDC to agree a consistent approach to recording and invoicing, and the submission of evidence from 3rd parties. | 31/07/19 | As above |
| 2018/19 Section 106 Agreements and Funds | 2 | To ensure the Council can be held to account in managing the delivery of S106 obligations, the progress of S106 Agreements should be regularly reported to all Members and on the Council's website | Portfolio holders will be regularly updated going forward. Once CIL has been implemented, the CIL system will aide with the reporting of S106s to Members and on the Council's webpages will also be developed to allow the delivery of S106s to be reported there. | 31/07/19 | As above |
| 2018/19 Housing Benefit and Council Tax Support | 2 | Remind Benefit Officers that all claims must be correctly updated to ensure information displayed and held in Northgate is correct. Priority | Legislative changes have been clearly identified and guidance issued to ensure officers are aware as to how claims for Housing Benefit are affected in order to prevent further overpayments arising during assessment. | 30/09/19 | Will be followed up as part of the 2019/20 audit |

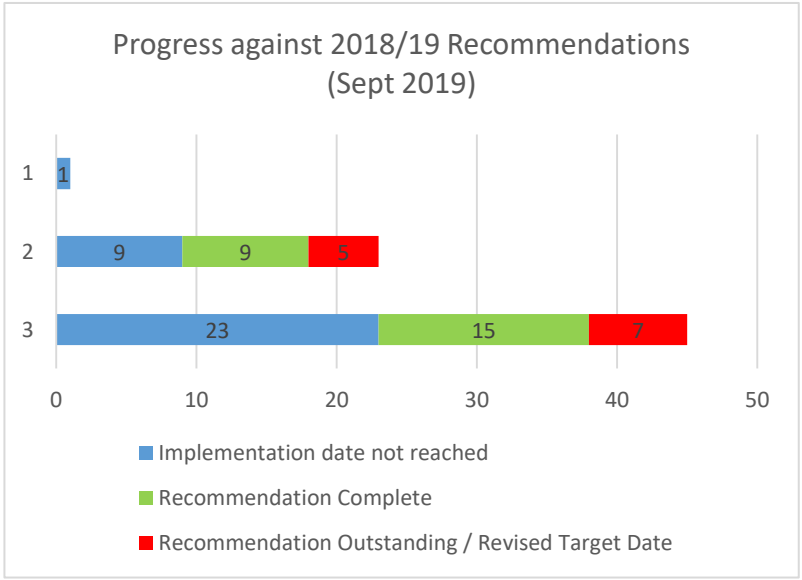
# High Priority Recommendation Follow-Up APPENDIX D

| Audit Name | Priority | Recommendation | Management Response | Due Date | Update September 2019 |
|---|---|---|---|---|---|
| 2018/19 Subsidy Claims | 2 | Increased quality assurance should be undertaken in the areas where errors were found in the 2017/18 Subsidy Claim calculation, to mitigate against issues resulting from local authority error. | We already check a proportion of these claims, but moving forward there will be a closer monitoring and increase in QA in these areas | 29/09/19 | |
| | | | | | |


Progress against 2017/18 Recommendations
(July 2019)
Priority
1
2
3
1
2
9
1
8
45
0
10
20
30
40
50
60
Outstanding / Revised Target Date
Complete
Follow-up in progress


Progress against 2017/18 Recommendations
(Sept 2019)
Priority
1
2
3
1
1
11
6
47
0
10
20
30
40
50
60
Outstanding / Revised Target Date
Complete
Follow-up in progress


Progress against 2018/19 Recommendations
(July 2019)
1
2
3
1
11
5
3
21
14
2
0
10
20
30
40
50
Implementation date not reached
Recommendation Complete
Recommendation Outstanding / Revised Target Date


Progress against 2018/19 Recommendations
(Sept 2019)
1
2
3
1
9
9
5
23
15
7
0
10
20
30
40
50
Implementation date not reached
Recommendation Complete
Recommendation Outstanding / Revised Target Date

COTSWOLD DISTRICT COUNCIL

| | |
|---|---|
| Council name | **COTSWOLD DISTRICT COUNCIL** |
| Name and date of Committee | **AUDIT COMMITTEE – 14 NOVEMBER 2019** |
| Report Number | **AGENDA ITEM 12** |
| Subject | **COUNTER FRAUD UNIT REPORT** |
| Wards affected | All indirectly |
| Accountable member | Cllr Mike Evemy, Deputy Leader and Cabinet Member for Finance<br>Tel: 07850 373022 Email: Mike.Evemy@cotswold.gov.uk |
| Accountable officer | Emma Cathcart, Counter Fraud Manager<br>Tel: 01285 623356 Email: Emma.Cathcart@cotswold.gov.uk |
| Summary/Purpose | To provide the Audit Committee with assurance over the counter fraud activities of the Council. The Counter Fraud Unit will continue to provide Audit Committee with direct updates biannually.<br>Work plans are presented to the Audit Committee detailing progress and results for consideration and comment as the body charged with governance in this area.<br>The report also provides the Audit Committee with two Policies, for comment, in relation to the Regulation of Investigatory Powers Act 2000, the Investigatory Powers Act 2016 and the Council's existing Policies and arrangements. |
| Annexes | Annex A – Work Plan 2019/2020<br>Annex B – Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy (draft)<br>Annex C – Investigatory Powers Act 2016 Acquisition of Communications Data Policy (draft) |
| Recommendation/s | Please write recommendations using letters and italics as below.<br>a) *That the Audit Committee notes the report and the work plan and makes comment as necessary.*<br>b) *That the Audit Committee considers the Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy to comment thereon to Cabinet, to aid its deliberations and decision making.* |

| | |
|---|---|
| | *c) That the Audit Committee considers the Investigatory Powers Act 2016 Acquisition of Communications Data Policy to comment thereon to Cabinet, to aid its deliberations and decision making.* |
| Corporate priorities | Ensure that all services delivered by the Council are delivered to the highest standard. |
| Key Decision | NO |
| Exempt | NO |
| Consultees/ Consultation | The Policies have been reviewed by the Legal Team and have been issued to Governance Group and Joint Management Team for comment. |

## 1. BACKGROUND

**1.1.** The Audit Committee oversees the Council's counter fraud arrangements and it is therefore appropriate for the Committee to be updated in relation to counter fraud activity.

**1.2.** Work plans for 2019/20 have been agreed with the Chief Finance Officer and Corporate Management and work is underway. The Audit Committee, as the body charged with governance in this area, is presented with a copy of the work plan for information.

**1.3.** Attached at Annex A is a copy of the work plan for 2019/2020.

## 2. MAIN POINTS

### 2.1. Counter Fraud Unit Update.

**2.2.** The Serious and Organised Crime Strategy (2013) introduced by government, raised concerns about the vulnerability of public procurement to organised crime. The Home Office conducted a pilot programme to explore the threat and produced a report detailing findings which showed areas such as waste, taxi and transport services and lower level spend are particularly at risk. The report suggested interventions which included the completion of a high level checklist to identify risks. The Counter Fraud Unit (CFU) have completed the checklist in relation to serious and organised crime and issued a copy to Governance Group for consideration. This piece of work has resulted in an action plan to raise awareness and review controls in areas of high risk such as procurement and housing.

**2.3.** The Counter Fraud and Anti-Corruption Policy has been reviewed and minor amendments were made to reflect changes to data protection legislation.

**2.4.** In addition to Annex A, as a dedicated investigatory support service, the CFU undertakes a wide range of enforcement and investigation work according to the requirements of each Council. This includes criminal investigation and prosecution support for enforcement teams, investigations into staff/member fraud and corruption, or tenancy and housing fraud investigation work. As at the beginning of the year, the CFU had 7 open cases. During Quarters 1 and 2:

- The team received 11 referrals from across the Council and closed 6 cases.
- The team undertake disciplinary investigations for Publica across the partnership. 5 cases have been referred and 2 cases have been closed during the period. Both of the closed cases resulted in disciplinary hearings; a final written warning was issued and a member of staff was dismissed for gross misconduct.
- Assisting the Planning, Heritage and Conservation Teams. The work undertaken by Council's Conservation Officer and the Counter Fraud Unit resulted in legal services being able to successfully prosecute a guilty plea under the Planning (Listed Buildings and Conservation Areas) Act 1990 for unlawful works to a II* listed building. The defendant received a fine of £20,000 and was ordered to pay £5,651 towards the Council's costs.

- Assisting the Parking Services Team. The work undertaken by the Council's Projects and Contracts Officer and the Counter Fraud Unit resulted in the successful listing of a fraud case at Cheltenham Magistrates Court. The defendant failed to attend and a warrant without bail has been issued.

**2.5. Regulation of Investigatory Powers Act 2000 / Investigatory Powers Act 2016 Policies**

**2.6.** The Council's Policies are based on the legislative requirements of these Acts and the Codes of Practice relating to directed surveillance and the acquisition of communications data. Attached at Annex B and at Annex C, are revised draft Policies.

**2.7.** The Investigatory Powers Act 2016 now governs communication data requests. The legislation widened the scope of information the Council may obtain for investigations, introduced the necessity for a serious crime threshold and removed the requirement for judicial approval.

**2.8.** All applications for communications data are made online via the National Anti-Fraud Network (NAFN) which acts as the single point of contact for Councils. NAFN send requests to the Office for Communication Data Authorisations (OCDA) who ratify all applications from public authorities for approval and if granted, NAFN will then obtain the requested data for the applicant.

**2.9.** There is a requirement for the Council to nominate a Designated Senior Officer who will confirm to NAFN that the Council is aware of any request and approve its submission. This role is undertaken by the Counter Fraud Manager and the Deputy Counter Fraud Manager.

**2.10.** Surveillance and the use of a Covert Human Intelligence Source (CHIS) is still governed by the Regulation of Investigatory Powers Act 2000 (RIPA) and any applications are subject to the same application processes as outlined in the previous Policy – the offence must meet the serious crime threshold and the Council must obtain judicial approval.

**2.11.** The Council must have a Senior Responsible Officer and Authorising Officers to approve the application before the Court is approached. These roles are as outlined in the Counter Fraud Unit Audit Committee Report April 2019.

**2.12.** The refreshed Policy introduces a mandatory requirement for staff to complete a Non-RIPA Application Form where surveillance is being undertaken but the offence does not meet the serious crime criteria.

**2.13.** The work plan and reactive case results are presented for information and comment.

**2.14.** The Policies relating to surveillance, the use of a CHIS and the acquisition of communications data have been updated in line with legislative changes and are presented to Audit Committee for comment thereon.

## 3. FINANCIAL IMPLICATIONS

**3.1.** The report details financial savings generated by the Counter Fraud Unit.

**3.2.** The adoption and approval of these Policies will support the Council's objectives in reducing crime and financial loss to the Council.

## 4. LEGAL IMPLICATIONS

**4.1.** In general terms, the existence and application of an effective fraud risk management regime assists the Council in effective financial governance which is less susceptible to legal challenge.

**4.2.** The Council is required to ensure that it complies with the Regulation of Investigatory Powers Act 'RIPA' 2000, the Investigatory Powers Act 2016 and any other relevant/statutory legislation regarding investigations. Any authorisations for directed/covert surveillance or the acquisition of communications data undertaken should be authorised by the appropriate Officer and recorded in the Central Register.

**4.3.** The Council has a statutory obligation for enforcing a wide range of legislation, where it is necessary and proportionate to do so. Human rights implications are a consideration of this type of activity and this is included within the Policy.

## 5. RISK ASSESSMENT

**5.1.** The Council is required to proactively tackle fraudulent activity in relation to the abuse of public funds. The Counter Fraud Unit provides assurance in this area.

**5.2.** Failure to undertake such activity would accordingly not be compliant and expose the authority to greater risk of fraud and/or corruption.

**5.3.** If the Council does not have effective counter fraud and corruption controls it risks both assets and reputation.

**5.4.** The Policies demonstrate the Council's consideration of necessity, proportionality and public interest when deciding on surveillance activity or the decision to obtain personal communication data.

## 6. EQUALITIES IMPACT

**6.1.** The promotion of effective counter fraud controls and a zero tolerance approach to internal misconduct promotes a positive work environment.

**6.2.** The application of these Policies, to govern surveillance and the obtaining of personal communications data, ensures that there is less risk that an individual's human rights will be breached. Furthermore it protects the Council from allegations of the same.

## 7. ALTERNATIVE OPTIONS

**7.1.** The Council is the lead authority for the Gloucestershire Counter Fraud Unit. This Unit is working with all of the Gloucestershire Local Authorities, West Oxfordshire District Council and other public sector bodies such as housing associations.

## 8. BACKGROUND PAPERS - NONE

## ANNEX A – Cotswold District Council Work Plan 2019/2020

| Department / Contact | Task | Dates / Notes |
|---|---|---|
| Corporate / Strategy | Delivery of two reports for Audit Committee | April & November |
| Corporate / Strategy | RIPA Coordinator Role - Review of Policies / annual report to Members / advisory role for staff | Annual update - April<br>3 Policies reviewed and redrafted - Social Media Policy to Governance Group December<br>Role decisions complete and IPCO updated<br>Draft Surveillance and Communications Policy issued to Legal, Audit Committee November & Cabinet December |
| Corporate / Strategy | Home Office Serious and Organised Crime Checklist and accompanying work plan | Draft issued to Governance Group – June / completed September for cascade to managers and work plan implementation |
| Corporate / Strategy | Home Office Bribery and Corruption Assessment Template and accompanying work plan | Draft commenced |
| Corporate / Strategy | Development / Review of Fraud Response Plan | Q4 - SOC consideration |
| Corporate / Strategy | Review Corporate Risk Register | Q3 - SOC consideration / SWAP recommendation Fighting Fraud & Corruption 1.1.1a |
| Corporate / Strategy | Development of Fraud awareness literature for staff and members | Q3 |
| Corporate / Strategy | Development of RTB / debt recovery process | |
| Corporate / Strategy | Staff and Members Fraud Awareness Sessions | April - July – complete |
| Corporate / Strategy | Collation and Publication of Fraud Transparency Data | Published August |
| Procurement | Assist with review of Procurement and Contract Strategy | Q3 / Q4 - SOC consideration / SWAP recommendation Fighting Fraud & Corruption 1.1.2a |
| Procurement | Supplier payment review | Q3 / Q4 |
| SWAP | Policy and Procedure: Staff Declarations of Interest / Conflicts of Interest | Q3 / Q4 - SOC consideration / SWAP recommendations Members' and Officers' Gifts, Hospitality and Declarations |
| SWAP | Review of the Gifts and Hospitality Policy and Procedure | Q3 / Q4 - SOC consideration / SWAP recommendations Members' and Officers' Gifts, Hospitality and Declarations |
| HR | Review of HR Recruitment and Vetting Policy and Procedures | Q3 - SOC consideration |
| Policy | Drafting / consultation / adoption of Money Laundering Policy | Q4 |
| Revenues and Housing | National Fraud Initiative (NFI) Match Review | Commenced September |
| Revenues and Housing | NNDR (Business Rates) Charity Shop Review | Q4 |
| Revenues and Housing | Review of the Housing List and related NFI Data Matches | Commenced September |
| Planning | Waterpark Review | Instruction to Legal |
| ERS | Licensing / Invoice Review | Q3 |

SOC = Serious and Organised Crime / IPCO = Investigatory Powers Commissioner's Office

| Version Control: | |
|---|---|
| **Document Name:** | Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy |
| **Version:** | 2 |
| **Responsible Officer:** | Emma Cathcart, Counter Fraud Unit |
| **Approved by:** | Cabinet |
| **Date First Approved:** | TBC |
| **Next Review Date** | |
| **Retention Period:** | N/A |

**Revision History**

| Revision date | Version | Description |
|---|---|---|
| April 2019 | 2 | Change in legislation / introduction of IPA 2016 |
| | | |

**Consultees**

| Internal | External |
|---|---|
| Audit Committee | |
| Legal Department | |
| Corporate Management | |

**Distribution**

| Name | |
|---|---|
| Enforcement Officers | |
| | |

**CONTENTS**

1. INTRODUCTION ....4
2. SCOPE OF POLICY ....4
3. BACKGROUND ....4
4. SURVEILLANCE WITHOUT RIPA ....5
5. INDEPENDENT OVERSIGHT ....5
6. LEGAL ADVICE ....6
7. REVIEW OF POLICY AND PROCEDURE ....6
8. RIPA ROLES AND RESPONSIBILITIES ....6
8.1 THE SENIOR RESPONSIBLE OFFICER ....6
8.3 THE RIPA COORDINATOR ....7
8.6 INVESTIGATING OFFICER/APPLICANT ....7
8.9 AUTHORISING OFFICERS ....7
9. SURVEILLANCE TYPES AND CRITERIA ....9
9.4 OVERT SURVEILLANCE ....9
9.6 COVERT SURVEILLANCE ....9
9.9 INTRUSIVE SURVEILLANCE ....9
9.14 DIRECTED SURVEILLANCE ....10
10. PRIVATE INFORMATION ....10
11. CONFIDENTIAL OR PRIVILEGED MATERIAL ....11
12. INTERNET AND SOCIAL MEDIA INVESTIGATIONS ....11
13. CCTV ....11
14. AUTOMATIC NUMBER PLATE RECOGNITION (ANPR) ....12
15. JOINT AGENCY SURVEILLANCE ....12
16. USE OF THIRD PARTY AGENTS ....12
17. EQUIPMENT ....12
18. COVERT HUMAN INTELLIGENCE SOURCES (CHIS) ....13
18.9 DEFINITION OF CHIS ....13
18.19 VULNERABLE CHIS ....14
18.24 USE OF EQUIPMENT BY A CHIS ....15
18.27 CHIS MANAGEMENT ....15
18.30 CHIS RECORD KEEPING ....15
19. NECESSITY ....16
20. PROPORTIONALITY ....16
21. COLLATERAL INTRUSION ....17
22. THE APPLICATION AND AUTHORISATION PROCESS ....17
22.2 DURATION OF AUTHORISATIONS ....17

22.5 APPLICATIONS/AUTHORISATION....18
22.15 ARRANGING THE COURT HEARING....18
22.18 ATTENDING THE HEARING....19
22.23 DECISION OF THE JP....19
22.32 POST COURT PROCEDURE....20
22.35 MANAGEMENT OF THE ACTIVITY....20
22.37 REVIEWS....20
22.44 RENEWAL....21
22.52 CANCELLATION....21
23. SURVEILLANCE OUTSIDE OF RIPA....22
24. SAFEGUARDING AND THE USE OF SURVEILLANCE MATERIAL....23
24.2 AUTHORISED PURPOSE....23
24.1 USE OF MATERIAL AS EVIDENCE....23
24.6 HANDLING AND RETENTION OF MATERIAL....23
24.13 DISSEMINATION OF INFORMATION....24
24.17 STORAGE....24
24.19 COPYING....25
24.22 DESTRUCTION....25
25. ERRORS....25
25.2 RELEVANT ERROR....25
25.6 SERIOUS ERRORS....25
26. COMPLAINTS....26

## 1. INTRODUCTION

1.1 The performance of certain investigatory functions by Local Authorities may require the surveillance of individuals or the use of undercover Officers and informants. Such actions may intrude on the privacy of individuals and can result in private information being obtained and as such, should not be undertaken without full and proper consideration. The Regulation of Investigatory Powers Act 2000 (RIPA) regulates these types of activities and the Act and this Policy must be followed at all times.

1.2 Neither RIPA nor this Policy covers the use of any overt surveillance, or general observation that forms part of the normal day to day duties of Officers, or circumstances where members of the public volunteer information to the Council. The majority of the Council's enforcement functions are carried out in an overt manner.

1.3 RIPA was introduced to ensure that public authorities' actions are consistent with the Human Rights Act 1998 (HRA). It balances safeguarding the rights of the individual against the needs of society as a whole to be protected from crime and other public safety risks. This reflects the requirements of Article 8 (right to privacy) under the HRA. RIPA provides a statutory mechanism for authorising covert surveillance and the use of a covert human intelligence source (CHIS).

1.4 RIPA also introduced a legal gateway for public authorities to apply for telecommunications and postal data. However, these have been amended by the Investigatory Powers Act 2016 (IPA), and for guidance in relation to the obtaining of Communications Data please see the IPA Acquisition of Communications Data Policy.

## 2. SCOPE OF POLICY

2.1 The purpose of this document is to ensure that the Council complies with RIPA.

2.2 This document provides guidance on the regulation of any Directed Covert Surveillance that is carried out by the Council. This includes the use of undercover Officers and informants, known as Covert Human Intelligence Sources (CHIS).

2.3 Covert surveillance will only be used by the Council where it judges such use to be necessary and proportionate to the seriousness of the crime or matter being investigated.

2.4 All directed surveillance must be authorised and conducted in accordance with RIPA. Therefore, all Officers involved in the process must have regard to this document and the statutory Codes of Practice issued under section 71 RIPA. The Codes of Practice are available from:

https://www.gov.uk/government/collections/ripa-codes#current-codes-of-practice

2.5 There must be no situation where a Council Officer engages in covert surveillance without obtaining authorisation in accordance with the procedures set out in this document and the RIPA Codes of Practice.

2.6 Any queries concerning the content of the document should be addressed to the RIPA Coordinator, Counter Fraud Unit.

## 3. BACKGROUND

3.1 RIPA provides a legal framework for the control and regulation of covert surveillance techniques which public authorities undertake as part of their duties. As was highlighted in the introduction to this Policy, the need for such control arose as a result of the HRA. Article 8 of the European Convention on Human Rights states that:-

1) Everyone has the right of respect for his private and family life, his home and his correspondence.

2) There shall be no interference by a Public Authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protection of the rights and freedoms of others.

3.2 The right under Article 8 is a qualified right and public authorities can interfere with this right for the reasons given in 2.3 above. RIPA provides the legal framework for lawful interference.

3.3 However, under RIPA, Local Authorities can only authorise directed covert surveillance for the purpose of preventing or detecting conduct which constitutes a criminal offence which is:

- An offence that is capable of attracting a maximum prison sentence of 6 months or more punishable whether on summary conviction or indictment meets the serious crime threshold or,
- Relates to the underage sale of alcohol or tobacco.

3.4 Furthermore, the Council's authorisation can only be given effect once an Order approving the authorisation has been granted by a Justice of the Peace (JP).

3.5 The serious crime criteria do not apply to CHIS authorisations.

3.6 RIPA ensures that any surveillance undertaken following a correct authorisation and approval from a JP is lawful and therefore protects the Council from legal challenge. It allows the information obtained to be used as evidence in the investigation. It can also be used if required in other investigations.

## 4. SURVEILLANCE WITHOUT RIPA

4.1 Section 27 of RIPA provides that surveillance shall be lawful for all purposes if authorised and conducted in accordance with an authorisation granted under RIPA.

4.2 Lawful surveillance is exempted from civil liability.

4.3 Although not obtaining authorisation does not make the surveillance unlawful per se, it does have some consequences:-

- Evidence that is gathered may be inadmissible in court;
- The subjects of surveillance can bring their own proceedings or defeat proceedings brought by the Council against them on human rights grounds i.e. we have infringed their rights under Article 8;
- If a challenge under Article 8 is successful, the Council could face a claim for financial compensation;
- The Government has also introduced a system of tribunal to deal with complaints. Any person who believes that their rights have been breached can have their complaint dealt with by the Investigatory Powers Tribunal (IPTC) (See Complaints section within the Code of Practice)

## 5. INDEPENDENT OVERSIGHT

5.1 From 1 September 2017 oversight of RIPA is provided by the Investigatory Powers Commissioner's Office (IPCO). They are the independent inspection office whose remit includes providing comprehensive oversight of the use of the powers to which the RIPA

Codes of Practice apply, and adherence to the practices and processes described in it. They also provide guidance to be followed which is separate to the codes.

5.2 Anyone, including anyone working for the Council, who has concerns about the way that investigatory powers are being used, may report their concerns to the IPCO

5.3 IPCO has unfettered access to all locations, documentation and information systems as is necessary to carry out its full functions and duties and it will periodically inspect the records and procedures of the Council to ensure the appropriate authorisations have been given, reviewed, cancelled, and recorded properly.

5.4 It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information required for the purpose of enabling them to carry out their functions.

5.5 It is important that the Council can show it complies with this Policy and with the provisions of RIPA.

## 6. LEGAL ADVICE

6.1 The Council's legal representatives will provide legal advice to staff making, renewing or cancelling authorisations. Requests and responses for legal advice will be in writing and copied to the RIPA Coordinator, Counter Fraud Unit to keep on file.

## 7. REVIEW OF POLICY AND PROCEDURE

7.1 The Audit Committee will receive annual reports regarding the use of RIPA. Those reports will contain information on:

- Where and when the powers have been used;
- The objective;
- The authorisation process;
- The job title of the Senior Responsible Officer (SRO), Authorising Officers (AO) and RIPA Coordinator;
- The outcomes including any legal court case;
- Any costs.

## 8. RIPA ROLES AND RESPONSIBILITIES

8.1 THE SENIOR RESPONSIBLE OFFICER

8.2 The SRO has responsibility for the following:

- The integrity of the process in place within the Council to authorise Directed and Intrusive Surveillance;
- Compliance with the relevant sections of RIPA and the Codes of Practice;
- Oversight of the reporting of errors to the Investigatory Powers Commissioner (IPC) and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the IPCO and the inspectors who support the IPC when they conduct their inspections;

- Where necessary, overseeing the implementation of any recommended post-inspection action plans and;
- Ensuring that all AO are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the IPC.

8.3 THE RIPA COORDINATOR

8.4 The RIPA Coordinator is responsible for storing all the original authorisations, reviews, renewals and cancellation forms and the signed approval or refusal documentation from the JP. This will include any authorisations that have not been authorised by the AO or refused by a JP.

8.5 The RIPA Coordinator will:

- Keep the copies of the forms for a period of at least 3 years;
- Keep the Central Register (a requirement of the Codes of Practice) of all of the authorisations, renewals and cancellations; and issue a unique reference number. This record should contain the information outlined within the Covert Surveillance and Property Interference revised Code of Practice;
- Keep a database for identifying and monitoring expiry dates and renewal dates;
- Along with Officers (AO and Investigating Officers (IO)), ensure that any electronic and paper records relating to a RIPA investigation are used, retained or destroyed in line with the Council's Information Management Policies, Departmental Retention Schedules and Data Protection Legislation /Regulations;
- Provide administrative support and guidance on the processes involved;
- Not provide legal guidance or advice;
- Monitor the authorisations, renewals and cancellations with a view to ensuring consistency throughout the Council;
- Monitor each department's compliance and act on any cases of non-compliance;
- Provide training and further guidance and awareness of RIPA and the provisions of this Policy; and review the contents of this Policy.

8.6 INVESTIGATING OFFICER/APPLICANT

8.7 The applicant is normally an IO who completes the application section of the RIPA form. IOs should think about the need to undertake directed surveillance or the use of a CHIS before they seek authorisation. IOs must consider whether they can obtain the information by using techniques other than covert surveillance. Advice can be given by the RIPA Coordinator.

8.8 The applicant or IO must carry out a feasibility study and this should be seen by the AO. The IO seeking authorisation should then complete the application form having regard to the guidance given in this Policy and the statutory Codes of Practice. There should not be any significant delay between the feasibility study and the completion of the application form in order to ensure that the details within the application are accurate. The form should then be submitted to the AO for authorisation.

8.9 AUTHORISING OFFICERS

8.10 The role of the AO is to authorise, review, renew and cancel directed surveillance.

8.11 AOs should not be responsible for authorising investigations or operations in which they are directly involved. Where an AO authorises such an investigation or operation the Central Record of Authorisations should highlight this, and it should be brought to the attention of the ICO or Inspector during their next inspection.

8.12 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that for the Council, the AO shall be a Director, Head of Service, Service Manager or equivalent as distinct from the Officer responsible for the conduct of an investigation.

8.13 A designated AO must qualify both by rank and by competence. Officers who wish to be designated must have been trained to an appropriate level in order to have an understanding of RIPA and the requirements that must be satisfied before an authorisation can be granted.

8.14 Authorisations must be given in writing by the AO by completing the relevant section on the authorisation form. Before giving authorisation for directed surveillance, an AO must be satisfied that the reason for the request is for the prevention and detection of crime and that the crime attracts a custodial sentence of a maximum of 6 months or more, or is an offence relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

8.15 The lawful criteria for CHIS are prevention and detection of crime and prevention of disorder and the offence does not have to have a sentence of 6 months imprisonment but consideration must be given to the risk of collateral intrusion (the risk of obtaining private information about persons who are not the subject of investigation), the possibility of collecting confidential personal information and that the result cannot reasonably be achieved by any other means.

8.16 When completing an authorisation, the case should be presented in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the authorisation.

8.17 The application should explain why the activity is both necessary and proportionate, having regard to the collateral intrusion. It should also explain exactly what is being authorised, against whom, in what circumstances, where and so on, and that the level of the surveillance is appropriate to achieve the objectives. It is important that this is very clear as the surveillance operatives will only be able to carry out activity that has been authorised. This will assist with avoiding errors.

8.18 If any equipment such as covert cameras are to be used, the AO should know the capability of the equipment before authorising its use. This will have an impact on collateral intrusion, necessity and proportionality. It is important that they consider all the facts to justify their decision and that it is not merely a rubber-stamping exercise.

8.19 The AO may be required to attend court to explain what has been authorised and why. Alternatively, they may have to justify their actions at a tribunal. AOs are also responsible for carrying out regular reviews of applications, for authorising renewals and cancelling any authorisation (see relevant sections below).

8.20 AOs must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA and the current Procedures and Guidance issued by the Commissioner. This document also details the latest operational guidance to be followed. It is recommended that AOs hold their own copy of this document.

8.21 AOs, through the Council's Data Controller, must ensure compliance with the appropriate data protection requirements under data protection legislation and regulation and any relevant internal protocols of the Council relating to the handling and storage of material.

## 9. SURVEILLANCE TYPES AND CRITERIA

9.1 Surveillance is:

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.
- Recording anything monitored, observed or listened to in the course of surveillance, with or without the assistance of a device.

9.2 By its very nature, surveillance may involve invading an individual's right to privacy. The level of privacy which individuals can expect depends upon the nature of the environment they are within at the time. For example, within an individual's own home or private vehicle, an individual can expect the highest level of privacy. The level of expectation of privacy may reduce if the individual transfers out into public areas.

9.3 There are different types of surveillance which, depending on their nature, are either allowable or not allowable and that require different degrees of authorisation and monitoring under RIPA.

9.4 OVERT SURVEILLANCE

9.5 Overt surveillance is where the subject of surveillance is aware that it is taking place. This could be by way of signage, such as in the use of CCTV, or because the subject of the surveillance has been informed of the activity. Overt surveillance is outside the scope of RIPA and therefore does not require authorisation. However, it still must take account of privacy under the HRA.

9.6 COVERT SURVEILLANCE

9.7 Covert Surveillance is defined as "surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place" and is covered by RIPA. Covert surveillance is categorised as either intrusive or directed.

9.8 There are three categories of covert surveillance regulated by RIPA:

1) **Directed Surveillance;**
2) **Covert Human Intelligence Sources** (CHIS); and
3) **Intrusive surveillance** (the Council is not permitted to carry out intrusive surveillance).

9.9 INTRUSIVE SURVEILLANCE

9.10 The Council has no authority in law to carry out Intrusive Surveillance. Intrusive surveillance is defined in section 26(3) of RIPA as covert surveillance that:

- Is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

9.11 Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. Thus, an observation

post outside premises, which provides a limited view and no sound of what is happening inside the premises, would not be considered as intrusive surveillance.

9.12 A risk assessment of the capability of equipment being used for surveillance of residential premises and private vehicles should be carried out to ensure that it does not fall into intrusive surveillance.

9.13 If you are considering conducting surveillance that may fall within the scope of intrusive surveillance you must contact the RIPA Coordinator for clarification or seek legal advice from the legal department before you undertake any surveillance.

9.14 DIRECTED SURVEILLANCE

9.15 Surveillance is directed surveillance within RIPA if the following are applicable:

- It is covert, but not intrusive surveillance;
- It is conducted for the purposes of a specific investigation or operation;
- It is likely to result in the obtaining of private information (see private information below) about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- It is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought.
- The offence under investigation attracts a maximum custodial sentence of six months, or it is an investigation into criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

## 10. PRIVATE INFORMATION

10.1 The Code of Practice provides guidance on the definition of private information and states it includes any information relating to a person's private or family life. As a result, private information is capable of comprising any aspect of a person's relationship with others including family and professional or business relationships.

10.2 Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public.

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

10.4 Surveillance of publicly accessible areas of the internet should be treated in a similar way particularly when accessing information on social media websites. (See the Internet and Social Media Research and Investigations Policy for further guidance)

10.5 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish a pattern of behaviour. Consideration must be given if one or more pieces of information (whether or not available in the public domain) are covertly and / or overtly obtained for the purpose of making a permanent record about

a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorisation may be considered appropriate.

10.6 Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate

## 11. CONFIDENTIAL OR PRIVILEGED MATERIAL

11.1 Particular consideration should be given in cases where the subject of the investigation or operation might reasonably assume a high degree of confidentiality. This includes where the material contains information that is legally privileged; confidential journalistic material or where material identifies a journalist's source; or material containing confidential personal information or communications between a Member of Parliament and another person on constituency business. Directed surveillance likely or intended to result in the acquisition of knowledge of confidential or privileged material must be authorised by the SRO. Advice should be sought from the RIPA Coordinator and the Legal Department if there is a likelihood of this occurring.

## 12. INTERNET AND SOCIAL MEDIA INVESTIGATIONS

12.1 Online open source research is widely regarded as the collection, evaluation and analysis of material from online sources available to the public, whether by payment or otherwise to use as intelligence and evidence.

12.2 The use of online open source internet and social media research techniques has become a productive method of obtaining information to assist the Council with its regulatory and enforcement functions. It can also assist with service delivery issues and debt recovery. However, the use of the internet and social media is constantly evolving and with it the risks associated with these types of enquiries, particularly regarding breaches of privacy under Article 8 Human Rights Act (HRA) and other operational risks. The activity may also require RIPA authorisations for Directed Surveillance or CHIS. Where this is the case, the application process and the contents of this policy are to be followed.

12.3 There is a detailed Internet and Social Media Research and Investigations Policy that covers online open source research which should be read and followed in conjunction with this policy.

## 13. CCTV

13.1 The use of the CCTV systems operated by the Council does not normally fall under the RIPA regulations. However, it does fall under the data protection legislation and regulations, the Surveillance Camera Code 2013 and the Council's CCTV Policy. However, should there be a requirement for the CCTV cameras to be used for a specific purpose to conduct surveillance it is likely that the activity will fall under directed surveillance and therefore require an authorisation under RIPA. The Council's CCTV Policy and Procedures should be referred to.

13.2 If an IO envisages using any other CCTV system they should contact the RIPA Coordinator concerning any clarification on the administrative process or seek legal advice before they undertake any surveillance.

## 14. AUTOMATIC NUMBER PLATE RECOGNITION (ANPR)

14.1 Automated Number Plate Recognition (ANPR) does not engage RIPA if it is used for the purpose it is registered for, such as traffic flow management or safety and enforcement within car parks. However, it is capable of being a surveillance device if used in a pre-planned way to carry out surveillance by monitoring a particular vehicle or by plotting its locations, e.g. in connection with illegally disposing of waste.

14.2 Should it be necessary to use the Police ANPR systems to monitor vehicles, the same RIPA principles apply regarding when a directed surveillance authorisation should be sought.

## 15. JOINT AGENCY SURVEILLANCE

15.1 In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the Police. If it is a joint operation involving both agencies, the lead agency should seek authorisation.

15.2 Council staff involved with joint agency surveillance must ensure that all parties taking part are authorised on the form to carry out the activity. When Council Officers are operating on another organisation's authorisation they are to ensure they see what activity they are authorised to carry out and make a written record. They should also provide a copy of the authorisation to the RIPA Coordinator at the Council to assist with oversight and monitoring.

## 16. USE OF THIRD PARTY AGENTS

16.1 In some circumstances it may be appropriate or necessary for the Council to work with third parties who are not themselves a public Authority (such as an individual, company or non-governmental organisation) to assist with an investigation. Where that third party is acting in partnership with or under the direction of the Council, then they are acting as our agent and any activities that the third party conducts which meet the RIPA definitions of directed surveillance should be authorised. The agent will be subject to RIPA in the same way as any employee of the Council would be. The AO should ensure that the agents are qualified or have the necessary skills to achieve the objectives. They should also ensure that they understand their obligations under RIPA. If advice is required, please contact the Legal Department.

16.2 If the above circumstances apply and it is intended to instruct an agent to carry out the covert activity, the agent must complete and sign the appropriate form.

16.3 Similarly, a surveillance authorisation should also be considered where the Council is aware that a third party (that is not a public Authority) is independently conducting surveillance and the Council intends to make use of any suitable material obtained by the third party for the purposes of a specific investigation or is to act as the prosecuting body.

## 17. EQUIPMENT

17.1 All equipment capable of being used for directed surveillance, such as cameras, should be fit for the purpose for which they are intended. The equipment should be logged on the central register of equipment held by the RIPA Coordinator. This will require a description, Serial Number, and an explanation of its capabilities.

17.2 When completing an Authorisation, the applicant must provide the AO with details of any equipment to be used and its technical capabilities. The AO will have to take this into

account when considering the intrusion issues and proportionality. The AO must make it clear on the Authorisation exactly what equipment, if any, they are authorising and under what circumstances.

## 18. COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

18.1 This policy applies to all use of under-cover Officers or informants, referred to as Covert Human Intelligence Sources (CHIS). Not all human source activity will meet the definition of a CHIS. For example, a source may be a public volunteer or someone who discloses information out of a professional or statutory duty or has been tasked to obtain information other than by way of a covert relationship.

18.2 Test purchase activity does not in general require authorisation under RIPA as vendor-purchaser activity does not constitute a relationship. However, if a number of visits are undertaken, a relationship may be established and authorisation as a CHIS should be considered. Equally a test purchase may meet the definition of directed surveillance.

18.3 If you intend to instruct a third party to act as the CHIS, the agent must complete and sign the appropriate form. The agent will be subject to RIPA in the same way as any employee of the Council would be. If advice is required, please contact either the RIPA Coordinator or the Legal Department.

18.4 An application for either directed surveillance or the use of a CHIS will need authorising internally by an AO. If authorised by the AO, approval will be required from a Justice of the Peace (JP) prior to any activity taking place. (See the appropriate sections below).

18.5 The authorisation request should be accompanied by a risk assessment, giving details of how the CHIS is going to be handled and the arrangements which are in place for ensuring that there is at all times a person with responsibility for maintaining a record of the use made of CHIS. The risk assessment should take into account the safety and welfare of the CHIS in relation to the activity and should consider the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS after the cancellation of the authorisation should also be considered at the outset.

18.6 Where surveillance or the use of a CHIS is likely to result in the obtaining of confidential information, it is imperative that legal advice should first be sought from the SRO or the Legal Department. Confidential information includes, though is not limited to, matters subject to legal privilege, confidential personal information and confidential journalistic material. Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it.

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

18.8 Legal advice should always be sought where consideration is given to the use of CHIS.

18.9 DEFINITION OF CHIS

18.10 A CHIS is a person who: -

- Establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within the following paragraphs;
- Covertly uses such a relationship to obtain information or to provide access to any information to another person; or

- Covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

18.11 A relationship is established, maintained or used for a covert purpose if, and only if, it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

18.12 The serious crime criteria of the offences under investigation do not apply to CHIS.

18.13 CHIS's may only be authorised if the following arrangements are in place:

- That there will at all times be an Officer (the handler) within the Council who will have day to day responsibility for dealing with the source on behalf of the authority, and for the source's security. The handler is likely to be the IO,
- That there will at all times be another Officer within the Council who will have general oversight of the use made of the source; (controller) i.e. the Line Manager.
- That there will at all times be an Officer within the Council who has responsibility for maintaining a record of the use made of the source.
- That the records relating to the source maintained by the local authority will always contain particulars of all matters specified by the Secretary of State in Regulations.

18.14 The Handler will have day to day responsibility for:

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

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

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

18.17 In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example, a member of the public is asked to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has <u>not</u> been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, directed surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual.

18.18 Authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked. Rather, an authorisation might cover, in broad terms, the nature of the source's task.

18.19 VULNERABLE CHIS

18.20 Special consideration must be given to the use of a Vulnerable Individual as a CHIS. 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 unable to protect himself against significant harm or exploitation. Any individual of this description, or a Juvenile as defined below, should only be authorised to

act as a source in the most exceptional circumstances and only then when authorised by the Senior Responsible Officer.

18.21 Special safeguards also apply to the use or conduct of Juvenile Sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for them.

18.22 If the use of a Vulnerable Individual or a Juvenile is being considered as a CHIS you must consult the Legal Department before authorisation is sought as authorisations should not be granted unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied. Authorisations for Juvenile Sources must be authorised by the Senior Responsible Officer within the Council.

18.23 It is unlikely that the use of a Vulnerable Individual or Juvenile CHIS by the Council will meet the requirements of necessity and proportionality and be considered justifiable.

18.24 USE OF EQUIPMENT BY A CHIS

18.25 If a CHIS is required to wear or carry a surveillance device such as a covert camera it does not need a separate intrusive or directed surveillance authorisation, provided the device will only be used in the presence of the CHIS. It should be authorised as part of the conduct of the CHIS.

18.26 CHIS, whether or not wearing or carrying a surveillance device, in residential premises or a private vehicle, does not require additional authorisation to record any activity inside those premises or that vehicle which takes place in their presence. This also applies to the recording of telephone conversations.

18.27 CHIS MANAGEMENT

18.28 The operation will require managing by the handler and controller which will include ensuring that the activities of the source and the operation remain focused and there is no status drift. It is important that the intrusion is assessed on an ongoing basis to ensure the operation remains proportionate. The security and welfare of the source will also be monitored. The AO should maintain general oversight of these functions.

18.29 During CHIS activity there may be occasions when unforeseen action or undertakings occur. Such incidences should be recorded as soon as practicable after the event and if the existing authorisation is insufficient, it should either be dealt with by way of a review and re-authorisation (for minor amendments only) or it should be cancelled, and a new authorisation obtained before any further action is carried out. Similarly, where it is intended to task a CHIS in a new significantly different way than previously identified, the proposed tasking should be referred to the AO, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and details of such referrals must be recorded.

18.30 CHIS RECORD KEEPING

18.31 The records relating to the source maintained by the Council will always contain particulars as laid down by the Covert Human Intelligence Sources codes of practice, revised CHIS codes of practice and the RIPA (Source Records) Regulations 2000; SI No: 2725 which details the particulars that must be included in these records.

## 19. NECESSITY

19.1 Obtaining an authorisation under RIPA will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place.

19.2 RIPA first requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds applicable to the Council.

19.3 The applicant must be able to demonstrate why it is necessary to carry out the covert activity to achieve the objectives and that there was no other means of obtaining the same information in a less intrusive method. The applicant must detail the crime being investigated and the information or evidence they are hoping to obtain. They should also state that they have considered other means of obtaining this information and have either concluded this is the only method available or that other methods are not appropriate and state the reason; for example it would alert the subject to their investigation which would be detrimental to the case.

## 20. PROPORTIONALITY

20.1 If the activities are deemed necessary, the AO must also believe that they are proportionate to the objective they are aiming to achieve. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

20.2 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render the proposed actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

20.3 When completing the authorisation the AO should explain why the methods and tactics to be adopted during the surveillance are justified in the particular circumstances of the case.

20.4 The Codes provide guidance relating to proportionality which should be considered by both applicants and AOs:

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

20.5 When completing an application for authorisation, the case should be presented in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the authorisation.

## 21. COLLATERAL INTRUSION

21.1 Before authorising applications for directed surveillance, the AO should also take into account the risk of collateral intrusion - obtaining private information about persons who are not subjects of the surveillance.

21.2 Officers should take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to the aims of the operation. The same proportionality tests apply to anticipated collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

21.3 All applications must include an assessment of the risk of collateral intrusion and details of any measures taken to limit this (within the relevant section of the form), to enable the AO to fully consider the proportionality of the proposed actions.

21.4 In order to give proper consideration to collateral intrusion, an AO should be given full information regarding the potential scope of the anticipated surveillance, including the likelihood that any equipment or software deployed may cause intrusion on persons or property other than the subject(s) of the application. If an automated system such as an online search engine is used to obtain the information, the AO should be made aware of its potential extent and limitations. Material which is not necessary or proportionate to the aims of the operation or investigation should be discarded or securely retained separately where it may be required for future evidential purposes. The AO should ensure appropriate safeguards for the handling, retention or destruction of such material, as well as compliance with Data Protection Act requirements.

21.5 Where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy of such individuals should not be considered as collateral intrusion but rather as intended intrusion.

21.6 Where the Council intends to access a social media or other online account to which they have been given access with the consent of the owner, the authority will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a Directed Surveillance authorisation should be considered, particularly (though not exclusively) where it is intended to monitor the account going forward.

## 22. THE APPLICATION AND AUTHORISATION PROCESS

22.1 All forms relating to RIPA can be found at https://www.gov.uk/government/collections/ripa-forms--2

22.2 DURATION OF AUTHORISATIONS

22.3 Authorisations must be given for the maximum duration from the date approved by the JP/Magistrate but reviewed on a regular basis and formally cancelled when no longer needed. They do not expire – they must be cancelled when the surveillance is no longer proportionate or necessary. Therefore, a directed surveillance authorisation will cease to have effect after three months from the date of approval by the Magistrate unless renewed or cancelled. Durations detailed below:

- Directed Surveillance 3 Months
- Renewal 3 Months
- Covert Human Intelligence Source 12 Months
- Renewal 12 months

- Juvenile Sources 4 Months
- Renewal 4 Months

22.4 It is the responsibility of the IO to make sure that the authorisation is still valid when they undertake surveillance.

22.5 APPLICATIONS/AUTHORISATION

22.6 The applicant or some other person must carry out a feasibility study and intrusion assessment as this may be required by the AO. The person seeking the authorisation should then complete the application form having regard to the guidance given in this Policy and the statutory Codes of Practice. There should not be any real delay between the feasibility study and the completion of the application form to ensure that the details within the application remain accurate. The form should then be submitted to the AO for authorisation.

22.7 When completing an application, the applicant must ensure that the case for the authorisation is presented in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the warrant or authorisation.

22.8 For directed surveillance, the offence must be a criminal offence that attracts a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

22.9 All the relevant sections must be completed with enough information to ensure that applications are sufficiently detailed for the AO to consider necessity and proportionality, having taken into account the collateral intrusion issues. AOs should refuse to authorise applications that are not to the required standard and should refer them back to the originating Officers. Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.

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

22.11 All applications will be submitted to the AO via the Line Manager of the appropriate enforcement team in order that they are aware of the application and activities being undertaken by their staff. The Line Manager will perform an initial quality check of the application. However, they should not be involved in the sanctioning of the authorisation.

22.12 Applications, whether authorised or refused, will be issued with a unique number (obtained from the RIPA Coordinator) by the AO, taken from the next available number in the central record of authorisations which is held by the RIPA Coordinator.

22.13 If not authorised, feedback will be provided to the applicant and the application will be forwarded to the RIPA Coordinator for recording and filing.

22.14 If authorised, the applicant will then complete the relevant section of the judicial application/order form. Although this form requires the applicant to provide a brief summary of the circumstances of the case, this is supplementary and does not replace the need to supply the original RIPA authorisation form to the Court.

22.15 ARRANGING THE COURT HEARING

22.16 Within office hours a hearing must be arranged at the Magistrates' Court with Her Majesty's Courts and Tribunals Service (HMCTS). The hearing will be in private and heard by a single JP. The application to the JP will be on oath.

22.17 Officers who may present the application at these proceedings will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or information as required by the JP. The legal department can advise who is duly authorised and able to present.

22.18 ATTENDING THE HEARING

22.19 The applicant and the AO should attend the Hearing to answer any questions directed at them. Upon attending the hearing, the presenting Officer must provide to the JP the partially completed judicial application/order form, a copy of the RIPA application/authorisation form, and the original form, together with any supporting documents setting out the case.

22.20 The original RIPA authorisation should be shown to the JP but will be retained by the Council so that it is available for inspection by IPCO, and in the event of any legal challenge or investigations by the IPT.

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

22.22 The JP will consider whether they are satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. In addition, they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate Designated Person within the Council and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

22.23 DECISION OF THE JP

22.24 The JP has a number of options:

22.25 Approve or renew an authorisation. If approved by the JP, the date of the approval becomes the commencement date and the three months duration will commence on this date, the Officers are now allowed to undertake the activity.

22.26 Refuse to approve or renew an authorisation. The RIPA authorisation will not take effect and the Council may **not** use the technique in that case.

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

22.28 For, a technical error (as defined by the JP), the form may be remedied without going through the internal authorisation process again. The Officer may then wish to reapply for judicial approval once those steps have been taken.

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

22.30 The JP will record their decision on the order section of the judicial application/order form. The court administration will retain a copy of the Council's RIPA application and authorisation form and the judicial application/order form. The Officer will retain the original authorisation and a copy of the judicial application/order form.

22.31 The Council may only appeal a JP decision on a point of law by judicial review. If such a concern arises, the Legal Department will decide what action if any should be taken.

22.32 POST COURT PROCEDURE

22.33 It will be necessary to work out the cancellation date from the date of approval and ensure that the applicant and the AO are aware. The original application and the copy of the judicial application/order form should be forwarded to the RIPA Coordinator. A copy will be retained by the applicant and if necessary by the AO. The Central Register of Authorisations will be updated with the relevant information to comply with the Codes of Practice and the original documents filed and stored securely.

22.34 Where dates are set within the process such as reviews, they must be adhered to. This will help with demonstrating that the process has been managed correctly in line with the Codes of Practice.

22.35 MANAGEMENT OF THE ACTIVITY

22.36 All RIPA activity will need to be managed by all the persons involved in the process. It is important that all those involved in undertaking directed surveillance activities are fully aware of the extent and limits of the authorisation. There should be an ongoing assessment of the need for the continued activity, including ongoing assessments of the intrusion. All material obtained including evidence should be stored in line with relevant legislation and procedures to safeguard its integrity and reduce a risk of challenge. (See use of material as evidence**)**

22.37 REVIEWS

22.38 When an application has been authorised and approved by a JP, regular reviews must be undertaken by the AO to assess the need for the surveillance to continue.

22.39 In each case the AO should determine at the outset how often a review should take place. This should be as frequently as is considered necessary and practicable. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides a high level of intrusion into private life or significant collateral intrusion, or may obtain confidential information. Review periods will be recorded on the application form and the decision will be based on the circumstances of each application. However, reviews should be conducted at least monthly to ensure that the activity is managed. It will be important for the AO to be aware of when reviews are required following an authorisation, to ensure timely submission of the review form.

22.40 Applicants are responsible for submitting a review form by the date set by the AO. They should also use a review form for any changes in circumstances to the original application which would comprise a change to the level of intrusion so that the requirement to continue the activity can be reassessed. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances. If the circumstances or the objectives have changed considerably, or the techniques to be used are now different, a new RIPA application form should be submitted and the process followed to obtain approval by a JP.

22.41 Line managers should also make themselves aware of the required review periods to ensure that the relevant forms are completed on time.

22.42 The reviews are dealt with internally by submitting the review form to the AO. There is no requirement for a review form to be submitted to a JP.

22.43 The results of a review should be recorded on the Central Record of Authorisations.

22.44 RENEWAL

22.45 A renewal form is to be completed by the applicant when the original authorisation period is about to expire but directed surveillance or the use of a CHIS is still required.

22.46 Renewals must be approved by a JP.

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

22.48 The applicant should complete all the sections within the renewal form and submit the form to the AO for consideration.

22.49 AOs should examine the circumstances with regard to necessity, proportionality and the collateral intrusion issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The AO must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

22.50 If the AO refuses to renew the application, the cancellation process should be completed. If the AO authorises the renewal of the activity, the same process is to be followed as for the initial application whereby approval must be sought from a JP.

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

22.52 CANCELLATION

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

22.54 As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other IO involved in the investigation should inform the AO. The AO will formally instruct the IO to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the Central Record of Authorisations**.**

22.55 The IO submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and also detail if any images were obtained, particularly any images containing third parties. The AO should then take this into account and issue instructions regarding the management and disposal of the images. See section below; Safeguarding and the Use of Surveillance Material.

22.56 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant acted within the authorisation. This check will form part of the oversight function. Where issues are identified, they will be brought to the attention of the Line Manager and the SRO.

22.57 When cancelling a CHIS authorisation an assessment of the welfare and safety of the source should be assessed, and any issues identified and reported as above.

## 23. SURVEILLANCE OUTSIDE OF RIPA

23.1 As previously detailed, amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 mean that Councils can now only grant an authorisation under RIPA where the Council is investigating criminal offences which attract a maximum custodial sentence of at least six months or criminal offences relating to the underage sale of alcohol or tobacco.

23.2 As a result of the changes in legislation, it is envisaged that surveillance may be required which falls outside of RIPA (for example in the case of anti-social behaviour disorders which do not attract a maximum custodial sentence of at least six months imprisonment).

23.3 As stated, conducting surveillance outside of RIPA is not fundamentally unlawful, however in order for the Council to defend claims that they have breached an individual's right to privacy under the HRA the Council needs to demonstrate that their actions were justified in the circumstances of the case. It is therefore the Council's policy that, in order to undertake surveillance that falls outside of RIPA, Officers will follow the same initial process as when they are making an application for authorisation under RIPA. The IO must complete a Non-RIPA application form that is authorised by an AO and the application will be lodged with and monitored by the RIPA Coordinator. The AO will need to be satisfied that the actions are necessary and proportionate and give due consideration to any collateral intrusion. The Non-RIPA authorisation form is available from the RIPA Coordinator. The procedure for review and renewal of the surveillance application will be the same, however there is no requirement/ability to obtain authorisation from a JP.

23.4 Non-RIPA surveillance also includes staff surveillance in serious disciplinary investigations. Any surveillance of staff must be formally recorded on the Non-RIPA surveillance application form and authorised by the AO in consultation with the RIPA Coordinator. The review of staff usage of the internet and e-mail would also not fall under RIPA. This surveillance outside of RIPA must however be compliant with any Council Policies with regard to monitoring at work and business practices legislation and should also consider ICO guidance in relation to surveillance of staff. Surveillance of staff should only be carried out in exceptional circumstances.

23.5 The RIPA codes also provide guidance that authorisation under RIPA is <u>not</u> required for the following types of activity:

- General observations that do not involve the systematic surveillance of an individual or a group of people and should an incident be witnessed the Officer will overtly respond to the situation.
- Use of overt CCTV and Automatic Number Plate Recognition systems.
- Surveillance where no private information is likely to be obtained.
- Surveillance undertaken as an immediate response to a situation.
- Covert surveillance <u>not</u> relating to criminal offence which carries a maximum sentence of 6 months imprisonment and does not relate to the sale of alcohol or tobacco to children (surveillance outside of RIPA).
- The use of a recording device by a CHIS in respect of whom an appropriate use or conduct authorisation has been granted permitting them to record any information in their presence.
- The covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance,

the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance this is outside of RIPA.

## 24. SAFEGUARDING AND THE USE OF SURVEILLANCE MATERIAL

24.1 This section provides guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained through directed surveillance or CHIS activity. This material may include private, confidential or legally privileged information.

24.2 AUTHORISED PURPOSE

24.3 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. For the purposes of this Code this is defined as follows:-

- It is, or is likely to become, necessary for any of the statutory purposes set out in the RIPA in relation to covert surveillance or CHIS activity;
- It is necessary for facilitating the carrying out of the functions of public authorities under RIPA;
- It is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- It is necessary for the purposes of legal proceedings; or
- It is necessary for the performance of the functions of any person by or under any enactment.

24.1 USE OF MATERIAL AS EVIDENCE

24.2 Material obtained through directed surveillance, may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996 (CPIA), the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998.

24.3 Ensuring the continuity and integrity of evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the CPIA and these considerations will apply to any material acquired through covert surveillance that is used in evidence. When information obtained under a covert surveillance authorisation is used evidentially, the Council must be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

24.4 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements. In a criminal case the codes issued under CPIA will apply. They require that the investigator record and retain all relevant material obtained in an investigation and later disclose relevant material to the prosecuting solicitor. They in turn will decide what is disclosed to the defence solicitor.

24.5 There is nothing in RIPA which prevents material obtained under directed or intrusive surveillance authorisations from being used to further other investigations.

24.6 HANDLING AND RETENTION OF MATERIAL

24.7 All material associated and obtained with an application will be subject to the provisions of all data protection legislation and regulations and CPIA Codes of Practice and to any

Council Policies with regard to data retention and security. All Officers involved within this process should make themselves aware of the provisions within this legislation and how it impacts on the RIPA process. Material obtained together with relevant associated paperwork should be held securely. Extra care needs to be taken if the application and material relates to a CHIS.

24.8 Material required to be retained under CPIA should be retained until a decision is taken whether to institute proceedings against a person for an offence or if proceedings have been instituted, at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case.

24.9 Where the accused is convicted, all material which may be relevant must be retained at least until the convicted person is released from custody, or six months from the date of conviction, in all other cases.

24.10 If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction.

24.11 If an appeal against conviction is in progress when the convicted person is released, or at the end of the period of six months, all material which may be relevant must be retained until the appeal is determined.

24.12 Retention beyond these periods must be justified under data protection legislation and regulations. AOs, through the Council's Data Controller, must ensure compliance with the appropriate Data Protection requirements and any relevant internal arrangements produced by the Council relating to the handling and storage of material.

24.13 DISSEMINATION OF INFORMATION

24.14 It may be necessary to disseminate material acquired through the RIPA covert activity within the Council or with other Councils or agencies, including the Police. The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary. It must also be in connection with an authorised purpose as set out above. It will be necessary to consider exactly what and how much information should be disclosed. Only so much of the material may be disclosed as the recipient needs; for example, if a summary of the material will suffice, no more than that should be disclosed.

24.15 The obligations apply not just to the Council as the original authority acquiring the information, but also to anyone to whom the material is subsequently disclosed. In some cases, this will be achieved by requiring the latter to obtain permission from the Council before disclosing the material further. It is important that the Officer in Charge (OIC) of the enquiry considers these implications at the point of dissemination to ensure that safeguards are applied to the data.

24.16 A record will be maintained justifying any dissemination of material. If in doubt, seek legal advice.

24.17 STORAGE

24.18 Material obtained through covert surveillance, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss. It must be held so as to be inaccessible to persons who are not required to see the material (where applicable). This requirement applies to all those who are responsible for the handling of the material. It will be necessary to ensure that an appropriate security clearance regime is in place to safeguard the material whether held electronically or physically.

24.19 COPYING

24.20 Material obtained through covert surveillance may only be copied to the extent necessary for the authorised purposes set out above. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance, and any record which refers to the covert surveillance and the identities of the persons to whom the material relates.

24.21 In the course of an investigation, the Council must not act on or further disseminate legally privileged items unless it has first informed the IPC that the items have been obtained.

24.22 DESTRUCTION

24.23 Information obtained through covert surveillance, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s) set out above. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible.

## 25. ERRORS

25.1 Proper application of the surveillance provisions in the RIPA codes and this Policy should reduce the scope for making errors.

25.2 RELEVANT ERROR

25.3 An error must be reported if it is a "**relevant error**". A relevant error is any error by the Council in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of RIPA.

25.4 Examples of relevant errors occurring would include circumstances where:

- Surveillance activity has taken place without lawful authorisation.
- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Surveillance Codes of Practice relating to the safeguards of the material.

25.5 Errors can have very significant consequences on an affected individual's rights. All relevant errors made by the Council must be reported to the Investigatory Powers Commissioner as soon as reasonably practicable, and a full report no later than ten working days after the error is discovered. The report should include information on the cause of the error; the amount of surveillance conducted, and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

25.6 SERIOUS ERRORS

25.7 The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a **serious error** and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless they consider that the error has caused significant prejudice or harm to the person concerned. The fact that

there has been a breach of a person's convention rights (within the meaning of the HRA) is not sufficient by itself for an error to be a serious error.

25.8 It is important that all staff involved in the RIPA process report any issues, so they can be assessed as to whether it constitutes an error which requires reporting.

## 26. COMPLAINTS

26.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against the Council's use of investigatory powers, including those covered by this code. Any complaints about the use of powers as described in this code should be directed to the IPT.

26.2 Complaints should be addressed to:
The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

| **Version Control:** | |
|---|---|
| **Document Name:** | Investigatory Powers Act 2016 Acquisition of Communications Data Policy |
| **Version:** | 1 |
| **Responsible Officer:** | Emma Cathcart, Counter Fraud Unit |
| **Approved by:** | Cabinet |
| **Date First Approved:** | |
| **Next Review Date** | |
| **Retention Period:** | N/A |

**Revision History**

| Revision date | Version | Description |
|---|---|---|
| April 2019 | 1 | Change in legislation / introduction of IPA 2016 |
| | | |

**Consultees**

| Internal | External |
|---|---|
| Audit Committee | |
| Legal Department | |
| Corporate Management | |

**Distribution**

| Name | |
|---|---|
| Enforcement Officers | |
| | |

**CONTENTS**

1. INTRODUCTION ..... 4
2. SCOPE OF POLICY ..... 4
3. ROLES OF STAFF INVOLVED IN THE PROCESS ..... 4
4. APPLICANT ..... 5
5. DESIGNATED PERSON ..... 5
6. SINGLE POINT OF CONTACT ..... 5
7. OCDA AUTHORISING INDIVIDUAL ..... 6
8. WHAT IS COMMUNICATIONS DATA ..... 6
9. COMMUNICATIONS DATA DEFINITIONS ..... 6
10. POSTAL DEFINITIONS ..... 7
11. WEB BROWSING AND COMMUNICATIONS DATA ..... 8
12. RELEVANT COMMUNICATIONS DATA ..... 8
13. INTERNET CONNECTION RECORDS ..... 9
14. PREPAID MOBILE PHONES ..... 9
15. WHO CAN COMMUNICATIONS DATA BE OBTAINED FROM? ..... 9
16. LAWFUL REASONS TO ACCESS COMMUNICATIONS DATA ..... 10
17. USING OTHER POWERS ..... 10
18. INTERNAL INVESTIGATIONS ..... 10
19. SERIOUS CRIME THRESHOLD ..... 10
20. NECESSITY AND PROPORTIONALITY ..... 11
21. NECESSITY ..... 11
22. PROPORTIONALITY ..... 11
23. COLLATERAL INTRUSION ..... 12
24. THE TWO WAYS OF OBTAINING COMMUNICATIONS DATA ..... 12
25. THE APPLICATION PROCESS ..... 13
26. TIME SCALES ..... 14
27. APPLICATION FORM ..... 14
28. URGENT ORAL AUTHORISATION ..... 15
29. ERRORS ..... 15
30. REPORTABLE ERROR ..... 16
31. RECORDABLE ERROR ..... 16
32. EXCESS DATA ..... 16
33. RECORD KEEPING AND SECURITY OF DATA ..... 17
34. CRIMINAL PROCEDURES AND INVESTIGATIONS ACT (CPIA) ..... 17
35. DATA PROTECTION ACT 2018 (DPA) AND THE GENERAL DATA PROTECTION REGULATIONS (GDPR) ..... 18

36. OVERSIGHT ..... 18
37. COMPLAINTS ..... 19
38. STRATEGY AND POLICY REVIEW ..... 19

## 1. INTRODUCTION

1.1. The Investigatory Powers Act 2016 (IPA) governs how law enforcement agencies use the investigatory powers available to them, in relation to the lawful acquisition of Communications Data (CD). The IPA provides unprecedented transparency and substantial privacy protection, strengthening safeguards and introducing oversight arrangements. It also introduces a powerful new Investigatory Powers Commission (IPC) to oversee how these powers are used.

1.2. The powers provided by the Regulation of Investigatory Powers Act 2000 (RIPA) allowed the Council to obtain CD from Communications Service Providers (CSPs) in connection with criminal investigations.

1.3. The IPA extends the range of data Councils are able to request from providers but ensures independent authorisation for the acquisition through the new Office for Communications Data Authorisations (OCDA). However, it continues only to be a justifiable interference with an individual's human rights if such conduct is authorised, is both necessary and proportionate, and is in accordance with the law.

1.4. All applications for CD must be made via an Accredited Officer known as a Single Point of Contact (SPoC) who has passed a Home Office approved course. All Councils must use the National Anti-Fraud Network (NAFN) as their SPoC. Therefore, all applications to access CD will be made through NAFN via their online application service.

1.5. The introduction of OCDA means the acquisition of CD by Council officers no longer requires judicial approval.

1.6. These powers should not be confused with any Policy and practices with regard to monitoring under the lawful business practices legislation. This latter legislation relates to the monitoring of the Council's own communication and computer systems.

## 2. SCOPE OF POLICY

2.1. This Policy sets out the Council's procedures and approach for obtaining and handling CD for the purposes of preventing or detecting crime or of preventing disorder; the only lawful reasons for Council staff to use IPA legislation to access CD.

2.2. This Policy should be read in conjunction with the Communications Data Code of Practice (COP), currently in draft. This also creates a system of safeguards, consistent with the requirements of Article 8 (rights to privacy) of the Human Rights Act 1998. The Codes of Practice are admissible in evidence in criminal and civil proceedings.

2.3. The draft Code can be obtained using the link detailed below and is available to all Council staff involved in the acquisition of CD.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757851/Communications_Data_Code_of_Practice.pdf

2.4. Both this Policy and the COP will be followed at all times and under no circumstances should access to CD be sought outside of this guidance.

2.5. The Council will review and amend this Policy as necessary to ensure that it continues to remain compliant and meets legislative requirements and the objectives of the Council.

## 3. ROLES OF STAFF INVOLVED IN THE PROCESS

3.1. The process for the acquisition of CD under the IPA requires the following personnel:

- Applicant
- Designated Person (DP)
- Single Point of Contact (SPoC)
- OCDA Authorising Individual

## 4. APPLICANT

4.1. The Applicant is a person involved in conducting an investigation or operation who makes an application in writing for the acquisition of CD. The Applicant completes an application form, setting out for consideration the necessity and proportionality of a specific requirement for acquiring CD. Prior to the completion of the relevant paperwork, it may be advisable for the Applicant to consult with the SPoC at NAFN.

## 5. DESIGNATED PERSON

5.1. The DP is a person of Service Manager level or equivalent within the Council who confirms to NAFN that they are aware that an application has been made. They do not have any authorising function but are responsible for the integrity of the process in place and the overall quality of that process.

## 6. SINGLE POINT OF CONTACT

6.1. The SPoC is either an accredited individual (passed the Home Office course) or a group of accredited individuals such as the National Anti-Fraud Network, who are trained to facilitate lawful acquisition of CD. All accredited officers are issued a Personal Identification Number (PIN). Details of all accredited individuals are available to Communication Service Providers (CSPs) for authentication purposes.

6.2. An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for CD are undertaken. The SPoC provides objective judgement and advice to the Applicant and provides a "guardian and gatekeeper" function, ensuring that public authorities act in an informed and lawful manner.

6.3. As already explained, this Council can only use the services of NAFN as the Council's SPoC. Therefore, all applications to access CD will be made through NAFN.

6.4. The SPoC will be in a position to:

- Engage proactively with Applicants to develop strategies to obtain CD and use it effectively in support of operations or investigations;
- Assess whether the acquisition of specific CD from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data;
- Advise Applicants on the most appropriate method for the acquisition of data where the data sought engages a number of CSPs;
- Advise Applicants on the type of data that can be obtained to meet their purposes.
- Provide assurance to DPs that Authorisations and Notices are lawful under the IPA and free from errors;
- Provide assurance to OCDA that an application has been verified and checked.

- Assess whether CD disclosed by a CSP in response to a Notice fulfils the requirement of the Notice;
- Assess whether CD obtained by means of an Authorisation fulfils the requirement of the Authorisation;
- Assess any cost and resource implications to both the Council and the CSP of data requirements.

## 7. OCDA AUTHORISING INDIVIDUAL

7.1. The OCDA officer receives the application from the NAFN SPoC and checks the application meets the necessary criteria before authorising or rejecting and issuing a Decision Document. NAFN will retain the original of all the documents. These will be retained within the on-line portal. Copies of the documents must be retained by the Applicant, DP or within the relevant department for inspection by the IPC and for audit, filing and disclosure purposes under the Criminal Procedures Investigation Act 1996. (OCDA will only hold the applications and Decision Documents for a limited period of time due to the degree of sensitivity and risk arising from the accumulation of these documents in a central database.)

## 8. WHAT IS COMMUNICATIONS DATA

8.1. CD does not include the content of any communication. It is not lawfully possible for Council employees under any circumstances to obtain the content of communications.

8.2. The term 'CD' embraces the 'who', 'when' and 'where' of a communication but not the content - not what was said or written. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within a communication including text, audio and video

8.3. CD can include the address to which a letter is sent, the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.

8.4. CD is generated, held or obtained in the provision, delivery and maintenance of communications services – i.e. postal services or telecommunications services.

8.5. Where the provision of a communication service engages a number of providers, the SPoC will determine the most appropriate plan for acquiring the data.

8.6. When enquiries regarding CD are being considered within an investigation, it may be advisable that Applicants seek advice and guidance from the SPoC at NAFN. The RIPA Coordinator /DP within the Counter Fraud Unit can provide contact details.

## 9. COMMUNICATIONS DATA DEFINITIONS

9.1. The IPA introduces new terminology for CD – Entity Data and Events Data

9.2. Entity Data describes the 'who' involved in the communication – the subscriber and the links between different entities or communicators. Entities could be individuals, groups and objects (such as mobile phones or other communications devices).

9.3. Examples of entity data requests include:

- Subscriber checks, such as who is the subscriber of phone number 01234 567 890?
- Who is the account holder of e-mail account example@example.co.uk?
- Who is entitled to post to web space www.example.co.uk?
- Subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments e.g. for pre-paid mobiles.
- Information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services.
- Information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes.
- Information about selection of preferential numbers or discount calls.

9.4. Event Data identifies or describes events in relation to a telecommunications system which consists of one or more entities engaging in an activity at a specific point or points in time – the 'what, when and where'. For obtaining Event Data there is a Serious Crime Threshold (see 11.1)

9.5. Examples of events data include, but are not limited to:

- Information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- Information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- Information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- Routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);
- Itemised telephone call records (numbers called)12;
- Itemised internet connection records;
- Itemised timing and duration of service usage (calls and/or connections);
- Information about amounts of data downloaded and/or uploaded;
- Information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

## 10. POSTAL DEFINITIONS

10.1. A postal service is a service which involves one or more of the collection, sorting, conveyance, distribution and delivery of postal items and where its main purpose is to

make available or facilitate the transmission of postal items containing communications. CD in relation to a postal service is defined at section 262(3) of the IPA and comprises three elements:

- Postal data which is or has been comprised in or attached to a communication for the purpose of the service by which it is transmitted;
- Data relating to use made by a person of a postal service;
- Information held or obtained by a postal operator about persons to whom the postal operator provides or has provided a communications service and which relates to the provision of the service.

10.2. Postal data is defined in section 262(4) of the IPA and includes specified categories of data written on the outside of a postal item. All information on the outside of a postal item concerning its postal routing, for example the address of the recipient, the sender and the post-mark, is postal data.

10.3. In the postal context anything included inside a postal, item, which is in transmission, will be content. Any message written on the outside of a postal item which is in transmission may be content and fall within the scope for the interception of communications. For example, a message written by the sender for the recipient will be content but a message written by a postal worker concerning the delivery of the postal item will not. All information on the outside of a postal item concerning it's routing, for example the address of the recipient, the sender and the postmark, is postal data and will not be content.

## 11. WEB BROWSING AND COMMUNICATIONS DATA

11.1. Web browser software provides one way for users to access web content. When using a browser to access the web, a user may enter a web address. These are also referred to as uniform resource locators (URLs).

11.2. Some elements of a URL are necessary to route a communication to the intended recipient and are therefore CD. The URL may also contain the port, which is an extended part of the Internet Provider (IP) address and the user information – including usernames and authorisations. The port and user information will be CD.

## 12. RELEVANT COMMUNICATIONS DATA

12.1. A data retention notice under the IPA may only require the retention of relevant CD. This is defined at section 87 of the IPAt and is a subset of CD.

It is data which may be used to identify or assist in identifying any of the following:

- The sender or recipient of a communication;
- The time or duration of a communication;
- The type, method or pattern, or fact of a communication;
- The telecommunication system to or through which a communication is transmitted;
- The location of any such system.

## 13. INTERNET CONNECTION RECORDS

13.1. An internet connection record (ICR) is a record of an event held by a telecommunications operator about the service to which a customer has connected on the internet. An ICR is CD.

13.2. An ICR will only identify the service that a customer has been using. For example many social networking apps on a device maintain persistent connections to a service. Even in this case the relevant ICR will signpost the service accessed by the device, enabling the authority to make further enquiries of the social networking provider identified.

13.3. Further detail on the definitions described above and the types of CD that can be accessed is available in the COP.

13.4. The SPoC will provide advice and assistance with regard to the types of data which can be lawfully obtained and how that data may assist an investigation. Where an applicant is unsure of the category of data they are seeking (entity or events data) or what additional types of CD may be retained by a telecommunications operator or postal operator for their own business use, the applicant should discuss this with their Single Point of Contact (SPoC).

## 14. PREPAID MOBILE PHONES

14.1. Unregistered prepaid mobile phones are common amongst criminals as it allows them to avoid detection more easily. It is possible that a subscriber check will identify a number as belonging to one of these devices. This does not necessarily prevent an investigating officer obtaining useful information. The Applicant can ask for further information about the subscriber under section 21(4)(c), including top-up details, method of payment, the bank account used or customer notes etc.

14.2. So as to allow for the widening of the data capture, the Applicant should outline in their original application that further information will be required if the phone turns out to be prepaid, this information could be requested in two stages. Firstly, asking for the subscriber details and then, if this turns out to be an unregistered prepaid phone, asking for the further information.

14.3. The information that is received can then be developed to try to obtain further information about the user of the phone. Solution Providers such as EasyPay, EPay etc. are the third parties involved in the transaction of credit placed on a mobile phone. If a Solution Provider is provided with the mobile telephone number, the transaction date and the transaction number, they are often able to provide the method of payment and the location of the top-up. Solution Providers are not CSPs and therefore they cannot be issued with a Notice under the IPA; instead the data can be applied for under the Data Protection Act via the SPoC.

## 15. WHO CAN COMMUNICATIONS DATA BE OBTAINED FROM?

15.1. CD can be obtained from a Communications Service Provider (CSP). A CSP is an operator who provides a postal service such as Royal Mail or telecommunications service, such as the usual telephone service providers. However, there may be less obvious companies which may be classed as a CSP. The SPoC at NAFN will determine which CSP they will contact to obtain the data on behalf of the Applicant. However, any intelligence obtained which establishes which CSP may provide the data should be included within the application or by notifying the SPoC.

## 16. LAWFUL REASONS TO ACCESS COMMUNICATIONS DATA

16.1. As mentioned earlier the Council's only lawful reasons to access CD is for the purpose of preventing or detecting crime or of preventing disorder.

16.2. Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed.

16.3. The Council can only lawfully process and consider applications to access CD on behalf of the Council. Under no circumstances will applications be accepted for outside authorities/agencies. However, it may be necessary during joint investigations to obtain CD; in these circumstances the Council can only apply for data which it would usually be allowed to access. It should be clear in the investigation Policy log that it is a joint investigation as it may have to be justified to a Court or Tribunal.

16.4. Staff must not apply on behalf of any third parties who do not have lawful authority to obtain CD. Should an organisation make such an approach this must be reported to the Senior Responsible Officer (SRO) who has the responsibility for the Council's working practices in relation to obtaining CD.

16.5. Where the Council is contracted to undertake work on behalf of a third party, CD may be obtained if the Council is the investigating and prosecuting body.

## 17. USING OTHER POWERS

17.1. The IPA is the primary legislation for the acquisition of CD and should always be the first option considered due to the rigorous and independent assessment and authorisation process.

## 18. INTERNAL INVESTIGATIONS

18.1. The Codes state 'where an investigation relates to an allegation of criminal conduct by a member of a public authority, that public authority (or another public authority appointed to investigate the complaint) may use their powers under Chapter II to obtain CD for the purpose of preventing and detecting the alleged or suspected crime where the investigating officer intends the matter to be subject of a prosecution within a criminal court. Should it be determined there are insufficient grounds to continue the investigation or insufficient evidence to initiate a prosecution within a criminal court, it will, with immediate effect, no longer be appropriate to obtain CD under the Act'.

18.2. If CD is sought in connection with officers of the Council committing crimes against the Council, it is important that the enquiry is a genuine criminal investigation with a view to proceeding criminally as opposed to just a disciplinary matter. Advice may be required from the Council's Legal section if this arises.

## 19. SERIOUS CRIME THRESHOLD

19.1. With effect from 1st November 2018 the IPA introduced a new Serious Crime Threshold to applications for CD. This means the Council may only acquire Events Data where the crime can be defined as a serious crime. Where the crime cannot be defined as serious, only Entity Data may be obtained.

19.2. The following definitions of serious crime apply:

- An offence that is capable of attracting a prison sentence of 12 months or more;
- An offence by a person who is not an individual (i.e. a corporate body);
- An offence falling within the definition of serious crime in section 263(1)of the IPA (i.e. where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common purpose);
- An offence which involves, as an integral part of it, the sending of a communication;
- An offence which involves, as an integral part of it a breach of a person's privacy.

## 20. NECESSITY AND PROPORTIONALITY

20.1. The COP states the acquisition of CD under the IPA will be a justifiable interference with an individual's human rights under Article 8 Right to Privacy, only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with law.

20.2. Below is guidance to assist Applicants with factors that impact on necessity and proportionality.

## 21. NECESSITY

21.1. In order to justify the application is necessary, the Applicant needs as a minimum to consider three main points:

1. The event under investigation, such as a crime or disorder offence;
2. The person, such as a suspect, witness or missing person and how they are linked to the event;
3. The Communication Data, such as a telephone number or IP address, and how this data is related to the person and the event.

21.2. In essence, necessity should be a short explanation of 1**) the event**, 2**) the person and 3) the CD and how these three link together.** The application must establish a link between the three aspects to be able to demonstrate the acquisition of CD is necessary for the statutory purpose specified.

21.3. Necessity does not entail explaining 'what will be achieved by acquiring the data' or 'why specific time periods have been requested', these points are relevant to proportionality and should be covered in the relevant section to stop repetition.

## 22. PROPORTIONALITY

22.1. Applicants should include an outline of how obtaining the data will benefit the investigation or operation. If more than one item of data is being sought, the relevance of the additional data should be explained.

22.2. This outline should include an explanation of how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. This justification should include confirmation that relevant less intrusive investigations have already been undertaken where possible. For example, the subscriber details of a phone number may be obtained from online enquiries or other publicly available sources.

22.3. The relevance of any time periods requested must be explained, outlining how these periods are proportionate to the event under investigation. The two basic questions are:

- What are you looking for in the data to be acquired and;
- If the data contains what you are looking for, what will be your next course of action?

22.4. Particular consideration should be given to any periods of days or shorter periods of time which might achieve the objective. They should specify the shortest period in which the objective for which the data is sought can be achieved. To do otherwise will impact on the proportionality of the Authorisation or Notice and impose unnecessary burden upon a CSP.

22.5. An explanation as to how CD once acquired will be used, and how it will benefit the investigation or operation will enable the Applicant to set out the basis of proportionality.

22.6. An explanation of the proportionality of the application should include a consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation.

22.7. An examination of the proportionality of the application should also involve consideration of possible unintended consequences and, when relevant this should be noted. Unintended consequences of an application are outcomes that are not intended by the application.

## 23. COLLATERAL INTRUSION

23.1 Consideration of collateral intrusion forms part of the proportionality considerations and becomes increasingly relevant when applying for Events Data. Applications should include details of what collateral intrusion may occur and how the time periods requested impact on the collateral intrusion.

23.2 The question to be asked is 'Will the data set to be acquired result in collateral intrusion to persons outside the line of enquiry the data is being obtained for?' For example, itemised billing on the subject's family home will be likely to contain calls made by the family members.

23.3 Applicants should not write about a potential or hypothetical 'error' and if the Applicant cannot identify any meaningful collateral intrusion, that factor should be recorded in the application i.e. 'none identified'.

23.4 It is accepted that for a straight forward subscriber check there will be no meaningful collateral intrusion.

## 24. THE TWO WAYS OF OBTAINING COMMUNICATIONS DATA

24.1. The legislation provides two different methods of acquiring CD (see below). The SPoC at NAFN will be responsible for deciding the process for obtaining the data required and passing responses from the service provider to the Council.

24.2. The two methods are:

- **Authorisation of conduct,** or
- **Authorisation to give a Notice**

24.3. An authorisation of conduct to acquire CD may be appropriate where, for example:

- there is an agreement in place between a public authority and a telecommunications operator or postal operator to facilitate the secure and swift disclosure of CD. Many telecommunications operators and postal operators have auditable acquisition systems in place to ensure accurate and timely acquisition of CD, while maintaining security and an audit trail;
- where the data can be acquired directly from a telecommunication system and the activity does not constitute interception or equipment interference; or
- a public authority considers there is a requirement to identify a person to whom a service is provided but the specific telecommunications operator or postal operator has yet to be conclusively determined as the holder of the CD.

An authorisation to give a notice may be appropriate where a telecommunications operator or postal operator is known to be capable of disclosing (and, where necessary, obtaining) the CD

## 25. THE APPLICATION PROCESS

25.1. From April 2019 the IPA removes the requirement to obtain judicial approval. Applications will only require Independent Authorisation.

25.2. Prior to an Applicant applying for CD, they should contact a SPoC at NAFN who will be in a position to advise them regarding the obtaining and use of CD within their investigation. This will reduce the risk of the Applicant applying for data which they are not able to obtain. It will also assist the Applicant to determine their objectives and apply for the most suitable data for those circumstances.

25.3. The Council will use the automated application process provided by NAFN. This automated service contains the relevant documentation for the Applicant to complete the relevant forms.

25.4. To use the system, Applicants and the DP have to individually register on the NAFN website - www.nafn.gov.uk. A number of departments within the Council have contributed towards the NAFN annual membership fee; therefore an Applicant needs to confirm with their Line Manager that they are allowed to register. Should you have any queries, please contact the Counter Fraud Unit.

25.5. With regard to shared services, the Council on whose behalf the request is being made must be a member of NAFN and the request made via login details for that Council. Applicants and DPs cannot make use of one Council's membership to obtain any information on behalf of another. Login details will be necessary for each Council that an individual is employed by or works on behalf of.

25.6. The online application form, once completed by the Applicant will be forwarded electronically to a SPoC at NAFN who will then perform their responsibilities and if required they will contact the Applicant regarding the contents of the application form. The SPoC at NAFN will obtain confirmation from the nominated DP that they are aware of the application before proceeding.

25.7. The SPoC confirms that the Council is permitted to use the recorded statutory purpose and determines the conduct to satisfy the Council's need (the type of data that is required). If event data is required the SPoC checks the Applicant has recorded a description of the offence(s) and a justification for the seriousness of the offence(s)

25.8. The SPoC can return the application to the Council for a re-work if it does not meet the necessary criteria.

25.9. Once approved the SPoC refers the application to OCDA for authorisation. OCDA then return the application to NAFN for the SPoC to obtain the authorised data from the CSP.

25.10. If the OCDA officer rejects the application it can be returned to the applicant for a re-work.

## 26. TIME SCALES

26.1. A new Operational Prioritisation has been introduced to enable NAFN to convey to OCDA the operational urgency for the acquisition of data and ensure it is appropriately triaged and handled to meet these demands.

26.2. Operational Prioritisation is categorised in Priority Levels 1-4 and for each Priority rating there is an expected Service response time.

26.3. The Council will generally be submitting requests that are Priority Level 4 – Routine- for which the response should be within 4 working days or 60 working hours.

## 27. APPLICATION FORM

27.1. The Applicant will complete an application form setting out for consideration the necessity and proportionality of a specific requirement for CD.
An application to acquire CD must:

- describe the CD required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the data is required, by reference to a statutory purpose under the Act;
- include a unique reference number;
- include the name and the office, rank or position held by the person making the application;
- describe whether the CD relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- identify and explain the time scale within which the data is required;
- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it;
- present the case for the authorisation in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;

- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;
- consider and, where appropriate, describe any possible unintended consequences of the application; and
- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data
- include the operation name (if applicable) to which the application relates;

**28. URGENT ORAL AUTHORISATION**

28.1. There is no provision within the legislation for the Council to orally provide authority to obtain CD. All requests will be made in writing on the NAFN portal and require authorisation from a DP.

**29. ERRORS**

29.1. There is a requirement to record or in some instances report to IPCO errors that occur when accessing CD. The thorough checking of operating procedures, including the careful preparation and checking of applications, Notices and Authorisations, should reduce the scope for making errors. Attention to detail will be required by all persons involved in the process.

29.2. Reporting and recording of errors will draw attention to those aspects of the process of acquisition and disclosure of CD that require further improvement to eliminate errors and the risk of undue interference with any individual's rights. Therefore, the SPoC or other persons involved in the process should bring to the immediate attention of the SRO either a recordable error or a reportable error and the necessary action can then be taken in line with the COP.

29.3. Where material is disclosed by a CSP in error, which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it, that material and any copy of it should be destroyed as soon as the report to the Commissioner has been made.

29.4. An error can only occur after:

- The granting of an Authorisation and the acquisition of data has been initiated, or
- Notice has been given and the Notice has been served on a CSP in writing, electronically or orally.

29.5. It is important to apply the procedures correctly to reduce the risk of an error occurring. Where any error occurs, a record will be kept.

29.6. There are two types of errors:

- Reportable
- Recordable

## 30. REPORTABLE ERROR

30.1. Where CD is acquired or disclosed wrongly a report must be made to the IPCO. Such errors can have very significant consequences on an affected individual's rights with details of their private communications being disclosed to a public authority and, in extreme circumstances, being wrongly detained or wrongly accused of a crime as a result of that error.

30.2. Examples can include:

- An Authorisation or Notice made for a purpose, or for a type of data which the relevant public authority cannot call upon or seek, under the Act;
- Human error, such as incorrect transposition of information from an application to an Authorisation or Notice;
- Disclosure of the wrong data by a CSP when complying with a Notice;
- Acquisition of the wrong data by a public authority when engaging in conduct specified in an Authorisation;

30.3. Any reportable error must be reported to the SRO as soon as it is identified and then a report will be made to the IPCO within five working days. The report must contain the unique reference number of the Notice and details of the error, plus an explanation how the error occurred and indicate whether any unintended collateral intrusion has taken place. It will also provide an indication of the steps that will take place to prevent a reoccurrence. The 'reporting an error by accredited SPoC form' (CD5) should be used for this purpose.

30.4. If the report relates to an error made by a CSP, the Authority must still report it. The CSP should also be notified to enable them to investigate the cause.

## 31. RECORDABLE ERROR

31.1. In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the Council and NAFN of such occurrences. These records must be available for inspection by the IPCO.

31.2. The staff involved in the process of acquiring CD must report errors once they have been identified. It will not be acceptable for the error to be ignored.

31.3. Examples can include:

- A Notice given, which is impossible for a CSP to comply with and an attempt to impose the requirement has been undertaken by the public authority;
- Failure to review information already held, for example unnecessarily seeking the acquisition or disclosure of data already acquired or obtained for the same investigation or operation, or data for which the requirement to acquire or obtain it is known to be no longer valid.

## 32. EXCESS DATA

32.1. Where authorised conduct results in the acquisition of excess data, the excess data acquired or disclosed should only be retained by the public authority where appropriate to do so – for example in relation to a criminal investigation.

32.2. Where a public authority is bound by the Criminal Procedure and Investigations Act 1996 and the IPA Codes of Practice, there will be a requirement to record and retain

data which is relevant to a criminal investigation, even if that data was disclosed or acquired beyond the scope of a valid authorisation.

32.3. If having reviewed the excess data, it is intended to make use of the excess data in the course of the investigation or operation, an applicant must set out the reason(s) for needing to use that material in an addendum to the application upon which the authorisation or notice was originally granted or given. The SRO (or a person of equivalent grade or authority) will review the data and consider whether it is necessary and proportionate for the excess data to be used in the investigation.

32.4. As with all CD, the requirements of relevant data protection legislation and data retention policies should be adhered to in relation to excess data.

## 33. RECORD KEEPING AND SECURITY OF DATA

33.1. All the records and any data obtained must be kept secure and confidential.

33.2. The Council must retain copies of all Applications, as a printed copy of the online application submitted via NAFN, and any other associated documentation where copies have been provided by the NAFN SPoC. This will be coordinated by the RIPA Coordinating Officer/DP who also holds copies of applications for surveillance as per the Council's overarching RIPA Policy.

33.3. The copy application records must be available for inspection by the IPCO. The IPCO will also be able to obtain copies direct from NAFN.

33.4. The SRO will have access to all of these forms as and when required.

33.5. The Council must also keep a record of the following:

- Number of applications submitted to the NAFN SPoC;
- Number of applications submitted to the NAFN SPoC which were referred back to the Applicant for amendment or declined by the SPoC;
- The reason for any amendments being required or application being declined by the SPoC;
- The reason for any referrals back or rejections;
- Whether any part of the application relates to a person who is member of a profession that handles privileged or otherwise confidential information (such as a Medical Doctor, Lawyer, Journalist, MP or Minister of Religion (and if so, which profession);

## 34. CRIMINAL PROCEDURES AND INVESTIGATIONS ACT 1996 (CPIA)

34.1. The Criminal Procedure and Investigations Act 1996 (CPIA) requires that material which is obtained in the course of an investigation and which may be relevant to the investigation must be recorded, retained and revealed to the prosecutor. Therefore, all material relating to the accessing of CD falls under these provisions. If the Applicant is not the Disclosure Officer in the case, they must make the Disclosure Officer aware of all of the material relating to the application and acquisition of the CD.

34.2. All material which may be relevant to the investigation must be retained until a decision is taken whether to institute proceedings against a person for an offence and if prosecuted, at least until the accused is acquitted or convicted, or the prosecutor decides not to proceed with the case and in line with the Council's Data Retention Policies.

34.3. Where the accused is convicted, the data which is relevant must be retained at least for six months from the date of conviction, and where the court imposes a custodial sentence, until the convicted person is released from custody.

34.4. If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction and in line with the Council's Data Retention Policies.

## 35. DATA PROTECTION ACT 2018 (DPA) AND THE GENERAL DATA PROTECTION REGULATIONS (GDPR)

35.1. CD acquired or obtained under the provisions of the IPA, and all copies, extracts and summaries of it must be handled and stored securely in line with the requirements of data protection legislation and regulations.

35.2. There is no provision in the IPA preventing CSPs from informing individuals about the disclosure of their CD in response to a Subject Access Request. However, a CSP may exercise certain exemptions to the right of subject access. If a CSP receives a Subject Access Request they must carefully consider whether in the particular case, disclosure of the fact of the Notice would be likely to prejudice the prevention or detection of crime.

35.3. Should a request for advice be made from a CSP to the SPoC regarding a disclosure, the SPoC will consult with the Data Protection Officer for the Council and the Applicant if necessary before a decision is made. Each case should be examined on its own merits.

35.4. Equally, these rules will apply should a Subject Access Request be made from an individual where material under this legislation is held by the Council.

35.5. A record will be made of the steps taken in determining whether disclosure of the material would prejudice the apprehension or detection of offenders. This might be useful in the event of the data controller having to respond to enquiries made subsequently by the Information Commissioner and the courts etc.

## 36. OVERSIGHT

36.1. The IPA provides for an Investigatory Powers Commissioner (IPC) whose remit includes providing comprehensive oversight of the use of the powers contained within the IPA and adherence to the practices and processes in the Code of Practice. They carry out inspections, and for the purposes of Council applications, carry out inspections of NAFN. Should they have any concerns regarding an application they would contact the relevant staff involved at the Council. It is possible that they could also inspect the Council.

36.2. It is important to note that should the Commissioner establish that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under the IPA in relation to the acquisition or disclosure of CD, he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable him or her to effectively engage the Tribunal.

## 37. COMPLAINTS

37.1. The Information Commissioner is responsible for the oversight of the security, integrity and destruction of data retained in accordance with the Act. Any concerns about compliance with data protection and related legislation should be passed to the ICO at the following address:

37.2.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
0303 123 1113
www.ico.org.uk

The Investigatory Powers Tribunal (IPT) has jurisdiction to consider and determine complaints regarding public authority use of investigatory powers, including those covered by the IPA.

The IPT is an independent body made up of members of the judiciary and senior members of the legal profession. Following receipt of a complaint the IPT can undertake its own enquiries and complaints and can demand access to all information necessary. Information regarding the IPT and how to make a complaint can be found at www.ipt-uk.com, or by writing to:

The Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

## 38. STRATEGY AND POLICY REVIEW

38.1. The Counter Fraud Unit will review and amend this Policy as necessary to ensure that it continues to remain compliant and meets legislative requirements and the vision of the Council.

Responsible Department: Counter Fraud Unit

Date: April 2019

Review frequency as required by legislative changes / every year.

COTSWOLD DISTRICT COUNCIL

| | |
|---|---|
| Council name | **COTSWOLD DISTRICT COUNCIL** |
| Name and date of Committee | **AUDIT COMMITTEE – 14 NOVEMBER 2019** |
| Report Number | **AGENDA ITEM 13** |
| Subject | **CORPORATE RISK REGISTER UPDATES** |
| Wards affected | ALL |
| Accountable member | Councillor Joe Harris, Leader<br>Email: joe.harris@cotswold.gov.uk |
| Accountable officer | Nigel Adams Head of Paid Service<br>Tel: 01285 623202 Email: nigel.adams@cotswold.gov.uk |
| Summary/Purpose | To update the Committee on the changes to the Council's corporate risk register at the end of 2019/20 Q2 |
| Annexes | Annex A Corporate Risk Register 2019/20 Q2 |
| Recommendation/s | Please write recommendations using letters and italics as below.<br>*a) To note the updates to the Council's corporate risk register* |
| Corporate priorities | Always refer to named priorities from the corporate plan. |
| Key Decision | NO |
| Exempt | NO |
| Consultees/ Consultation | None |

## 1. BACKGROUND

**1.1.** The Corporate Risk Register was updated by the risk owners during October and reviewed by the Shared Risk Management group (SRMG), comprising the partner Councils' statutory officers and the Publica Directors, on 21 October 2019.

**1.2.** The Corporate Risk Register is attached at Annex A.

**1.3.** The SRMG also has oversight of Publica's strategic risk register and high scoring risks from the Transformation Programme risk register. The risk registers, when considered together with the partner Councils' corporate risk registers provide SRMG with an overview of risk across the organisations, and enables it to manage risk more effectively.

## 2. FINANCIAL IMPLICATIONS

**2.1.** There are no direct financial implications

## 3. LEGAL IMPLICATIONS

**3.1.** None

## 4. RISK ASSESSMENT

**4.1.** None

## 5. EQUALITIES IMPACT (IF REQUIRED)

**5.1.** Not required

## 6. CLIMATE CHANGE IMPLICATIONS (IF REQUIRED)

**6.1.** Not required

## 7. ALTERNATIVE OPTIONS

**7.1.** None

## 8. BACKGROUND PAPERS

**8.1.** None

**Cotswold District Council - Corporate Risk Register 2019-20 Q2**

Overarching strategic risks

| Risk Code | Description | Risk Factors | Internal Controls | Current Impact | Current Likelihood | Current Rating | Last Review Date | Latest Note | Assigned To |
|---|---|---|---|---|---|---|---|---|---|
| CRR-D01-017 | If the UK leaves the European Union with no deal then there could be a disruption to the delivery of Council services which would impact on residents/communities | Community<br>Financial<br>Performance | Support from the LGA<br><br>Local Resilience Forum<br><br>Government funding to support Councils<br><br>Business Continuity Plans<br><br>Service specific planning - Publica ERS, Ubico and GLL<br><br>Publica Executive Director undertaking role of Brexit Lead Officer as per requirement from MHCLG | 3 | 3 | 9 | 07-Oct-19 | 07-Oct-19 No change in rating. The current date for exiting is 31 October and the new government is committed to leaving on that date. All LRF/SCG meetings are on hold at the present time but updates are reviewed as and when they are provided. Government (via MHCLG) is escalating preparations for leaving with or without a deal. A lead officer has been designated to represent the council in communications with central government and updates are being provided on a regular basis. A 'Brexit' Risk Register has been prepared for CDC and is reviewed on a weekly basis by the Brexit Planning Group. | Executive Director - Commissioning; Head of Paid Service |
| CRR-D01-018 | If the Government does not provide adequate funding to the Council to enable the Council to fulfil new expectations of the Council's role in preparations for the UK exit from the EU, there could be negative implications on the Council's reputation or the Council's finances | Financial<br>Community | Publica Executive Director undertaking role of Brexit Lead Officer as per requirement from MHCLG<br><br>Local Resilience Forum<br><br>Government funding | 3 | 3 | 9 | 07-Oct-19 | 07-Oct-2019 Secretary of State has written to the Council setting out his expectations of the role the Council should fulfil in preparations for the UK leaving the EU. £53k has been provided to date by the government to CDC to fund its Brexit preparations. | Executive Director - Commissioning; Head of Paid Service |

| Risk Code | Description | Risk Factors | Internal Controls | Current Impact | Current Likelihood | Current Rating | Last Review Date | Latest Note | Assigned To |
|---|---|---|---|---|---|---|---|---|---|
| CRR-D01-014 | If the Government imposes legislative changes that are not expected then it could have an impact on the Council's finances and other resources | Financial<br>Community | Horizon scanning<br><br>Professional publications<br><br>Four year funding settlement | 3 | 3 | 9 | 07-Oct-19 | 07-Oct-2019 No change in rating. The Council responded to the consultation on Defra's Waste and Resources strategy. The Strategy suggests that garden waste collection should be free which if imposed would have a significant financial impact on the Council. Defra published its consultations response to the Resources and Waste Strategy on 23 July. There are likely to be further developments with Statute once Brexit is concluded. Any financial implications will be considered as part of the update to the Council's MTFS | Chief Finance Officer |
| CRR-D01-019 (new) | If there are insufficient resources to deliver the objectives of the new Corporate Strategy and Plan then the expectations of our communities may not be met resulting in lower satisfaction and reputational damage | Financial<br>Community<br>Reputational | Medium Term Financial Strategy | 3 | 3 | 9 | 07-Oct-19 | New risk added in Q2. The financial implications of the Council's new Corporate Strategy will be developed over coming months and will feed into the refresh of the Medium Term Financial Strategy.<br><br>This risk links to risk CRR-D02-028 regarding the Local Government Funding Settlement over the Medium Term. This is the biggest risk to the deliverability of the objectives in the new Corporate Strategy. | Chief Finance Officer |
| CRR-D01-016 | If the Council fails to successfully implement the Local Plan and new National Planning Framework then central government may intervene and/or speculative planning applications may increase | Financial<br>Reputational | Local Plan Adopted in Aug 2018.<br><br>Local Plan Programme Board reconvened with updated Terms of Reference and membership | 3 | 1 | 3 | 04-Oct-19 | 04-Oct-2019 No change in rating. On-going monitoring of the housing supply and delivery indicates that we are on target. New programmes of work are being developed to ensure clarity of timeframes and resource requirements as part of the local plan review. | Group Manager - Strategic Support |

Financial management & control

| Risk Code | Description | Risk Factors | Internal Controls | Current Impact | Current Likelihood | Current Rating | Last Review Date | Latest Note | Assigned To |
|---|---|---|---|---|---|---|---|---|---|
| CRR-D02-028 | If the Local Government settlement over the medium term is unfavourable then the Council's savings target may need to increase | Financial | Medium Term Financial Strategy<br><br>Capped value of New Homes Bonus in MTFS (mitigates against fall in housing development)<br><br>2020 Vision Programme/shared working<br><br>Four year funding settlement | 5 | 4 | 20 | 07-Oct-19 | 07-Oct-2019 No change in rating. The MTFS is currently in the process of being updated. A one-year Spending Round 2019 has been announced which is indicating a roll-forward of funding from 2019/20 with an inflationary increase. New Homes Bonus awarded for 2020/21 will be for one year only (no legacy payments from 2021/22 due to implementation of Fairer Funding changes). The significant changes to LG Funding (75% Business Rate Retention, Business Rate Reset, Fairer Funding Review and new Spending Round) have been delayed until 2021/22.<br><br>Members and Officers are working on contingency plans to address the potential funding gap from 2021/22. | Chief Finance Officer |
| CRR-D02-018 | If unavoidable budget pressures exceed provision within the MTFS then the Council may need to: find additional income or savings, use its reserves,or there may be pressures on services or tax levels and agreed budget targets will not be achieved | Financial | Service Delivery Planning<br><br>Budgetary control system<br><br>CT/HoS consider financial pressures<br><br>Key variances reported to Cabinet and Overview and Scrutiny Committee | 4 | 5 | 20 | 07-Oct-19 | 07-Oct-2019 No change in rating. The MTFS is currently being updated and will include significant additional costs of the new waste service from 2020/21.<br><br>The Council has announced a Climate Emergency and financial resources will be required to enable the Council to take action. Funding for a Climate Change Manager will be included in the update to the MTFS. One-off funding has been made available from earmarked reserves to fund research which will enable the Council to develop a costed action plan.<br><br>Members and Officers are working on a plan to increase income to the Council to fund both new objectives from the new Corporate Strategy and to bridge the expected funding gap from 2021 as a result of changes to local government funding. | Chief Finance Officer |

| Risk Code | Description | Risk Factors | Internal Controls | Current Impact | Current Likelihood | Current Rating | Last Review Date | Latest Note | Assigned To |
|---|---|---|---|---|---|---|---|---|---|
| CRR-D02-030 | If Ubico is unable to deliver services to the required standard or to budget then it could damage the Council's reputation and result in additional costs for the Council | Financial<br>Reputational | Service management<br><br>Performance monitoring<br><br>Service risk registers | 4 | 5 | 20 | 07-Oct-19 | 07-OCT-2019 No change in rating. The waste fleet has deteriorated before expected resulting in high levels of breakdown, and as a consequence is impacting on residents and increasing service costs. The fleet is being re-procured as part of a new service. Modelled costs for the new service were agreed at Council in December and embedded in the budget in February, however, costs have been reviewed and estimates revised. There are elements such as fleet numbers and tonnages which are based on estimates and may be subject to change which could increase costs. The new service will now launch in March 2020 but new vehicles will go into service as soon as they are received in the Autumn replacing vehicles in poor condition. | Group Manager - Commissioning |
| CRR-D02-027 | If Publica does not deliver the agreed objectives in accordance with its business plan then the planned savings for the Council would not be delivered and consequently there would be a risk that services could not be delivered in line with the budget | Financial<br>Reputational | Programme Board<br><br>Local Political Support<br><br>National Political Support<br><br>Early Engagement with employees and Unions<br><br>Funding provided to develop detailed business case | 3 | 4 | 12 | 07-Oct-19 | 07-Oct-2019 Likelihood increased from 2 to 4. At the end of Q1, good progress was being made in delivering the savings of £930,000 included in the revenue budget for 19/20 and a small underspend was reported. Progress in preparing actions to deliver against business case targets for 2020/21 has not yet identified sufficient deliverables to give assurance that the remaining business case and MTFS savings for the councils will be achievable in 2020/21. | Head of Paid Service; Managing Director |

| Risk Code | Description | Risk Factors | Internal Controls | Current Impact | Current Likelihood | Current Rating | Last Review Date | Latest Note | Assigned To |
|---|---|---|---|---|---|---|---|---|---|
| CRR-D02-024 | If the Council is unable to meet the savings required to balance the budget then it may need to make unplanned use of revenue reserves, raise council tax, find further savings and/or cut services | Financial<br>Performance<br>Community | Regular meetings with Members and Cabinet<br><br>MTFS and budget process<br><br>CT/SMT discussions and lead<br><br>Vision 2020 programme | 3 | 3 | 9 | 07-Oct-19 | 07-Oct-2019 Likelihood reduced from 4 to 3. At the end of Q1, the Council's financial performance was in line with budget expectations and Publica was on target to deliver the savings for Q1.<br><br>The level of savings required as a result of changes to local government funding which will now come into effect in 2021/22 remains unclear. The Council is developing contingency plans to deliver the savings, or generate additional income, required from changes to local government funding | Chief Finance Officer |
| CRR-D02-029 | If contractors do not meet their obligations under key contracts then it could lead to a fall in service standards, reduced customer service or a failure to meet legal requirements | Financial<br>Reputational | Robust and effective contract management to ensure standards and requirements in contracts are met and any failings are identified and addressed quickly and effectively<br><br>Regular meetings to review performance/standards | 3 | 3 | 9 | 07-Oct-19 | 07-Oct-2019 No change in rating. An internal audit report has identified improvement in procurement and contract management to be implemented. | Group Manager - Commissioning |
| CRR-D02-005 | If there is a legal challenge to any of the Council's decisions or actions then there may be financial or policy implications | Financial<br>Legal<br>Reputational | Managerial advice and supervision<br><br>Legal advice and effective role of monitoring officer<br><br>Robust internal procedures<br><br>200k in MTFS for planning appeals | 3 | 2 | 6 | 09-Oct-19 | 09-Oct-2019 No change in rating | Head of Legal |

| Risk Code | Description | Risk Factors | Internal Controls | Current Impact | Current Likelihood | Current Rating | Last Review Date | Latest Note | Assigned To |
|---|---|---|---|---|---|---|---|---|---|
| CRR-D02-002 | If the Council fails to meet income targets then it may need to make unplanned use of revenue reserves, raise council tax, find further savings and/or cut services | Financial<br>Performance<br>Community | Systems of budgetary control<br><br>Appropriate marketing of services and consideration of effective charging levels<br><br>Project management arrangements | 3 | 3 | 9 | 07-Oct-19 | 7-Oct-2019 Impact increased from 2 to 3 as development control income is significantly under the budget expectation. Income budget will be reviewed as part of update of MTFS. | Chief Finance Officer |
| CRR-D02-017 | If the level of pay inflation exceeds provision in the MTFS then the Council may need to make unplanned use of revenue reserves, raise council tax, find further savings and/or cut services | Financial | National negotiations on pay award | 3 | 3 | 9 | 07-Oct-19 | 07-Oct-2019 Impact and Likelihood increased from 2 to 3 to reflect pressure on the inflation assumption within the MTFS. Unions have submitted a claim of 10% for 2020. This risk will be kept under review as the pay claim progresses. | Chief Finance Officer |
| CRR-D02-023 | If there was a civil emergency in the District then there could be a financial burden on the Council in responding to it | Financial | Mutual aid arrangements would enable support and reduce the resource burden on one individual council<br><br>The Belwin scheme enables costs incurred over a threshold (approx. £22K) to be reclaimed<br><br>Insurance of council's assets and some loss income<br><br>General Fund Working Balance<br><br>Flood engineering schemes in place to minimise the impact of severe weather and reduce the risk of property flooding | 2 | 3 | 6 | 01-Oct-19 | 01-Oct-19 No change in rating. There are good internal controls in place to help mitigate this financial risk | Group Manager - Strategic Support |

## Customer focus

| Risk Code | Description | Risk Factors | Internal Controls | Current Impact | Current Likelihood | Current Rating | Last Review Date | Latest Note | Assigned To |
|---|---|---|---|---|---|---|---|---|---|
| CRR-D03-007 | If the Council does not consult properly, or Publica does not consult properly on the Council's behalf, then the Council's decisions could be challenged | Community<br>Reputational<br>Legal<br>Financial | Press and PR officer<br><br>Cotswold News<br><br>Engagement strategy<br><br>Neighbourhood coordination meetings<br><br>Annual Town & Parish council meetings<br><br>Annual Budget consultation | 3 | 2 | 6 | 07-Oct-19 | 07-Oct-2019 No change in rating. Consultation on Rugby Club parking project undertaken prior to Planning application being submitted and determined. Several consultations related to the Waterloo car park have taken place and will continue. No new consultations planned until later in the year on the budget | Head of Paid Service |

## Organisational learning, staffing & development

| Risk Code | Description | Risk Factors | Internal Controls | Current Impact | Current Likelihood | Current Rating | Last Review Date | Latest Note | Assigned To |
|---|---|---|---|---|---|---|---|---|---|
| CRR-D04-003 | If Publica or the Council is unable to recruit suitable staff and retain them, particularly in some key service areas then the level of service delivery may be reduced | Performance<br>Financial<br>Reputational<br>Community | Financial incentives (market force supplement scheme)<br><br>Work with partners to address skill shortages | 3 | 3 | 9 | 30-Sep-19 | 30-Sep-2019 No change in rating. Quarterly performance reports are shared with Joint Management Team so any necessary mitigation to maintain service delivery levels can be discussed. Some difficulty recruiting senior staff in certain professions, e.g. Planning & Building Control. Monthly HR reports to Exec also highlight recruitment. An apprentice scheme is in place and an intern and graduate scheme has commenced. Implementation of the new pay and grading structure which will provide more flexibility in rewarding staff will take place later this financial year. | Head of Paid Service; Managing Director |
| CRR-D04-010 | If secondments to posts in the Transformation team are not backfilled then the level of service delivery in some services may be reduced | Performance<br>Reputational<br>Community | Flexible working<br><br>Performance management framework<br><br>Partnership working | 3 | 3 | 9 | 30-Sep-19 | 30-Sep-2019 No change in rating. A review has been undertaken and concluded that there was no impact on the 'day job'. Customer satisfaction rate via face to face and telephone channels was high at 100% and 94% in Q2 | Head of Paid Service; Managing Director |

| Risk Code | Description | Risk Factors | Internal Controls | Current Impact | Current Likelihood | Current Rating | Last Review Date | Latest Note | Assigned To |
|---|---|---|---|---|---|---|---|---|---|
| CRR-D04-009 | If staff morale and motivation is low in Publica then the level of service delivered may be reduced in some services | Performance<br>Community | Communication<br><br>Comprehensive consultation and engagement process<br><br>Change management training<br><br>Joint Liaison Forum<br><br>2020 Engagement Strategy | 3 | 3 | 9 | 07-Oct-19 | 07-Oct-2019 No change to rating. Changes to Terms and Conditions have been agreed with Unions and have been implemented reducing one of the areas that was causing concerns for staff. Amendments to the pay and grading proposals were made during the summer and further discussions held with unions. Whilst working relationships with unions remain strong they were unable to support a ballot on the proposals and therefore Publica has commenced a direct 45 day consultation with staff with a view to implementing the scheme from 1 April 2020. Completion of the pay and grading proposals should complete the technical aspects of the organisational design changes and allow the completion of this major part of the transformation programme, reducing uncertainty for employees and improving organisational morale. | Head of Paid Service; Managing Director |
| CRR-D04-011 | If key Officers in the Council (such as the Head of Paid Service, Chief Finance Officer or Monitoring Officer) are not available, the Council may not be able to respond effectively to urgent matters which could result in reputational or financial damage | Legal<br>Financial<br>Reputational | Deputy CFO and Monitoring Officers in place<br><br>Support from Shared Legal Services team- employed by the Publica Partner Councils<br><br>Support from professionals within Publica (e.g. Strategic Directors, Group Managers, Accountants, HR)<br><br>Support available from other Statutory Officers from across the Publica Partner Councils<br><br>Effective working relationships between Officers and Cabinet Members | 3 | 2 | 6 | 07-Oct-19 | 07-Oct-2019 No change to rating. | Head of Paid Service; Managing Director |

Business processes

| Risk Code | Description | Risk Factors | Internal Controls | Current Impact | Current Likelihood | Current Rating | Last Review Date | Latest Note | Assigned To |
|---|---|---|---|---|---|---|---|---|---|
| CRR-D05-001 | If the Council's data is of poor quality or it does not make appropriate use of its data then the decisions it makes may be flawed | Reputational<br>Financial<br>Legal<br>Performance<br>Community | Internal processes and self assessments<br><br>Internal audit assurance and support<br><br>Dedicated staff resource on performance management and data quality<br><br>Performance Management Framework | 3 | 3 | 9 | 30-Sep-19 | 30-Sep-2019 No change in rating. Data quality and the use of information is being addressed as part of the organisational re-design. A Business Manager has now been appointed who is responsible for business analytics and a Lead officer for information | Chief Finance Officer; Head of Paid Service |
| CRR-D05-016 | If the Council does not comply with relevant Information Management legislation including the new GDPR and Transparency Agenda then the government may intervene which could have a reputational impact on the Council | Financial<br>Reputational<br>Legal | Access to Information Policy<br><br>FOI process reviewed<br><br>LGA guidance and supporting documents & templates | 3 | 3 | 9 | 01-Oct-19 | 01-Oct-2019 No change in rating. Progress on the GDPR action plan is being reported to the Council and Publica, and includes advice and guidance at staff inductions. The online training programme has now been successfully rolled out across Publica | Data Protection Officer; Head of Paid Service |
| CRR-D05-019 | If contractors do not comply with health and safety requirements then there could be both financial and reputational implications for the Council | Financial<br>Reputational | Contract management in place to ensure appropriate measures such as risk assessments, appropriate policies, and training is in place.<br><br>GOSS Health and Safety business partners provide advice and support | 4 | 2 | 8 | 07-Oct-19 | 07-Oct-2019 No change in rating | Group Manager - Commissioning |

| Risk Code | Description | Risk Factors | Internal Controls | Current Impact | Current Likelihood | Current Rating | Last Review Date | Latest Note | Assigned To |
|---|---|---|---|---|---|---|---|---|---|
| CRR-D05-013 | If there is insufficient capacity to respond to an emergency then the Council may not be able to deal effectively during emergencies resulting in reputational damage | Reputational<br>Legal<br>Financial<br>Community<br>Performance | Contract terms with Everyone Active and GOSS e.g. use of leisure centre as a rest centre<br><br>Mutual aid arrangements<br><br>Good will of staff<br><br>Ward Members, Town & Parish Councillors on hand/training provided<br><br>Enhanced community resilience arrangements | 3 | 2 | 6 | 01-Oct-19 | 01-Oct-19 At the end of quarter 4 2018/19 the likelihood rating was increased to 2 to 3 because the nominated District Emergency Planning Liaison Officer (DEPLO) had left and a replacement was yet to start in post.<br><br>A new emergency management framework has been developed which includes two deputy DEPLOs for Cotswold District, as a well as an overall emergency planning lead for the Publica partnership.<br><br>The likelihood rating has therefore been reduced back to 2. | Head of Paid Service; Managing Director |
| CRR-D05-010 | If there is severe weather then the Council may be unable to deliver key services which could impact on residents | Performance<br>Community<br>Reputational | BCPs<br><br>Weather reports/national news<br><br>Remote working solution available to staff | 3 | 2 | 6 | 01-Oct-19 | 01-Oct-2019 No change in rating. All business continuity plans have been updated. | Head of Paid Service; Managing Director |
| CRR-D05-011 | If the Council's IT System / infrastructure failed due to cyber attacks and/or virus then system performance could be reduced leading to poor service delivery/financial impact | Performance<br>Financial<br>Legal<br>Reputational | Preventative measures introduced such as blocking of USB and other devices<br><br>Undertaken and passed a central government ICT audit, meeting the very high standards set for network security<br><br>Introduction of new / revised joint policies<br><br>Periodic staff awareness training<br><br>BCP in place and reviewed & tested | 3 | 2 | 6 | 01-Oct-19 | 01-Oct-2019 No change in rating. All Councils have PSN accreditation, which compliments the Cyber Essential Plus, which is a Government-backed, industry-supported scheme to help organisations protect themselves against common online threats | Group Manager - Business Support Services |

| Risk Code | Description | Risk Factors | Internal Controls | Current Impact | Current Likelihood | Current Rating | Last Review Date | Latest Note | Assigned To |
|---|---|---|---|---|---|---|---|---|---|
| CRR-D05-012 | If there is a loss of data (both on site and as a result of remote/mobile working) / security failure in our IT systems then it could lead to a reduced level of service and have a negative impact on the Council's reputation and finances | Performance<br>Financial<br>Legal<br>Reputational | Preventative measures introduced such as blocking of USB and other devices<br><br>Undertaken and passed a central government ICT audit, meeting the very high standards set for network security<br><br>Introduction of new / revised joint policies<br><br>Periodic staff awareness training<br><br>BCP in place and reviewed & tested | 3 | 2 | 6 | 01-Oct-19 | 01-Oct-2019 No change in rating. All Councils have PSN accreditation, which compliments the Cyber Essential Plus. The final module of the online training system (Bob's Business) has now been rolled out and completed by staff which is helping to reinforce the need for staff to be aware of their responsibilities with regards to data security, passwords and GDPR | Group Manager - Business Support Services |
| CRR-D05-014 | If the Council's buildings are destroyed then it would be unable to operate/deliver services which would impact on residents /communities | Reputational<br>Financial<br>Legal<br>Performance<br>Community | BCPs including ICT contingency plans<br><br>Remote access<br><br>Mutual aid through Shared working strategy<br><br>Insurance<br><br>Fail over protocol | 3 | 2 | 6 | 01-Oct-19 | 01-Oct-2019 No change in rating. All business continuity plans have been updated. | Group Manager - Strategic Support |

Longer term risks

| Risk Code | Description | Risk Factors | Internal Controls | Current Impact | Current Likelihood | Current Rating | Last Review Date | Latest Note | Assigned To |
|---|---|---|---|---|---|---|---|---|---|
| CRR-D06-002 | If Health and Safety procedures and risk assessments are not in place /being followed then staff could be injured undertaking Council duties which would impact on their health and wellbeing, affect their ability to work and create liability issues for the Council | Legal<br>Financial<br>Reputational | Health and Safety procedures<br><br>Access to weather forecasts<br><br>Lone workers policy<br><br>Business Continuity Plans | 4 | 2 | 8 | 30-Sep-19 | 30-Sep-2019 No change in rating. No reportable incidents to the Health & Safety Executive in the quarter. Fire Risk Assessments on all our buildings in Cirencester have been carried out; the results have been reported to the responsible person. H&S policy will be reviewed in October. All guidance documents for staff have been reviewed, and now awaiting approval. H&S will be a standard item on the Senior Managers' meeting each quarter | Head of Paid Service; Managing Director |

**(14) WORK PLAN 2019/20**

| COMMITTEE DATE | ITEMS |
|---|---|
| **30 January 2020** | Internal Audit Monitoring Report |
| | Grant Thornton Reports |
| | Capital, Investment and Treasury Management Strategies 2019/20 |
| | Accounting Policies |
| | Work Plan 2019/20 |
| | |
| **23 April 2020** | Grant Thornton Reports |
| | Grant Thornton Assurance |
| | Corporate Risk Register Updates |
| | Counter Fraud Unit Report and annual RIPA / IPA update |
| | Internal Audit Monitoring Report |
| | Draft Annual Governance Statement 2019/2020 |
| | 2020/21 Internal Audit Plan and Internal Audit Charter |
| | Work Plan 2019/20 |