

NOTICE OF MEETING

Meeting: AUDIT COMMITTEE

Date and Time: FRIDAY, 25 JANUARY 2019, AT 9.30 AM*

Place: COMMITTEE ROOM 1, APPLETREE COURT,
LYNDHURST

Telephone enquiries to: Lyndhurst (023) 8028 5000
023 8028 5588 - ask for Andy Rogers
E-mail: andy.rogers@nfdc.gov.uk

PUBLIC PARTICIPATION:

*Members of the public may speak in accordance with the Council's public participation scheme:

- (a) immediately before the meeting starts, on items within the Committee's terms of reference which are not on the public agenda; and/or
 - (b) on individual items on the public agenda, when the Chairman calls that item.
- Speeches may not exceed three minutes. Anyone wishing to speak should contact the name and number shown above.

Bob Jackson
Chief Executive

Appletree Court, Lyndhurst, Hampshire. SO43 7PA
www.newforest.gov.uk

This Agenda is also available on audio tape, in Braille, large print and digital format

AGENDA

Apologies

1. MINUTES

To confirm the minutes of the meeting held on 26 October 2018 as a correct record.

2. DECLARATIONS OF INTEREST

To note any declarations of interest made by members in connection with an agenda item. The nature of the interest must also be specified.

Members are asked to discuss any possible interests with Democratic Services prior to the meeting.

3. PUBLIC PARTICIPATION

To note any issues raised during the public participation period.

4. EXTERNAL AUDIT PLAN (Pages 1 - 36)

To receive the External Audit Plan.

5. 2019 TREASURY MANAGEMENT STRATEGY (Pages 37 - 54)

To consider the proposed Treasury Management Strategy for 2019/20.

6. CERTIFICATION OF CLAIMS AND RETURNS ANNUAL REPORT (Pages 55 - 68)

To receive the Certification of Claims and Returns Annual Report.

7. INTERNAL AUDIT PROGRESS AGAINST THE AUDIT PLAN (Pages 69 - 84)

To note the Internal Audit Progress report.

8. REGULATION OF INVESTIGATORY POWERS ACT 2000 POLICY (Pages 85 - 130)

To receive a summary of the Council's use of its powers under the Regulation of Investigatory Powers Act (RIPA) 2000 and to consider updated policies for Surveillance and Acquisition of Communications Data.

9. AUDIT COMMITTEE WORK PLAN (Pages 131 - 132)

To consider the Audit Committee's Work Plan.

10. ANY OTHER ITEMS WHICH THE CHAIRMAN DECIDES ARE URGENT

To:

Councillors:

Councillors:

A D O'Sullivan (Chairman)
J G Ward (Vice-Chairman)
A R Alvey
W G Andrews

J D Heron
Mrs E L Lane
Miss A Sevier
C A Wise

New Forest District Council Audit planning report

Year ended 31 March 2019

January 2019



Private and Confidential
Members of the Audit Committee
New Forest District Council
Appletree Court
Beaulieu Road
Lyndhurst
S043 7PA

08 January 2019

Dear Audit Committee Members

Audit planning report

We are pleased to attach our Audit Plan which sets out how we intend to carry out our responsibilities as auditor. Its purpose is to provide the Audit Committee with a basis to review our proposed audit approach and scope for the 2018/19 audit in accordance with the requirements of the Local Audit and Accountability Act 2014, the National Audit Office's 2015 Code of Audit Practice, the Statement of Responsibilities issued by Public Sector Audit Appointments (PSAA) Ltd, auditing standards and other professional requirements. It is also to ensure that our audit is aligned with the Committee's service expectations.

This plan summarises our initial assessment of the key risks driving the development of an effective audit for the Council, and outlines our planned audit strategy in response to those risks.

This report is intended solely for the information and use of the Audit Committee and management, and is not intended to be and should not be used by anyone other than these specified parties.

We welcome the opportunity to discuss this report with you on 25 January 2019 as well as understand whether there are other matters which you consider may influence our audit.

Yours faithfully

Kevin Suter

Associate Partner

For and on behalf of Ernst & Young LLP

Contents

01	Overview of our 2018/19 audit strategy	02	Audit risks	03	Value for Money Risks	04	Audit materiality	05	Scope of our audit
									
	06	Audit team	07	Audit timeline	08	Independence	09	Appendices	

Public Sector Audit Appointments Ltd (PSAA) issued the "Statement of responsibilities of auditors and audited bodies". It is available from the PSAA website (<https://www.psa.co.uk/audit-quality/statement-of-responsibilities/>). The Statement of responsibilities serves as the formal terms of engagement between appointed auditors and audited bodies. It summarises where the different responsibilities of auditors and audited bodies begin and end, and what is to be expected of the audited body in certain areas.

The "Terms of Appointment and further guidance (updated April 2018)" issued by the PSAA sets out additional requirements that auditors must comply with, over and above those set out in the National Audit Office Code of Audit Practice (the Code) and in legislation, and covers matters of practice and procedure which are of a recurring nature.

This report is made solely to the Audit Committee and management of New Forest District Council in accordance with the statement of responsibilities. Our work has been undertaken so that we might state to the Audit Committee, and management of New Forest District Council those matters we are required to state to them in this report and for no other purpose. To the fullest extent permitted by law we do not accept or assume responsibility to anyone other than the Audit Committee and management of New Forest District Council for this report or for the opinions we have formed. It should not be provided to any third-party without our prior written consent.



Page 4

01

Overview of our 2018/19 audit strategy



Overview of our 2018/19 audit strategy

The following 'dashboard' summarises the significant accounting and auditing matters outlined in this report. It seeks to provide the Audit Committee with an overview of our initial risk identification for the upcoming audit and any changes in risks identified in the current year.

Audit risks and areas of focus

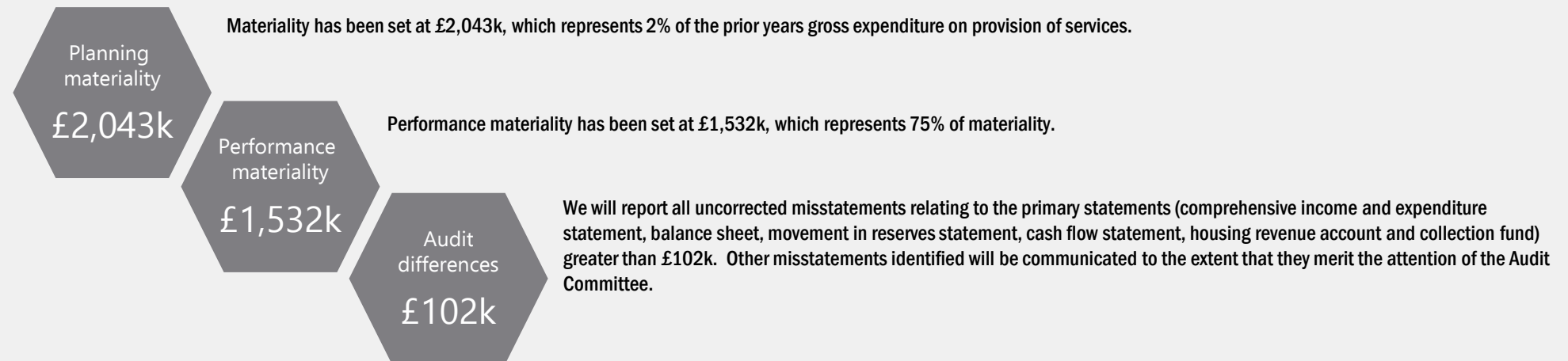
Risk / area of focus	Risk identified	Change from PY	Details
Misstatements due to fraud or error	Fraud risk	No change in risk or focus	As identified in ISA 240, management is in a unique position to perpetrate fraud because of its ability to manipulate accounting records directly or indirectly and prepare fraudulent financial statements by overriding controls that would otherwise appear to be operating effectively. In addition to our overall response, we consider where these risks may manifest themselves and identify separate fraud risks as necessary below.
Risk of fraud in revenue recognition – inappropriate capitalization of revenue expenditure	Fraud risk	No change in risk or focus	Under ISA240 there is a presumed risk that revenue may be misstated due to improper recognition of revenue. In the public sector, this requirement is modified by Practice Note 10, issued by the Financial Reporting Council, which states that auditors should also consider the risk that material misstatements may occur by the manipulation of expenditure recognition. Our judgement is the significant risk at the Council relates to the improper capitalisation of revenue expenditure.
Pension Liability Valuation	Inherent risk	No change in risk or focus.	The Local Authority Accounting Code of Practice and IAS19 require the Council to make extensive disclosures within its financial statements regarding its membership of the Local Government Pension Scheme administered by Hampshire County Council. The Council's pension fund asset is a material estimated balance and the Code requires that this asset be disclosed on the Council's balance sheet. The information disclosed is based on the IAS 19 report issued to the Council by the actuary to the County Council. Accounting for this scheme involves significant estimation and judgement and therefore management engages an actuary to undertake the calculations on their behalf. ISAs (UK and Ireland) 500 and 540 require us to undertake procedures on the use of management experts and the assumptions underlying fair value estimates.

Overview of our 2018/19 audit strategy

Risk / area of focus	Risk identified	Change from PY	Details
Valuation of Land and Buildings	Inherent risk	No change in risk or focus.	The fair value of Property, Plant and Equipment (PPE) represents a significant balance in the Council's accounts and are subject to valuation changes, impairment reviews and depreciation charges. Management is required to make material judgements and apply estimation techniques to calculate the year-end balances recorded in the balance sheet.
Valuation of Council Dwellings and Depreciation	Inherent risk	No change in risk or focus.	The fair value of Council Dwellings represents a significant balance in the Council's accounts and are subject to valuation changes, impairment reviews and depreciation charges. Management is required to make material judgements and apply estimation techniques to calculate the year-end balances recorded in the balance sheet.
New Accounting Standards	Inherent risk	New risk identified this year.	IFRS 9 (Financial Instruments) and IFRS 15 (Revenue from contracts) apply from 1 April 2018. We will assess the impact of these new standards to determine whether they have been appropriately implemented by the Council.

Page 6

Materiality



Overview of our 2018/19 audit strategy

Audit scope

This Audit Plan covers the work that we plan to perform to provide you with:

- Our audit opinion on whether the financial statements of New Forest District Council give a true and fair view of the financial position as at 31 March 2019 and of the income and expenditure for the year then ended; and
- Our conclusion on the Council's arrangements to secure economy, efficiency and effectiveness.

We will also review and report to the National Audit Office (NAO), to the extent and in the form required by them, on the Council's Whole of Government Accounts return.

Our audit will also include the mandatory procedures that we are required to perform in accordance with applicable laws and auditing standards.

When planning the audit we take into account several key inputs:

- Strategic, operational and financial risks relevant to the financial statements;
- Developments in financial reporting and auditing standards;
- The quality of systems and processes;
- Changes in the business and regulatory environment; and,
- Management's views on all of the above.

By considering these inputs, our audit is focused on the areas that matter and our feedback is more likely to be relevant to the Council.

Audit team changes

Key changes to our team.



James Stuttaford (Audit Manager)

- James is an Assistant Manager within the UK&I Assurance practice, with over four years experience of LG audits as a team leader and now an assistant manager. He will be the key contact for your Finance Team.
- He is a member of The Institute of Chartered Accountants in England and Wales (ICAEW).



Page 8

02 Audit risks



Our response to significant risks

We have set out the significant risks (including fraud risks denoted by*) identified for the current year audit along with the rationale and expected audit approach. The risks identified below may change to reflect any significant findings or subsequent issues we identify during the audit.

Misstatements due to fraud or error*

What is the risk?

As identified in ISA 240, management is in a unique position to perpetrate fraud because of its ability to manipulate accounting records directly or indirectly and prepare fraudulent financial statements by overriding controls that would otherwise appear to be operating effectively.

What will we do?

- Inquiry of management about risks of fraud and the controls put in place to address those risks.
- Understanding the oversight given by those charged with governance of management's processes over fraud.
- Consideration of the effectiveness of management's controls designed to address the risk of fraud.

Performing mandatory procedures regardless of specifically identified fraud risks, including:

- Testing the appropriateness of journal entries recorded in the general ledger and other adjustments made in the preparation of the financial statements
- Assessing accounting estimates for evidence of management bias, and
- Evaluating the business rationale for significant unusual transactions.

In addition to our overall response, we consider where these risk may manifest themselves and identify separate fraud risks as necessary below.

Our response to significant risks

We have set out the significant risks (including fraud risks denoted by*) identified for the current year audit along with the rationale and expected audit approach. The risks identified below may change to reflect any significant findings or subsequent issues we identify during the audit.

Risk of fraud in revenue recognition - inappropriate capitalisation of revenue expenditure*

Financial statement impact

Inappropriate capitalization of revenue expenditure would decrease the net expenditure from the general fund, and increase the value of non-current assets.

What is the risk?

Under ISA 240 there is a presumed risk that revenue may be misstated due to improper revenue recognition. In the public sector, this requirement is modified by Practice Note 10 issued by the Financial Reporting Council, which states that auditors should also consider the risk that material misstatements may occur by the manipulation of expenditure recognition.

From our risk assessment, we have assessed that the risk manifest itself solely through the inappropriately capitalisation of revenue expenditure to improve the financial position of the general fund.

Capitalized revenue expenditure could then be inappropriately be funded through borrowing with only minimal MRP charges recorded in the general fund, deferring the expenditure for 30+ years when the borrowing is repaid. Alternately, it could also inappropriately be funded by capital receipts or grants, that should not be used to support revenue.

Inappropriate classification of revenue expenditure as REFUCS (revenue expenditure funded by capital under statute) could also have the same impact, removing the spend incorrectly from the general fund through applying statutory overrides.

What will we do?

Our approach will focus on:

- ▶ For significant additions we will examine invoices, capital expenditure authorisations, leases and other data that support these additions. We review the sample selected against the definition of capital expenditure in IAS 16.
- ▶ Reviewing the appropriateness of items classified as REFUCS
- ▶ We will extended our testing of items capitalized in the year by lowering our testing threshold. We will also review a larger random sample of capital additions below our testing threshold.
- ▶ Journal testing – we will use our testing of Journals to identify high risk transactions, such as items originally recorded as revenue expenditure and subsequently capitalised reclassified as REFUCS.

Other areas of audit focus

We have identified other areas of the audit, that have not been classified as significant risks, but are still important when considering the risks of material misstatement to the financial statements and disclosures and therefore may be key audit matters we will include in our audit report.

What is the risk/area of focus?	What will we do?
<p>Valuation of Land and Buildings</p> <p>The fair value of Property, Plant and Equipment (PPE) and Investment Properties (IP) represent significant balances in the Council's accounts and are subject to valuation changes, impairment reviews and depreciation charges. Management is required to make material judgemental inputs and apply estimation techniques to calculate the year-end balances recorded in the balance sheet.</p>	<p>We will:</p> <ul style="list-style-type: none"> • Consider the work performed by the Council's valuers, including the adequacy of the scope of the work performed, their professional capabilities and the results of their work; • Sample testing key asset information used by the valuers in performing their valuation (e.g. floor plans to support valuations based on price per square metre); • Consider the annual cycle of valuations to ensure that assets have been valued within a 5 year rolling programme as required by the Code for PPE and annually for IP. We have also considered if there are any specific changes to assets that have occurred and that these have been communicated to the valuer; • Review assets not subject to valuation in 2018/19 to confirm that the remaining asset base is not materially misstated; • Consider changes to useful economic lives as a result of the most recent valuation; and • Test accounting entries have been correctly processed in the financial statements,
<p>Valuation of Council Dwellings</p> <p>As with other Land and Buildings, the value of Council Dwellings in the Council's accounts are subject to valuation changes, impairment reviews and depreciation charges. Management is required to make material judgemental inputs and apply estimation techniques to calculate the year-end balances recorded in the balance sheet.</p> <p>During our 2017/18 audit we identified a judgemental difference in the Council's HRA depreciation calculation, which was amended by management.</p>	<p>We will:</p> <ul style="list-style-type: none"> • Evaluate the application of the Beacon Methodology; • Review any changes to the Council's HRA depreciation calculation; and • Test accounting entries have been correctly processed in the financial statements.

Other areas of audit focus

We have identified other areas of the audit, that have not been classified as significant risks, but are still important when considering the risks of material misstatement to the financial statements and disclosures and therefore may be key audit matters we will include in our audit report.

What is the risk/area of focus?

Pension Liability Valuation

The Local Authority Accounting Code of Practice and IAS19 require the Council to make extensive disclosures within its financial statements regarding its membership of the Local Government Pension Scheme administered by Hampshire County Council.

The Council's pension fund deficit is a material estimated balance and the Code requires that this liability be disclosed on the Council's balance sheet. At 31 March 2018 this totalled £95,024k.

The information disclosed is based on the IAS 19 report issued to the Council by the actuary to the County Council.

Accounting for this scheme involves significant estimation and judgement and therefore management engages an actuary to undertake the calculations on their behalf. ISAs (UK) 500 and 540 require us to undertake procedures on the use of management experts and the assumptions underlying fair value estimates.

What will we do?

We will:

- Liaise with the auditors of Hampshire Pension Fund, to obtain assurances over the information supplied to the actuary in relation to New Forest District Council;
- Assess the work of the Pension Fund actuary (Aon Hewitt) including the assumptions they have used by relying on the work of PWC - Consulting Actuaries commissioned by the National Audit Office for all Local Government sector auditors, and considering any relevant reviews by the EY actuarial team; and
- Review and test the accounting entries and disclosures made within the Council's financial statements in relation to IAS19.

Other areas of audit focus

We have identified other areas of the audit, that have not been classified as significant risks, but are still important when considering the risks of material misstatement to the financial statements and disclosures and therefore may be key audit matters we will include in our audit report.

What is the risk/area of focus?

What will we do?

IFRS 9 financial instruments

This new accounting standard is applicable for local authority accounts from the 2018/19 financial year and will change:

- How financial assets are classified and measured;
- How the impairment of financial assets are calculated; and
- The disclosure requirements for financial assets.

There are transitional arrangements within the standard; and the 2018/19 Cipfa Code of practice on local authority accounting provides guidance on the application of IFRS 9. However, until the Guidance Notes are issued and any statutory overrides are confirmed there remains some uncertainty on the accounting treatment.

IFRS 15 Revenue from contracts with customers

This new accounting standard is applicable for local authority accounts from the 2018/19 financial year.

The key requirements of the standard cover the identification of performance obligations under customer contracts and the linking of income to the meeting of those performance obligations.

The 2018/19 Cipfa Code of practice on local authority accounting provides guidance on the application of IFRS 15 and includes a useful flow diagram and commentary on the main sources of LG revenue and how they should be recognised.

The impact on local authority accounting is likely to be limited as large revenue streams like council tax, non domestic rates and government grants will be outside the scope of IFRS 15. However where that standard is relevant, the recognition of revenue will change and new disclosure requirements introduced.

We will:

- Assess the authority's implementation arrangements that should include an impact assessment paper setting out the application of the new standard, transitional adjustments and planned accounting for 2018/19;
- Consider the classification and valuation of financial instrument assets;
- Review the new expected credit loss model impairment calculations for assets; and
- Check additional disclosure requirements.

We will:

- Assess the authority's implementation arrangements that should include an impact assessment paper setting out the application of the new standard, transitional adjustments and planned accounting for 2018/19. This will include any Local Authority Trading Companies consolidated into the Authority's Group Accounts if produced;
- Consider application to the authority's revenue streams and, where the standard is relevant, test to ensure revenue is recognised when (or as) it satisfies a performance obligation; and
- Check additional disclosure requirements.



03

Value for Money Risks





Background

We are required to consider whether the Council has put in place ‘proper arrangements’ to secure economy, efficiency and effectiveness on its use of resources. This is known as our value for money conclusion.

For 2018/19 this is based on the overall evaluation criterion:

“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”

Proper arrangements are defined by statutory guidance issued by the National Audit Office. They comprise your arrangements to:

- Take informed decisions;
- Deploy resources in a sustainable manner; and
- Work with partners and other third parties.

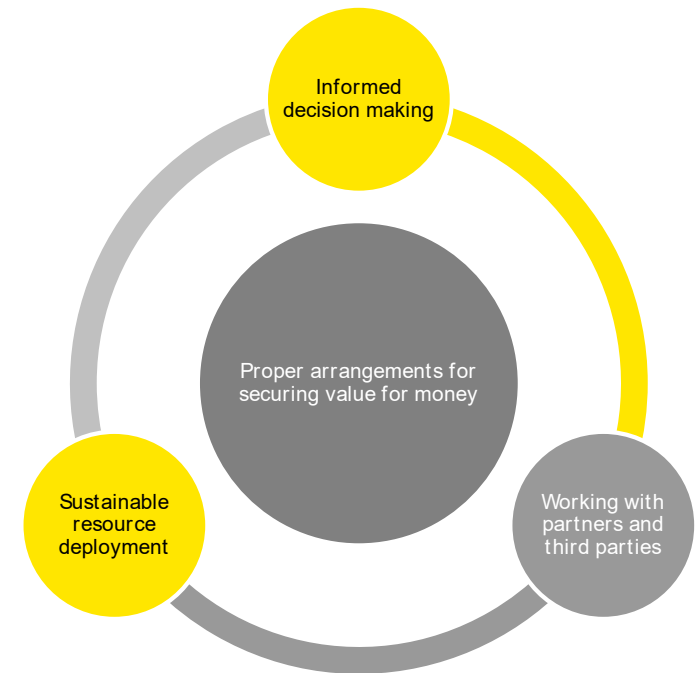
In considering your proper arrangements, we will draw on the requirements of the CIPFA/SOLACE framework for local government to ensure that our assessment is made against a framework that you are already required to have in place and to report on through documents such as your annual governance statement.

We are only required to determine whether there are any risks that we consider significant, which the Code of Audit Practice defines as:

“A matter is significant if, in the auditor’s professional view, it is reasonable to conclude that the matter would be of interest to the audited body or the wider public”

Our risk assessment supports the planning of sufficient work to enable us to deliver a safe conclusion on arrangements to secure value for money and enables us to determine the nature and extent of further work that may be required. If we do not identify any significant risks there is no requirement to carry out further work. We consider business and operational risks insofar as they relate to proper arrangements at both sector and organisation-specific level.

Our risk assessment has therefore considered both the potential financial impact of the issues we have identified, and also the likelihood that the issue will be of interest to local taxpayers, the Government and other stakeholders. This has resulted in the identification of no significant risks at the planning stage of our audit, but we will keep this assessment under review and update the Audit Committee as soon as possible if risks are identified during the remainder of our audit.





04

Audit materiality



Materiality

Materiality

For planning purposes, materiality for 2018/19 has been set at £2,043k. This represents 2% of the Council's prior year gross expenditure on provision of services. It will be reassessed throughout the audit process.



We request that the Audit Committee confirm its understanding of, and agreement to, these materiality and reporting levels.

Key definitions

Planning materiality – the amount over which we anticipate misstatements would influence the economic decisions of a user of the financial statements.

Performance materiality – the amount we use to determine the extent of our audit procedures. We have set performance materiality at £1,532k which represents 75% of planning materiality.

Audit difference threshold – we propose that misstatements identified below this threshold are deemed clearly trivial. We will report to you all uncorrected misstatements over this amount relating to the comprehensive income and expenditure statement, balance sheet, housing revenue account and collection fund that have an effect on income or that relate to other comprehensive income.

Other uncorrected misstatements, such as reclassifications and misstatements in the cashflow statement and movement in reserves statement or disclosures, and corrected misstatements will be communicated to the extent that they merit the attention of the audit committee, or are important from a qualitative perspective.



05

Scope of our audit



Our Audit Process and Strategy

Objective and Scope of our Audit scoping

Under the Code of Audit Practice our principal objectives are to review and report on the Council's financial statements and arrangements for securing economy, efficiency and effectiveness in its use of resources to the extent required by the relevant legislation and the requirements of the Code.

We issue an audit report that covers:

1. Financial statement audit

Our objective is to form an opinion on the financial statements under International Standards on Auditing (UK).

We also perform other procedures as required by auditing, ethical and independence standards, the Code and other regulations. We outline below the procedures we will undertake during the course of our audit.

Procedures required by standards

- Addressing the risk of fraud and error;
- Significant disclosures included in the financial statements;
- Entity-wide controls;
- Reading other information contained in the financial statements and reporting whether it is inconsistent with our understanding and the financial statements; and
- Auditor independence.

Procedures required by the Code

- Reviewing, and reporting on as appropriate, other information published with the financial statements, including the Annual Governance Statement; and
- Reviewing and reporting on the Whole of Government Accounts return, in line with the instructions issued by the NAO

2. Arrangements for securing economy, efficiency and effectiveness (value for money)

We are required to consider whether the Council has put in place 'proper arrangements' to secure economy, efficiency and effectiveness on its use of resources.

Our Audit Process and Strategy (continued)

Audit Process Overview

Our audit involves:

- Identifying and understanding the key processes and internal controls; and
- Substantive tests of detail of transactions and amounts.

For 2018/19 we plan to follow a substantive approach to the audit as we have concluded this is the most efficient way to obtain the level of audit assurance required to conclude that the financial statements are not materially misstated.

Analytics:

We will use our computer-based analytics tools to enable us to capture whole populations of your financial data, in particular journal entries. These tools:

- Help identify specific exceptions and anomalies which can then be subject to more traditional substantive audit tests; and
- Give greater likelihood of identifying errors than random sampling techniques.

We will report the findings from our process and analytics work, including any significant weaknesses or inefficiencies identified and recommendations for improvement, to management and the Audit Committee.

Internal audit:

We will regularly meet with the Head of Internal Audit, and review internal audit plans and the results of their work. We will reflect the findings from these reports, together with reports from any other work completed in the year, in our detailed audit plan, where they raise issues that could have an impact on the financial statements.



06

Audit team



Audit team

Audit team structure:

Kevin Suter
Associate Partner

James Stuttaford
Manager

Katie Lean
Senior

Use of specialists

When auditing key judgements, we are often required to rely on the input and advice provided by specialists who have qualifications and expertise not possessed by the core audit team. The areas where either EY or third party specialists provide input for the current year audit are:

Area	Specialists
Valuation of Land and Buildings	Authority's internal valuer (Stuart Yeo)
Pensions disclosure	EY Pensions/PWC/Aon Hewitt

In accordance with Auditing Standards, we will evaluate each specialist's professional competence and objectivity, considering their qualifications, experience and available resources, together with the independence of the individuals performing the work.

We also consider the work performed by the specialist in light of our knowledge of the Council's business and processes and our assessment of audit risk in the particular area. For example, we would typically perform the following procedures:

- Analyse source data and make inquiries as to the procedures used by the specialist to establish whether the source data is relevant and reliable;
- Assess the reasonableness of the assumptions and methods used;
- Consider the appropriateness of the timing of when the specialist carried out the work; and
- Assess whether the substance of the specialist's findings are properly reflected in the financial statements.



07

Audit timeline





Audit timeline

Timetable of communication and deliverables

Timeline

Below is a timetable showing the key stages of the audit and the deliverables we have agreed to provide to you through the audit cycle in 2018/19.

From time to time matters may arise that require immediate communication with the Audit Committee and we will discuss them with the Audit Committee Chair as appropriate. We will also provide updates on corporate governance and regulatory matters as necessary.

Audit phase	Timetable	Audit committee timetable	Deliverables
Planning: Risk assessment and setting of scopes. Walkthrough of key systems and processes	November		
	December		
	January	Audit Committee	Audit Planning Report
Interim audit testing	February		
	March		
	April		
	May		
Year end audit Audit Completion procedures	June		
	July	Audit Committee	Audit Results Report Audit opinions and completion certificates
	August - October	Audit Committee	Annual Audit Letter



08

Independence



Introduction

The FRC Ethical Standard and ISA (UK) 260 “Communication of audit matters with those charged with governance”, requires us to communicate with you on a timely basis on all significant facts and matters that bear upon our integrity, objectivity and independence. The Ethical Standard, as revised in June 2016, requires that we communicate formally both at the planning stage and at the conclusion of the audit, as well as during the course of the audit if appropriate. The aim of these communications is to ensure full and fair disclosure by us to those charged with your governance on matters in which you have an interest.

Required communications

Planning stage

- ▶ The principal threats, if any, to objectivity and independence identified by Ernst & Young (EY) including consideration of all relationships between the you, your affiliates and directors and us;
- ▶ The safeguards adopted and the reasons why they are considered to be effective, including any Engagement Quality review;
- ▶ The overall assessment of threats and safeguards;
- ▶ Information about the general policies and process within EY to maintain objectivity and independence.
- ▶ Where EY has determined it is appropriate to apply more restrictive independence rules than permitted under the Ethical Standard

Final stage

- ▶ In order for you to assess the integrity, objectivity and independence of the firm and each covered person, we are required to provide a written disclosure of relationships (including the provision of non-audit services) that may bear on our integrity, objectivity and independence. This is required to have regard to relationships with the entity, its directors and senior management, its affiliates, and its connected parties and the threats to integrity or objectivity, including those that could compromise independence that these create. We are also required to disclose any safeguards that we have put in place and why they address such threats, together with any other information necessary to enable our objectivity and independence to be assessed;
- ▶ Details of non-audit services provided and the fees charged in relation thereto;
- ▶ Written confirmation that the firm and each covered person is independent and, if applicable, that any non-EY firms used in the group audit or external experts used have confirmed their independence to us;
- ▶ Written confirmation that all covered persons are independent;
- ▶ Details of any inconsistencies between FRC Ethical Standard and your policy for the supply of non-audit services by EY and any apparent breach of that policy;
- ▶ Details of any contingent fee arrangements for non-audit services provided by us or our network firms; and
- ▶ An opportunity to discuss auditor independence issues.

In addition, during the course of the audit, we are required to communicate with you whenever any significant judgements are made about threats to objectivity and independence and the appropriateness of safeguards put in place, for example, when accepting an engagement to provide non-audit services.

We also provide information on any contingent fee arrangements, the amounts of any future services that have been contracted, and details of any written proposal to provide non-audit services that has been submitted;

We ensure that the total amount of fees that EY and our network firms have charged to you and your affiliates for the provision of services during the reporting period, analysed in appropriate categories, are disclosed.

Relationships, services and related threats and safeguards

We highlight the following significant facts and matters that may be reasonably considered to bear upon our objectivity and independence, including the principal threats, if any. We have adopted the safeguards noted below to mitigate these threats along with the reasons why they are considered to be effective. However we will only perform non –audit services if the service has been pre-approved in accordance with your policy.

Overall Assessment

Overall, we consider that the safeguards that have been adopted appropriately mitigate the principal threats identified and we therefore confirm that EY is independent and the objectivity and independence of Kevin Suter, your audit engagement partner and the audit engagement team have not been compromised.

Self interest threats

A self interest threat arises when EY has financial or other interests in the Council. Examples include where we receive significant fees in respect of non-audit services; where we need to recover long outstanding fees; or where we enter into a business relationship with you. At the time of writing, there are no long outstanding fees.

We believe that it is appropriate for us to undertake permissible non-audit services and we will comply with the policies that you have approved.

None of the services are prohibited under the FRC's ES or the National Audit Office's Auditor Guidance Note 01 and the services have been approved in accordance with your policy on pre-approval. The ratio of non audit fees to audits fees is not permitted to exceed 70%.

At the time of writing, we have not undertaken any non-audit work, therefore no additional safeguards are required.

A self interest threat may also arise if members of our audit engagement team have objectives or are rewarded in relation to sales of non-audit services to you. We confirm that no member of our audit engagement team, including those from other service lines, has objectives or is rewarded in relation to sales to you, in compliance with Ethical Standard part 4.

There are no other self interest threats at the date of this report.

Self review threats

Self review threats arise when the results of a non-audit service performed by EY or others within the EY network are reflected in the amounts included or disclosed in the financial statements.

There are no self review threats at the date of this report.

Management threats

Partners and employees of EY are prohibited from taking decisions on behalf of management of the Council. Management threats may also arise during the provision of a non-audit service in relation to which management is required to make judgements or decision based on that work.

There are no management threats at the date of this report.

Relationships, services and related threats and safeguards

Other threats

Other threats, such as advocacy, familiarity or intimidation, may arise.

There are no other threats at the date of this report.

Other communications

EY Transparency Report 2018

Ernst & Young (EY) has policies and procedures that instil professional values as part of firm culture and ensure that the highest standards of objectivity, independence and integrity are maintained.

Details of the key policies and processes in place within EY for maintaining objectivity and independence can be found in our annual Transparency Report which the firm is required to publish by law. The most recent version of this Report is for the year ended 1 July 2018 and can be found here:

<http://www.ey.com/uk/en/about-us/ey-uk-transparency-report-2018>



09

Appendices



Fees

Public Sector Audit Appointments Ltd (PSAA) has published the fee scale for the audit of the 2018/19 accounts of opted-in principal local government and police bodies.

This is defined as the fee required by auditors to meet statutory responsibilities under the Local Audit and Accountability Act 2014 in accordance with the requirements of the Code of Audit Practice and supporting guidance published by the National Audit Office, the financial reporting requirements set out in the Code of Practice on Local Authority Accounting published by CIPFA/LASAAC, and the professional standards applicable to auditors' work.

	Planned fee 2018/19	Scale fee 2018/19	Final Fee 2017/18
	£	£	£
Total Fee – Code work	42,721*	42,721	56,461
Total audit	42,721	42,721	56,461
Other non-audit services not covered above (Housing Benefits)	0	0	11,770
Total other non-audit services	0	0	11,770
Total fees	42,721	42,721	68,231

The agreed fee presented is based on the following assumptions:

- ▶ Officers meeting the agreed timetable of deliverables;
- ▶ Our accounts opinion and value for money conclusion being unqualified;
- ▶ Appropriate quality of documentation is provided by the Council; and
- ▶ The Council has an effective control environment.

If any of the above assumptions prove to be unfounded, we will seek a variation to the agreed fee. This will be discussed with the Council in advance.

Fees for the auditor's consideration of correspondence from the public and formal objections will be charged in addition to the scale fee.

Housing Benefits 2017/18

The fee for housing benefit 2017/18 certification is subject to approval by PSAA.

Impact of IFRS changes*

Our 2018/19 Code work includes additional planned procedures highlighted in section two of this report to address the new accounting requirements of IFRS 9 Financial Instruments and IFRS 15 Revenue from contracts with customers. As at the date of our planning report the Council is yet to evidence their assessment of the impact of these standards, and so we cannot currently quantify the expected scale fee variation for these additional procedures. We will agree this with management, depending on the identified impact of the new standards.

Additional procedures required relating to Housing Benefit expenditure*

To obtain sufficient assurance over housing benefits expenditure and subsidy income in the Council's financial statements, we will need to undertake some elements of the work which also form part of the housing benefit subsidy claim certification process. This work would previously have been covered by the certification fee and used additionally to provide assurance for the main audit. As we are no longer the reporting accountant for the Council's subsidy claim, we will need to consider the requirement for a scale fee variation to cover the performance of this work as part of the main audit for 2018/19.




Any additional fee will be subject to approval by the PSAA.

All fees exclude VAT





Required communications with the Audit Committee

We have detailed the communications that we must provide to the Audit Committee.





 **Our Reporting to you**

Required communications	 What is reported?	  When and where
Terms of engagement	Confirmation by the Audit Committee of acceptance of terms of engagement as written in the engagement letter signed by both parties.	The statement of responsibilities serves as the formal terms of engagement between the PSAA's appointed auditors and audited bodies.
Our responsibilities	Reminder of our responsibilities as set out in the engagement letter	The statement of responsibilities serves as the formal terms of engagement between the PSAA's appointed auditors and audited bodies.
Planning and audit approach	Communication of the planned scope and timing of the audit, any limitations and the significant risks identified.	Audit planning report
Significant findings from the audit	<ul style="list-style-type: none"> • Our view about the significant qualitative aspects of accounting practices including accounting policies, accounting estimates and financial statement disclosures • Significant difficulties, if any, encountered during the audit • Significant matters, if any, arising from the audit that were discussed with management • Written representations that we are seeking • Expected modifications to the audit report • Other matters if any, significant to the oversight of the financial reporting process 	Audit results report
Going concern	Events or conditions identified that may cast significant doubt on the entity's ability to continue as a going concern, including: <ul style="list-style-type: none"> • Whether the events or conditions constitute a material uncertainty • Whether the use of the going concern assumption is appropriate in the preparation and presentation of the financial statements • The adequacy of related disclosures in the financial statements 	Audit results report
Misstatements	<ul style="list-style-type: none"> • Uncorrected misstatements and their effect on our audit opinion, unless prohibited by law or regulation • The effect of uncorrected misstatements related to prior periods • A request that any uncorrected misstatement be corrected • Corrected misstatements that are significant • Material misstatements corrected by management 	Audit results report

Required communications with the Audit Committee (continued)

		 Our Reporting to you
Required communications	 What is reported?	  When and where
Fraud	<ul style="list-style-type: none"> • Enquiries of the Audit Committee to determine whether they have knowledge of any actual, suspected or alleged fraud affecting the entity • Any fraud that we have identified or information we have obtained that indicates that a fraud may exist • A discussion of any other matters related to fraud 	Audit results report
Related parties	<ul style="list-style-type: none"> • Significant matters arising during the audit in connection with the entity's related parties including, when applicable: • Non-disclosure by management • Inappropriate authorisation and approval of transactions • Disagreement over disclosures • Non-compliance with laws and regulations • Difficulty in identifying the party that ultimately controls the entity 	Audit results report
Independence	<p>Communication of all significant facts and matters that bear on EY's, and all individuals involved in the audit, objectivity and independence</p> <p>Communication of key elements of the audit engagement partner's consideration of independence and objectivity such as:</p> <ul style="list-style-type: none"> • The principal threats • Safeguards adopted and their effectiveness • An overall assessment of threats and safeguards • Information about the general policies and process within the firm to maintain objectivity and independence 	Audit Planning Report Audit Results Report
External confirmations	<ul style="list-style-type: none"> • Management's refusal for us to request confirmations • Inability to obtain relevant and reliable audit evidence from other procedures 	Audit results report

Required communications with the Audit Committee (continued)

		 Our Reporting to you
Required communications	 What is reported?	  When and where
Consideration of laws and regulations	<ul style="list-style-type: none"> Audit findings regarding non-compliance where the non-compliance is material and believed to be intentional. This communication is subject to compliance with legislation on tipping off Enquiry of the Audit Committee into possible instances of non-compliance with laws and regulations that may have a material effect on the financial statements and that the Audit Committee may be aware of 	Audit results report
Internal controls	<ul style="list-style-type: none"> Significant deficiencies in internal controls identified during the audit 	Audit results report
Representations	Written representations we are requesting from management and/or those charged with governance	Audit results report
Material inconsistencies and misstatements	Material inconsistencies or misstatements of fact identified in other information which management has refused to revise	Audit results report
Auditors report	<ul style="list-style-type: none"> Any circumstances identified that affect the form and content of our auditor's report 	Audit results report
Fee Reporting	<ul style="list-style-type: none"> Breakdown of fee information when the audit plan is agreed Breakdown of fee information at the completion of the audit Any non-audit work 	Audit planning report Audit results report

Additional audit information

Other required procedures during the course of the audit

In addition to the key areas of audit focus outlined in section 2, we have to perform other procedures as required by auditing, ethical and independence standards and other regulations. We outline the procedures below that we will undertake during the course of our audit.

Our responsibilities required by auditing standards

- Identifying and assessing the risks of material misstatement of the financial statements, whether due to fraud or error, design and perform audit procedures responsive to those risks, and obtain audit evidence that is sufficient and appropriate to provide a basis for our opinion.
- Obtaining an understanding of internal control relevant to the audit in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Council's internal control.
- Evaluating the appropriateness of accounting policies used and the reasonableness of accounting estimates and related disclosures made by management.
- Concluding on the appropriateness of management's use of the going concern basis of accounting.
- Evaluating the overall presentation, structure and content of the financial statements, including the disclosures, and whether the financial statements represent the underlying transactions and events in a manner that achieves fair presentation.
- Obtaining sufficient appropriate audit evidence regarding the financial information of the entities or business activities within the Council to express an opinion on the consolidated financial statements. Reading other information contained in the financial statements, the Audit Committee reporting appropriately addresses matters communicated by us to the Audit Committee and reporting whether it is materially inconsistent with our understanding and the financial statements; and
- Maintaining auditor independence.



Additional audit information (continued)

Purpose and evaluation of materiality

For the purposes of determining whether the accounts are free from material error, we define materiality as the magnitude of an omission or misstatement that, individually or in the aggregate, in light of the surrounding circumstances, could reasonably be expected to influence the economic decisions of the users of the financial statements. Our evaluation of it requires professional judgement and necessarily takes into account qualitative as well as quantitative considerations implicit in the definition. We would be happy to discuss with you your expectations regarding our detection of misstatements in the financial statements.

Materiality determines:

- The locations at which we conduct audit procedures to support the opinion given on the financial statements; and
- The level of work performed on individual account balances and financial statement disclosures.

The amount we consider material at the end of the audit may differ from our initial determination. At this stage, however, it is not feasible to anticipate all of the circumstances that may ultimately influence our judgement about materiality. At the end of the audit we will form our final opinion by reference to all matters that could be significant to users of the accounts, including the total effect of the audit misstatements we identify, and our evaluation of materiality at that date.

AUDIT COMMITTEE – 25 JANUARY 2019

TREASURY MANAGEMENT STRATEGY REPORT 2019/20

1. INTRODUCTION

- 1.1. Treasury management is the management of the Council's cash flows, borrowing and investments, and the associated risks. The Council has borrowed and invested 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 financial risk are therefore central to the Council's prudent financial management.
- 1.2. Treasury risk management at the Council is conducted within the framework of the CIPFA Code which requires the Council to approve a Treasury Management Strategy Statement (TMSS) before the start of each financial year. This report fulfils the Council's legal obligation under the Local Government Act 2003 to have regard to the CIPFA Code.
- 1.3. Investments held for service purposes or for commercial profit are considered in a different report, the Investment Strategy.

2. POLICIES AND APPROVALS REQUIRED

2.1. Treasury Management Strategy Statement

The Treasury Management Strategy Statement sets out how the Council's treasury service will support the capital expenditure and financing decisions taken over the three year period from 2019/20 to 2021/22. The day to day treasury management function and the limitations on activity through treasury indicators are also set out in the statement.

This report has been prepared prior to the finalisation of the Capital Programme for 2019/20 and subsequent years. Therefore the target indicators may be subject to minor variation. These indicators are targets only and minor adjustments will not be reported.

Any adjustments to the treasury management limits will be reported.

2.2. Treasury Management Investment Strategy

Treasury risk management at the Council is conducted within the framework of the Chartered Institute of Public Finance and Accountancy's Treasury Management in Public Services: Code of Practice 2017 Edition (the CIPFA Code). This report fulfils the Council's legal obligation under the Local Government Act 2003 to have regard to the CIPFA Code.

The Treasury Management investment strategy sets out the Council's criteria for choosing investment counterparties and limiting exposure to the risk of loss.

This strategy is shown in Annex A in Section 5.

The above policies and parameters provide an approved framework within which officers undertake the day to day treasury activities.

This strategy aims to strike a balance between allowing for current investment levels to continue, whilst also considering the Council's intention to directly invest in both commercial and residential property.

3. ENVIRONMENTAL IMPLICATIONS

3.1. There are no environment implications arising from this report.

4. CRIME AND DISORDER IMPLICATIONS

4.1. There are no crime and disorder implications arising from this report.

5. RECOMMENDATIONS

The Audit Committee is recommended to request Council to approve the key element of this report from 26 February 2018:

5.1. The Treasury Management Strategy 2019/20 to 2021/22 including the Annual Treasury Management Investment Strategy for 2019/20 (and the remainder for 2018/19) and the Treasury Indicators contained within Annex A.

5.2. That authority is delegated to the Section 151 Officer, who in turn delegates to Hampshire County Council's Director of Corporate Resources, as agreed in the Service Level Agreement, to manage all Council investments (other than the high yield investment portfolio) and borrowing according Treasury Management Strategy Statement as appropriate.

TREASURY MANAGEMENT STRATEGY 2019/20 – 2021/22

1. INTRODUCTION

- 1.1. Treasury management is the management of the Council's cash flows, borrowing and investments, and the associated risks. The Council has borrowed and invested 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 financial risk are therefore central to the Council's prudent financial management.
- 1.2. Treasury risk management at the Council is conducted within the framework of the CIPFA Code which requires the Council to approve a Treasury Management Strategy Statement (TMSS) before the start of each financial year. This report fulfils the Council's legal obligation under the Local Government Act 2003 to have regard to the CIPFA Code.
- 1.3. Investments held for service purposes or for commercial profit are considered in a different report, the Investment Strategy.

2. EXTERNAL CONTEXT

- 2.1. The following paragraphs explain the economic and financial background against which the TMSS is being set.

2.2. Economic background

The UK's progress negotiating its exit from the European Union, together with its future trading arrangements, will continue to be a major influence on the Council's TMSS for 2019/20.

UK Consumer Price Inflation for October was up 2.4% year-on-year, slightly below the consensus forecast and broadly in line with the Bank of England's (BoE) November Inflation Report. The most recent labour market data for October 2018 showed the unemployment rate edged up slightly to 4.1% while the employment rate of 75.7% was the joint highest on record. The 3-month average annual growth rate for pay excluding bonuses was 3.3% as wages continue to rise steadily and provide some pull on general inflation. Adjusted for inflation, means real wages grew by 1.0%, a level still likely to have little effect on consumer spending.

The rise in quarterly GDP growth to 0.6% in Quarter 3 from 0.4% in the previous quarter was due to weather-related factors boosting overall household consumption and construction activity over the summer following the weather-related weakness in Quarter 1. At 1.5%, annual Gross Domestic Product growth continues to remain below trend. Looking ahead, the BoE, in its November Inflation Report, expects GDP growth to average around 1.75% over the

forecast horizon, providing the UK's exit from the EU is relatively smooth.

Following the BoE's decision to increase Bank Rate to 0.75% in August, no changes to monetary policy has been made since. However, the Bank expects that should the economy continue to evolve in line with its November forecast, further increases in Bank Rate will be required to return inflation to the 2% target. The Monetary Policy Committee (MPC) continues to reiterate that any further increases will be at a gradual pace and limited in extent.

2.3. Credit outlook

The big four UK banking groups have now divided their retail and investment banking divisions into separate legal entities under ringfencing legislation. Bank of Scotland, Barclays Bank UK, HSBC UK Bank, Lloyds Bank, National Westminster Bank, Royal Bank of Scotland and Ulster Bank are the ringfenced banks that now only conduct lower risk retail banking activities. Barclays Bank, HSBC Bank, Lloyds Bank Corporate Markets and NatWest Markets are the investment banks. Credit rating agencies have adjusted the ratings of some of these banks with the ringfenced banks generally being better rated than their non-ringfenced counterparts.

European banks are considering their approach to Brexit, with some looking to create new UK subsidiaries to ensure they can continue trading here. The credit strength of these new banks remains unknown, although the chance of parental support is assumed to be very high if ever needed. The uncertainty caused by protracted negotiations between the UK and EU is weighing on the creditworthiness of both UK and European banks with substantial operations in both jurisdictions.

2.4. Interest rate forecast

Following the increase in Bank Rate to 0.75% in August 2018, the Council's treasury management adviser Arlingclose is forecasting two more 0.25% hikes during 2019 to take official UK interest rates to 1.25%. The BoE's MPC has maintained expectations for slow and steady rate rises over the forecast horizon. The MPC continues to have a bias towards tighter monetary policy but is reluctant to push interest rate expectations too strongly. Arlingclose believes that MPC members consider both that ultra-low interest rates result in other economic problems, and that higher Bank Rate will be a more effective policy weapon should downside Brexit risks crystallise when rate cuts will be required.

The UK economic environment remains relatively soft, despite seemingly strong labour market data. Arlingclose's view is that the economy still faces a challenging outlook as it exits the European Union and Eurozone growth softens. While assumptions are that a Brexit deal is struck and some agreement reached on transition and future trading arrangements before the UK leaves the EU, the

possibility of a “no deal” Brexit still hangs over economic activity (at the time of writing this commentary in mid-December). As such, the risks to the interest rate forecast are considered firmly to the downside.

A more detailed economic and interest rate forecast provided by Arlingclose is attached at Appendix A.

3. BALANCE SHEET SUMMARY AND FORECAST

- 3.1. On 31 December 2018, the Council held £139.7m of borrowing and £88.2m of investments. This is set out in further detail at Appendix B. Forecast changes in these sums are shown in the balance sheet analysis in Table 1 below.

Table 1: Balance Sheet Summary and Forecast	31/03/18 Actual £m	31/03/19 Estimate £m	31/03/20 Forecast £m	31/03/21 Forecast £m	31/03/22 Forecast £m
General Fund CFR	5.4	5.3	14.8	25.3	33.6
Housing Revenue Account CFR	138.6	134.5	130.4	126.3	122.2
HRA Settlement	1.9	1.9	1.9	1.9	1.9
Total CFR	145.9	141.7	147.1	153.5	157.7
Less: External borrowing *	(139.8)	(135.5)	(131.2)	(126.9)	(122.6)
Internal (over) borrowing	6.1	6.2	15.9	26.6	35.1
Less: GF Usable reserves	(24.6)	(28.9)	(24.9)	(19.1)	(16.9)
Less: HRA Usable reserves	(29.0)	(23.1)	(15.9)	(10.1)	(2.9)
Less: Working capital	(15.7)	(15.7)	(15.7)	(15.7)	(15.7)
Resources for investments	(69.3)	(67.7)	(56.5)	(44.9)	(35.5)
New borrowing (or investments)	(63.2)	(61.5)	(40.6)	(18.3)	(0.4)

* shows only loans to which the Council is committed and excludes optional refinancing

- 3.2. 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. The Council’s current strategy is to maintain borrowing and investments below their underlying levels, sometimes known as internal borrowing.
- 3.1. The CFR is showing an increase over the period as the Council looks to roll out its commercial and residential investment strategies. At the appropriate time, the Council will consult with its treasury advisors on how best to service any borrowing requirements, including the possibility of renewing maturing loans on the HRA. The level of

usable HRA reserves is set to decrease over the period as the Council works towards achieving its latest acquisition and development strategy, as well as continuing with principal repayments on the settlement loan.

- 3.2. CIPFA's Prudential Code for Capital Finance in Local Authorities recommends that the Council's total debt should be lower than its highest forecast CFR over the next three years. Table 1 shows that the Council expects to comply with this recommendation during 2019/10.

4. BORROWING STRATEGY

- 4.1. The Council currently holds £139.7m of loans, a decrease of £4.3m on the previous year, as a result of the HRA refinancing in 2012. The balance sheet forecast in Table 1 shows that the Council does not expect to need to borrow in 2019/20. The Council may however borrow to pre-fund future years' requirements, providing this does not exceed the authorised limit for borrowing of £201.6 million.

4.2. Objectives

The Council's chief objective when borrowing money is to strike an appropriately low risk balance between securing low interest costs and achieving certainty of those costs over the period for which funds are required. The flexibility to renegotiate loans should the Council's long-term plans change is a secondary objective.

4.3. Strategy

Given the significant cuts to public expenditure and in particular to local government funding, the Council's borrowing strategy continues to address the key issue of affordability without compromising the longer-term stability of the debt portfolio. With short-term interest rates currently much lower than long-term rates, if the Council does not need to borrow, it is likely to be more cost effective in the short-term to either use internal resources, or to borrow short-term loans instead.

By internally borrowing, the Council is able to reduce net borrowing costs (despite foregone investment income) and reduce overall treasury risk. The benefits of internal and short-term borrowing will be monitored regularly against the potential for incurring additional costs by deferring borrowing into future years when long-term borrowing rates are forecast to rise modestly. Arlingclose will assist the Council with this 'cost of carry' and breakeven analysis. Its output may determine whether the Council borrows additional sums at long-term fixed rates in 2019/20 with a view to keeping future costs low, even if this causes additional cost in the short-term.

In addition, the Council may borrow short-term loans (normally for up to one month) to cover unplanned cash flow shortages.

4.4. Sources of borrowing

The approved sources of long-term and short-term borrowing are:

- Public Works Loan Board (PWLB) and any successor body
- any institution approved for investments (see below)
- any other bank or building society authorised to operate in the UK
- any other UK public sector body
- UK public and private sector pension funds (except Hampshire Pension Fund)
- capital market bond investors
- UK Municipal Bonds Agency plc and other special purpose companies created to enable local authority bond issues

4.5. Other sources of debt finance

In addition, capital finance may be raised by the following methods that are not borrowing, but may be classed as other debt liabilities:

- leasing
- hire purchase
- Private Finance Initiative
- sale and leaseback

The Council has previously raised all of its long-term borrowing from the PWLB but it continues to investigate other sources of finance, such as local authority loans and bank loans, that may be available at more favourable rates.

4.6. Short-term and variable rate loans

These loans leave the Council exposed to the risk of short-term interest rate rises, which is monitored through the indicator on interest rate exposure in the treasury management indicators below.

4.7. Debt rescheduling

The PWLB allows authorities to repay loans before maturity and either pay a premium or receive a discount according to a set formula based on current interest rates. Other lenders may also be prepared to negotiate premature redemption terms. The Council may take advantage of this and replace some loans with new loans, or repay loans without replacement, where this is expected to lead to an overall cost saving or a reduction in risk.

5. TREASURY MANAGEMENT INVESTMENT STRATEGY

5.1. The Council holds invested funds, representing income received in advance of expenditure plus balances and reserves held. In the past 12 months, the Council's investment balance has ranged between £60.8m and £100.6m.

5.2. Objectives

Both the CIPFA Code requires the Council to invest its funds prudently, and to have regard to the security and liquidity of its investments before seeking the highest rate of return, or yield. The Council's objective when investing money is to strike an appropriate balance between risk and return, minimising the risk of incurring losses from defaults and the risk of receiving unsuitably low investment income. Where balances are expected to be invested for more than one year, the Council will aim to achieve a total return that is equal or higher than the prevailing rate of inflation, in order to maintain the spending power of the sum invested.

5.3. Negative interest rates

If the UK enters into a recession in 2019/20, there is a small chance that the Bank of England could set its Bank Rate at or below zero, which is likely to feed through to negative interest rates on all low risk, short-term investment options. This situation already exists in many other European countries. In this event, security will be measured as receiving the contractually agreed amount at maturity, even though this may be less than the amount originally invested.

5.4. Strategy

Given the increasing risk and very low returns from short-term unsecured bank investments, the Council aims to continue to diversify into more secure and/or higher yielding asset classes during 2019/20. This is especially the case for the estimated £40m that is available for longer-term investment. Approximately 59% of the Council's surplus cash is invested so that it is not subject to bail-in risk, as it is invested in local authorities, pooled property, equity and multi-asset funds, registered providers, corporate bonds and secured bank bonds. Whilst the remaining cash is subject to bail-in risk, 59% of this balance is held in overnight money market funds and cash plus funds which are subject to a reduced risk of bail-in, 33% is held in certificates of deposit which can be sold on the secondary market, and 8% is held in overnight call accounts with banks to allow for liquidity. This diversification will represent a continuation of the new strategy adopted in 2015/16.

The Council has invested in further high yield investments by increasing its investments in pooled property and pooled equity funds, and by investing in pooled multi-asset funds.

The investments in pooled property, equity and multi-asset funds allow the Council to diversify into asset classes other than cash without the need to own and manage the underlying investments. The funds which are operated on a variable net asset value (VNAV) basis offer diversification of investment risk, coupled with the services of a professional fund manager; they also offer enhanced returns over the longer term but are more volatile in the short-term. All of the Council's pooled fund investments are in the funds' distributing share classes which pay out the income generated.

Although money can be redeemed from the pooled funds at short notice, the Council's intention is to hold them for at least the medium term. Their performance and suitability in meeting the Council's investment objectives are monitored regularly and discussed with Arlingclose.

Table 2: High yield investments capital value	Principal invested £m	Market value 30/11/2018 £m	Capital yield (per annum) %
Pooled Property Funds	7.6	7.7	0.61
Pooled Equity Funds	3.0	3.1	(0.30)
Pooled Multi Asset Funds	2.0	1.9	(2.48)
Total	12.6	12.7	(0.10)

As shown in Appendix B, without this allocation the weighted average return of the Council's cash investments would have been 0.92%; the allocation to high yielding investments has added 0.53% (£0.5m based on the cash balance at 31 December 2018) to the average interest rate earned by the remainder of the portfolio.

5.5. Investment limits

The maximum that will be lent/invested to/with any one organisation (other than the UK Government) will be £12 million. A group of banks under the same ownership will be treated as a single organisation for limit purposes. Limits will also be placed on fund managers, and investments in pooled funds, as they would not count against a limit for any single foreign country, since the risk is diversified over many countries.

Table 3: Investment limits	Cash limit
Any single organisation, except the UK Central Government	£12m each
UK Central Government	unlimited
Any group of organisations under the same ownership	£12m per group
Any group of pooled funds under the same management	£12m per manager
Registered providers and registered social landlords	£10m in total
Money Market Funds	£50% in total
Real estate investment trusts	£12m in total

5.6. Approved counterparties

The Council may invest its surplus funds with any of the counterparty types in Table 4 below, subject to the cash limits (per counterparty) and the time limits shown.

Table 4: Approved investment counterparties and limits						
Credit rating	Banks		Government	Corporates	Registered Providers	
	Unsecured	Secured			Unsecured	Secured
UK Govt	n/a	n/a	£ Unlimited 30 years	n/a	n/a	n/a
AAA	£6m 5 years	£12m 20 years	£12m 50 years	£6m 20 years	£6m 20 years	£6m 20 years
AA+	£6m 5 years	£12m 10 years	£12m 25 years	£6m 10 years	£6m 10 years	£6m 10 years
AA	£6m 4 years	£12m 5 years	£12m 15 years	£6m 5 years	£6m 10 years	£6m 10 years
AA-	£6m 3 years	£12m 4 years	£12m 10 years	£6m 4 years	£6m 10 years	£6m 10 years
A+	£6m 2 years	£12m 3 years	£6m 5 years	£6m 3 years	£6m 5 years	£6m 5 years
A	£6m 13 months	£12m 2 years	£6m 5 years	£6m 2 years	£6m 5 years	£6m 5 years
A-	£6m 6 months	£12m 13 months	£6m 5 years	£6m 13 months	£6m 5 years	£6m 5 years
None	£1m 6 months	n/a	£12m 25 years	n/a	£6m 5 years	£6m 25 years
Pooled funds and real estate investment trusts	£12m per fund					

This table must be read in conjunction with the notes below

5.7. Credit rating

Investment limits are set by reference to the lowest published long-term credit rating from a selection of external rating agencies. Where available, the credit rating relevant to the specific investment or class of investment is used, otherwise the counterparty credit rating is used. However, investment decisions are never made solely based on credit ratings, and all other relevant factors including external advice will be taken into account.

5.8. Banks unsecured

Accounts, deposits, certificates of deposit and senior unsecured bonds with banks and building societies, other than multilateral

development banks. These investments are subject to the risk of credit loss via a bail-in should the regulator determine that the bank is failing or likely to fail. See below for arrangements relating to operational bank accounts.

5.9. Banks secured

Covered bonds, reverse repurchase agreements and other collateralised arrangements with banks and building societies. These investments are secured on the bank's assets, which limits the potential losses in the unlikely event of insolvency, and means that they are exempt from bail-in. Where there is no investment specific credit rating, but the collateral upon which the investment is secured has a credit rating, the higher of the collateral credit rating and the counterparty credit rating will be used to determine cash and time limits. The combined secured and unsecured investments in any one bank will not exceed the cash limit for secured investments.

5.10. Government

Loans, bonds and bills issued or guaranteed by national governments, regional and local authorities and multilateral development banks. These investments are not subject to bail-in, and there is generally a lower risk of insolvency, although they are not zero risk. Investments with the UK Central Government may be made in unlimited amounts for up to 30 years.

5.11. Corporates

Loans, bonds and commercial paper issued by companies other than banks and registered providers. These investments are not subject to bail-in, but are exposed to the risk of the company going insolvent.

5.12. Registered providers

Loans and bonds issued by, guaranteed by or secured on the assets of registered providers of social housing and registered social landlords, formerly known as housing associations. These bodies are tightly regulated by the Regulator of Social Housing (in England), the Scottish Housing Regulator, the Welsh Government and the Department for Communities (in Northern Ireland). As providers of public services, they retain the likelihood of receiving government support if needed.

5.13. Pooled funds

Shares or units in diversified investment vehicles consisting of any of the above investment types, plus equity shares and property. These funds have the advantage of providing wide diversification of investment risks, coupled with the services of a professional fund manager in return for a fee. Short-term Money Market Funds that offer same-day liquidity and very low or no volatility will be used as an alternative to instant access bank accounts, while pooled funds whose

value changes with market prices and/or have a notice period will be used for longer investment periods.

Bond, equity and property funds offer enhanced returns over the longer term, but are more volatile in the short term. These allow the Council to diversify into asset classes other than cash without the need to own and manage the underlying investments. Because these funds have no defined maturity date, but are available for withdrawal after a notice period, their performance and continued suitability in meeting the Council's investment objectives will be monitored regularly.

5.14. Real estate investment trusts (REITs)

Shares in companies that invest mainly in real estate and pay the majority of their rental income to investors in a similar manner to pooled property funds, REITs offer enhanced returns over the longer term, but are more volatile especially as the share price reflects changing demand for the shares as well as changes in the value of the underlying properties.

5.15. Risk assessment and credit ratings

Credit ratings are obtained and monitored by the Council's treasury advisers, who will notify changes in ratings as they occur. Where an entity has its credit rating downgraded so that it fails to meet the approved investment criteria then:

- no new investments will be made,
- any existing investments that can be recalled or sold at no cost will be, and
- full consideration will be given to the recall or sale of all other existing investments with the affected counterparty.

Where a credit rating agency announces that a credit rating is on review for possible downgrade (also known as "rating watch negative" or "credit watch negative") so that it may fall below the approved rating criteria, then only investments that can be withdrawn [on the next working day] will be made with that organisation until the outcome of the review is announced. This policy will not apply to negative outlooks, which indicate a long-term direction of travel rather than an imminent change of rating.

5.16. Other information on the security of investments

The Council understands that credit ratings are good, but not perfect, predictors of investment default. Full regard will therefore be given to other available information on the credit quality of the organisations in which it invests, including credit default swap prices, financial statements, information on potential government support and reports in the quality financial press and analysis and advice from the

Council's treasury management adviser. No investments will be made with an organisation if there are substantive doubts about its credit quality, even though it may otherwise meet the above criteria.

When deteriorating financial market conditions affect the creditworthiness of all organisations, as happened in 2008 and 2011, this is not generally reflected in credit ratings, but can be seen in other market measures. In these circumstances, the Council will restrict its investments to those organisations of higher credit quality and reduce the maximum duration of its investments to maintain the required level of security. The extent of these restrictions will be in line with prevailing financial market conditions. If these restrictions mean that insufficient commercial organisations of high credit quality are available to invest the Council's cash balances, then the surplus will be deposited with the UK Government, via the Debt Management Office or invested in government treasury bills for example, or with other local authorities. This will cause a reduction in the level of investment income earned, but will protect the principal sum invested.

5.17. Liquidity management

The Council has due regard for its future cash flows when determining the maximum period for which funds may prudently be committed. Historic cash flows are analysed in addition to significant future cash movements, such as payroll, grant income and council tax precept. Limits on long-term investments are set by reference to the Council's medium term financial position (summarised in Table 1) and forecast short-term balances.

6. TREASURY MANAGEMENT INDICATORS

6.1. The Council measures and manages its exposures to treasury management risks using the following indicators.

6.2. Interest rate exposures

The following indicator shows the sensitivity of the County Council's current investments and borrowing to a change in interest rates.

Table 5: Interest rate risk indicator	31 December 2018	Impact of +/-1% interest rate change
Sums subject to variable interest rates		
Investment	£69.2m	+/-£0.7m
Borrowing	(£0.0m)	+/-£0.0m

6.3. Maturity structure of borrowing

This indicator is set to control the Council's exposure to refinancing risk. The upper and lower limits on the maturity structure of borrowing will be:

Table 6: Refinancing rate risk indicator	Upper	Lower
Under 12 months	25%	0%
12 months and within 24 months	25%	0%
24 months and within 5 years	25%	0%
5 years and within 10 years	25%	0%
10 years and above	100%	0%

Time periods start on the first day of each financial year. The maturity date of borrowing is the earliest date on which the lender can demand repayment.

6.4. Principal sums invested for periods longer than a year

The purpose of this indicator is to control the Council's exposure to the risk of incurring losses by seeking early repayment of its investments. The limits on the long-term principal sum invested to final maturities beyond the period end will be:

Table 7: Price risk indicator	2019/20	2020/21	2021/22
Limit on principal invested beyond a year	£40m	£40m	£40m

7. RELATED MATTERS

7.1. The CIPFA Code requires the Council to include the following in its TMSS.

7.2. Financial derivatives

Local authorities have previously made use of financial derivatives embedded into loans and investments both to reduce interest rate risk (e.g. interest rate collars and forward deals) and to reduce costs or increase income at the expense of greater risk (e.g. LOBO loans and callable deposits). The general power of competence in Section 1 of the Localism Act 2011 removes much of the uncertainty over local authorities' use of standalone financial derivatives (i.e. those that are not embedded into a loan or investment).

The Council will only use standalone financial derivatives (such as swaps, forwards, futures and options) where they can be clearly demonstrated to reduce the overall level of the financial risks that the Council is exposed to. Additional risks presented, such as credit exposure to derivative counterparties, will be taken into account when determining the overall level of risk. Embedded derivatives, including those present in pooled funds and forward starting transactions, will

not be subject to this policy, although the risks they present will be managed in line with the overall treasury risk management strategy.

Financial derivative transactions may be arranged with any organisation that meets the approved investment criteria. The current value of any amount due from a derivative counterparty will count against the counterparty credit limit and the relevant foreign country limit.

7.3. Housing Revenue Account

On 1st April 2012, the Council notionally split each of its existing long-term loans into General Fund and HRA pools. In the future, new long-term loans borrowed will be assigned in their entirety to one pool or the other. Interest payable and other costs/income arising from long-term loans (e.g. premiums and discounts on early redemption) will be charged/credited to the respective revenue account. Differences between the value of the HRA loans pool and the HRA's underlying need to borrow (adjusted for HRA balance sheet resources available for investment) will result in a notional cash balance which may be positive or negative. This balance will be measured each month and interest transferred between the General Fund and HRA at the average % Local Authority 7 day rate.

7.4. Markets in Financial Instruments Directive

The Council has opted up to professional client status with its providers of financial services, including advisers, brokers and fund managers, allowing it access to a greater range of services but without the greater regulatory protections afforded to individuals and small companies. Given the size and range of the Council's treasury management activities, the s151 Officer believes this is the most appropriate status.

Appendix A – Arlingclose Economic & Interest Rate Forecast October 2018

Underlying assumptions:

- The MPC left Bank Rate unchanged at the September meeting, after voting unanimously to increase Bank Rate to 0.75% in August.
- Our projected outlook for the UK economy means we maintain the significant downside risks to our interest rate forecast. The UK economic environment is relatively soft, despite seemingly strong labour market data. GDP growth recovered somewhat in Q2 2018, but the annual growth rate of 1.2% remains well below the long term average. Our view is that the UK economy still faces a challenging outlook as the country exits the European Union and Eurozone economic growth softens.
- Cost pressures were projected to ease but have risen more recently and are forecast to remain above the Bank's 2% target through most of the forecast period. The rising price of oil and tight labour market means inflation may remain above target for longer than expected. This means that strong real income growth is unlikely in the near future.
- The MPC has a bias towards tighter monetary policy but is reluctant to push interest rate expectations too strongly. We believe that MPC members consider both that: 1) ultra-low interest rates result in other economic problems, and 2) higher Bank Rate will be a more effective policy weapon should downside Brexit risks crystallise and cuts are required.
- The global economy appears to be slowing, particularly the Eurozone and China, where the effects of the trade war has been keenly felt. Despite slower growth, the European Central Bank is adopting a more strident tone in conditioning markets for the end of QE, the timing of the first rate hike (2019) and their path thereafter. Meanwhile, European political issues, mostly lately with Italy, continue.
- The US economy is expanding more rapidly. The Federal Reserve has tightened monetary policy by raising interest rates to the current 2%-2.25% range; further rate hikes are likely, which will start to slow economic growth. Central bank actions and geopolitical risks have and will continue to produce significant volatility in financial markets, including bond markets.

Forecast:

- The MPC has maintained expectations of a slow rise in interest rates over the forecast horizon. Our central case is for Bank Rate is to rise twice in 2019. The risks are weighted to the downside.
- Gilt yields have remained at low levels. We expect some upward movement from current levels based on our interest rate projections, the strength of the US economy and the ECB's forward guidance on higher rates. However, volatility arising from both economic and political events will continue to offer borrowing opportunities.

	Dec-18	Mar-19	Jun-19	Sep-19	Dec-19	Mar-20	Jun-20	Sep-20	Dec-20	Mar-21	Jun-21	Sep-21	Dec-21	Average
Official Bank Rate														
Upside risk	0.00	0.00	0.00	0.00	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.17
Arlingclose Central Case	0.75	1.00	1.00	1.25	1.25	1.25	1.25	1.25	1.25	1.25	1.25	1.25	1.25	1.17
Downside risk	0.00	0.50	0.50	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.65
3-mth money market rate														
Upside risk	0.10	0.10	0.10	0.10	0.15	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.20	0.17
Arlingclose Central Case	0.80	1.00	1.10	1.20	1.30	1.30	1.25	1.20	1.20	1.20	1.20	1.20	1.20	1.17
Downside risk	0.20	0.50	0.60	0.70	0.80	0.80	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.68
1-yr money market rate														
Upside risk	0.20	0.30	0.30	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.33
Arlingclose Central Case	1.05	1.25	1.35	1.40	1.50	1.45	1.40	1.40	1.40	1.40	1.40	1.40	1.40	1.37
Downside risk	0.35	0.50	0.60	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.75	0.69
5-yr gilt yield														
Upside risk	0.15	0.20	0.25	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.32
Arlingclose Central Case	1.15	1.20	1.25	1.35	1.40	1.40	1.35	1.35	1.30	1.30	1.30	1.30	1.30	1.30
Downside risk	0.30	0.35	0.45	0.50	0.60	0.60	0.60	0.60	0.60	0.60	0.60	0.60	0.60	0.54
10-yr gilt yield														
Upside risk	0.20	0.25	0.25	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.32
Arlingclose Central Case	1.60	1.65	1.65	1.70	1.75	1.75	1.75	1.70	1.70	1.70	1.70	1.70	1.70	1.70
Downside risk	0.30	0.45	0.50	0.55	0.60	0.60	0.60	0.60	0.60	0.60	0.60	0.60	0.60	0.55
20-yr gilt yield														
Upside risk	0.20	0.25	0.25	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.32
Arlingclose Central Case	1.90	1.95	1.95	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	2.00	1.98
Downside risk	0.30	0.40	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.43
50-yr gilt yield														
Upside risk	0.20	0.25	0.25	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.35	0.32
Arlingclose Central Case	1.80	1.85	1.85	1.90	1.90	1.90	1.90	1.90	1.90	1.90	1.90	1.90	1.90	1.88
Downside risk	0.30	0.40	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.45	0.43

PWLB Certainty Rate (Maturity Loans) = Gilt yield + 0.80%

PWLB Local Infrastructure Rate (Maturity Loans) = Gilt yield + 0.60%

Appendix B – Existing Investment & Debt Portfolio Position

Investment Position (Treasury Investments)

Investments	30/09/2018 Balance £m	Movement £m	31/12/2018 Balance £m	31/12/2018 Rate %	31/12/2018 WAM* years
Short term Investments					
Banks and Building Societies:					
- Unsecured	13.9	1.1	15.0	0.84	0.15
- Secured	5.5	2.7	8.2	1.11	0.23
Money Market Funds	6.3	13.2	19.5	0.73	0.01
Cash Plus Funds	2.0	0.0	2.0	0.53	n/a
Local Authorities	13.0	-2.5	10.5	0.83	0.46
Corporate Bonds	7.1	-7.1	0.0	0	0
Registered Providers	4.0	0.0	4.0	1.25	0.1
	51.8	7.4	59.2	0.86	0.17
Long term investments					
Banks and Building Societies:					
- Secured	8.0	2.0	10.0	1.09	2.12
Local Authorities	6.0	0.0	6.0	1.25	1.92
	14.0	2.0	16.0	1.15	2.05
High yield investments					
Pooled Property Funds**	6.6	1.1	7.6	4.19	n/a
Pooled Equity Funds**	3.0	0.0	3.0	5.36	n/a
Pooled Multi-Asset Funds**	2.0	0.3	2.3	4.68	n/a
	11.6	1.4	12.9	4.55	n/a
TOTAL INVESTMENTS	77.4	10.8	88.2	1.45	0.56

* Weighted average maturity

** The rates provided for pooled fund investments are reflective of the average of the most recent dividend return as at 31 December 2018.

Treasury Management Position

	31/12/2018 Balance £m	31/12/2018 Rate %
External Borrowing		
PWLB	(139.7)	(3.17)
Investments		
Total Investments	88.2	1.45
Net Debt	(51.5)	

Certification of claims and returns annual report 2017-18

New Forest District Council
January 2019

Page 55



Building a better
working world

Agenda Item 6



Members of the Audit Committee

January 2019

New Forest District Council
Appletree Court
Beaulieu Road
Lyndhurst
SO43 7PA

Dear Audit Committee Members

We are pleased to report on our certification and other assurance work. This report summarises the results of our work on New Forest District Council's 2017-18 claims.

Local authorities claim large sums of public money in grants and subsidies from central government and other grant-paying bodies and must complete returns providing financial information to government departments. In some cases these grant-paying bodies and government departments require appropriately qualified reporting accountants to certify the claims and returns submitted to them.

From 1 April 2015, the duty to make arrangements for the certification of relevant claims and returns and to prescribe scales of fees for this work was delegated to the Public Sector Audit Appointments Ltd (PSAA) by the Secretary of State for Communities and Local Government.

For 2017-18, these arrangements required only the certification of the housing benefits subsidy claim. In certifying this we followed a methodology determined by the Department for Work and Pensions.

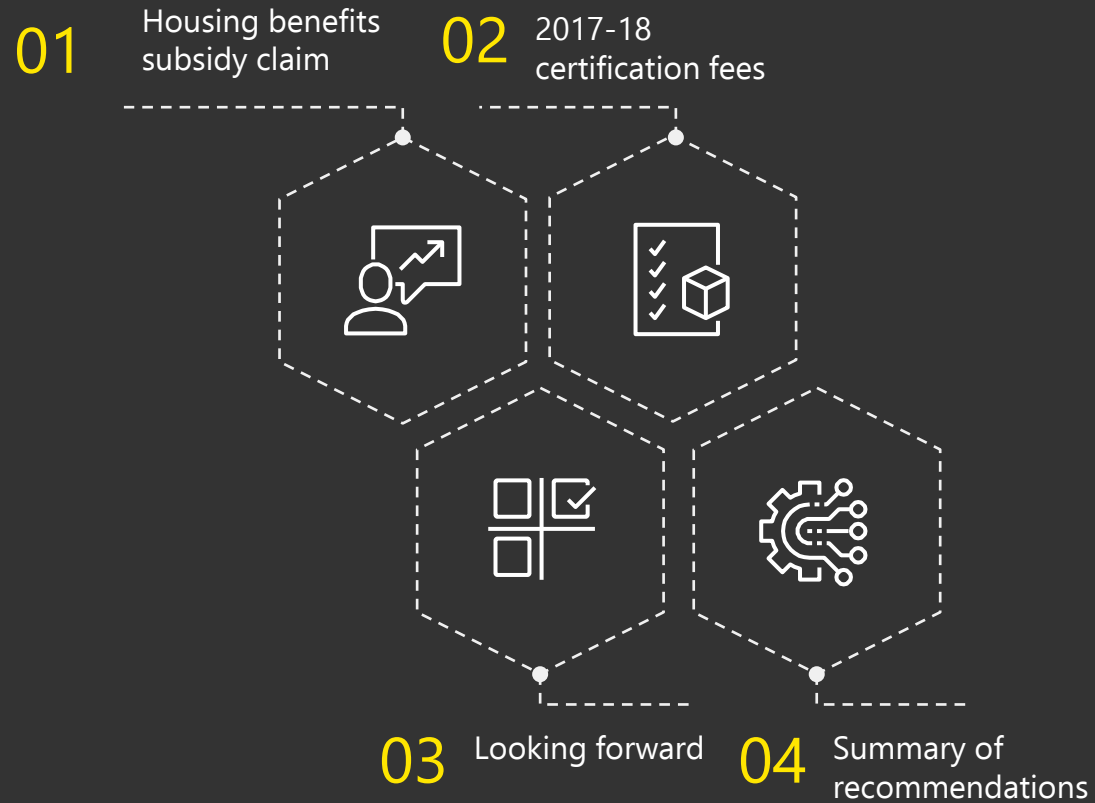
This report is intended solely for the information and use of the Audit Committee and management, and is not intended to be and should not be used by anyone other than these specified parties.

We welcome the opportunity to discuss this report with you at the Audit Committee on Friday 25 January 2019.

Yours faithfully

Kevin Suter
Associate Partner
For and on behalf of Ernst & Young LLP

Contents



In April 2015 Public Sector Audit Appointments Ltd (PSAA) issued "Statement of responsibilities of auditors and audited bodies". It is available from the via the PSAA website (www.PSAA.co.uk). The Statement of responsibilities serves as the formal terms of engagement between appointed auditors and audited bodies. It summarises where the different responsibilities of auditors and audited bodies begin and end, and what is to be expected of the audited body in certain areas.

The "Terms of Appointment (updated February 2017)" issued by the PSAA sets out additional requirements that auditors must comply with, over and above those set out in the National Audit Office Code of Audit Practice (the Code) and in legislation, and covers matters of practice and procedure which are of a recurring nature.

This report is made solely to the Audit Committee and management of New Forest District Council. Our work has been undertaken so that we might state to the Audit Committee and management of New Forest District Council those matters we are required to state to them in this report and for no other purpose. To the fullest extent permitted by law we do not accept or assume responsibility to anyone other than the Audit Committee and management of New Forest District Council for this report or for the opinions we have formed. It should not be provided to any third-party without our prior written consent.



01

Housing benefits subsidy claim



Housing benefits subsidy claim

Scope of work	Results
Value of claim presented for certification	£39,284,266
Amended/Not amended	Amended – subsidy increased by £1,933
Qualification letter	Yes
Fee – 2017-18	£11,770
Fee – 2016-17	£4,253

Local Government administers the Government's housing benefits scheme for tenants and can claim subsidies from the Department for Work and Pensions (DWP) towards the cost of benefits paid.

The certification guidance requires reporting accountants to follow a programme of work specified by DWP. Detailed case testing is carried out on an initial sample of 20 cases per benefit type. More extensive '40+' or extended testing is undertaken if initial testing identifies errors in the calculation of benefit or compilation of the claim. 40+ testing may also be carried out as a result of errors that have been identified in the certification of previous years claims.

Extended and other testing identified errors which the Council amended. They had a small net impact on the claim. We have reported underpayments, uncertainties and the extrapolated value of other errors in a qualification letter. The DWP then decides whether to ask the Council to carry our further work to quantify the error or to claw back the benefit subsidy paid.

A summary of the issues identified and their impact is presented on the next page.

We found errors and carried out extended testing in several areas.

Extended and other testing identified errors which the Council amended. They had a small net impact on the claim, as noted above.

We have reported underpayments, uncertainties and the extrapolated value of other errors in a qualification letter. The DWP then decides whether to ask the Council to carry our further work to quantify the error or to claw back the benefit subsidy paid. We include in this report a summary of the main issues we reported in our qualification letter.

Non Housing Revenue Account Rent Rebates: Incorrect Application of Family Premium

- ▶ Initial testing identified one error, where the Council had where the Authority had overpaid benefit as a result of incorrectly applying family premium when the claimant was not entitled to the allowance.
- ▶ Our extended testing identified no further errors. The extrapolated impact of the errors resulted in an overpayment of subsidy of £86.

Non Housing Revenue Account Rent Rebates: Incorrect Calculation of Earned Income

- ▶ Initial testing identified one error, where the Council had miscalculated earned income resulting in an underpayment of benefits. As there is no eligibility to subsidy for benefit which has not been paid, the underpayments identified do not affect subsidy, and thus has not been classified as error for subsidy purposes. However, given the nature of the population and the error found which in other circumstances may have led to an overpayment, an additional random sample of 40 cases was selected for testing from a subpopulation of cases with earnings
- ▶ Our extended testing identified eight further errors relating to the calculation of earned income. Four of these cases resulted in an overpayment of benefits, and four cases resulted in an underpayment of benefits. As there is no eligibility for subsidy for benefit that has not been paid, the four underpayments were not classified as errors for subsidy purposes and have no impact on the claim. The extrapolated impact of the errors resulted in an overpayment of subsidy of £293.

Rent Allowances: Incorrect Calculation of weekly rent liability

- ▶ Initial testing identified three errors, where the Council had miscalculated weekly rent liability resulting in an overpayment of benefits.
- ▶ Our extended testing identified two further cases where the council had miscalculated weekly rent liability resulting in an underpayment of benefit. As there is no eligibility for subsidy for benefit that has not been paid, the two underpayments were not classified as errors for subsidy purposes and have no impact on the claim. The extrapolated impact of the three errors resulted in overpayment of subsidy of £134.

Rent Allowances: Incorrect Calculation of Earned Income

- ▶ Initial testing identified one error, where the Council had miscalculated earned income resulting in an overpayment of benefits.
- ▶ Our extended testing identified nine further errors relating to the calculation of earned income. Five of these cases resulted in an overpayment of benefits, and four cases resulted in an underpayment of benefits. As there is no eligibility for subsidy for benefit that has not been paid, the four underpayments were not classified as errors for subsidy purposes and have no impact on the claim. The extrapolated impact of the errors resulted in an overpayment of subsidy of £61.



02

2017-18 certification fees





2017-18 certification fees

The PSAA determine an indicative fee each year for the certification of the housing benefits subsidy claim. For 2017-18 they are based on the outturn from 2015/16. These indicative fees were published by the Public Sector Audit Appointments Ltd (PSAA's) and are available on their website (www.psa.co.uk).

Claim or return	2017-18	2017-18	2016-17
	Actual fee £	Indicative fee £	Actual fee £
Housing benefits subsidy claim	£11,770	£5,492	£4,253

The significant increase in fee is due to the increased number of errors and therefore additional work required in 2017/18 when compared to 2015/16.

The indicative scale fee for 2017/18 of £5,492 is based on the final fee charged in 2015/16. In that year there was only one extended testing sample.

Our final fee for 2017/18 is £11,770, an increase of £6,278. Based on the errors described in section 1 of this report, we required additional time to complete compared to the 2015/16 baseline year. An additional 5 lots of extended testing were performed.

The 40+ testing initially performed by the client had to be re-captured in the HBCount workbooks, and test a sample of 10% of passed cases and all fails. The earnings workbooks in particular contained a number of complex failed cases which each took several hours to create and review.

We have discussed the overall fee increase and final fee with the Head of Finance and Head of Revenues and Benefits. The final fee is subject to agreement by both management and the Public Sector Auditor Appointments Ltd.



03

Looking forward



2018/19 and beyond

From 2018/19, the Council is responsible for appointing their own reporting accountant to undertake the work on their claims in accordance with the instructions determined by the relevant grant paying body.

These new freedoms represent an opportunity for Local Authorities to engage a Reporting Accountant that is not necessarily the same as the one appointed to undertake the audit of the financial statements, but rather one that it feels will best serve its assurance requirements.

Although we have not been selected to undertake the Housing Benefit Assurance Process for the Council for 2018/19, as the assurance provider to over 160 Local Government bodies, we believe that we are well placed to provide these services to you and can draw on a vast array of experienced and knowledgeable professionals to deliver the quality assurance that Local Government needs in these challenging times.

If you would like us to quote for the provision of grant claim work, please contact Kevin Suter who will be happy to discuss your requirements and provide a competitive quotation.



04

Summary of recommendations



Summary of recommendations

This section highlights the recommendations from our work and the actions agreed.

Recommendation	Priority	Agreed action and comment	Deadline	Responsible officer
Work with Northgate to quantify the extent of the misclassification error between cells 14 and 15 and account for the error in a future subsidy claim	High	<p>As part of our initial testing, we noted a fail which resulted in the incorrect classification of subsidy between underlying cells 14 & 15 (total error value £13.85). The Authority has confirmed that this has been a Northgate system error to be patched in 2018/19. Correspondence between the Authority and the Software Provider has confirmed the issue.</p> <p>The Authority has also logged this issue with the DWP. The Authority has considered if they could run any reports to identify potential claims which have been affected by this bug, and have concluded they are not able to do so due to the complexity of the issue. They will apply the fix to correct any affected claims (if any more) as soon as Northgate provide a solution and can confirm this in a future subsidy claim check.</p>	Action to be completed in time for 2018/19 Housing Benefit Grant Certification work	Sue Mullins

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2017 EYGM Limited.
All Rights Reserved.

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com

This page is intentionally left blank

EMT - 15 JANUARY 2019
AUDIT COMMITTEE – 25 JANUARY 2019

INTERNAL AUDIT PROGRESS REPORT 2018-19 – DECEMBER 2018

1. INTRODUCTION

- 1.1. The purpose of this report is to provide the Audit Committee with an overview of internal audit activity completed in accordance with the approved audit plan and to provide an overview of the status of 'live' reports.

2. SUMMARY

- 2.1. Under the Accounts and Audit (England) Regulations 2015, the Council is responsible for:

- ensuring that its financial management is adequate and effective and that it has a sound system of internal control which facilitates the effective exercise of functions and includes arrangements for the management of risk; and
- undertaking an adequate and effective internal audit of its accounting records and of its system of internal control in accordance with the proper practices in relation to internal control.

- 2.2. In accordance with the Public Sector Internal Audit Standards and the Council's Internal Audit Charter, the Chief Internal Auditor is required to provide a written status report to the Governance and Audit Committee, summarising:

'communications on the internal audit activity's performance relative to its' plan.'

- 2.3. Appendix 1 summarises the performance of Internal Audit for 2018-19.

3. FINANCIAL IMPLICATIONS

- 3.1. The audit plan consists of 470 audit days including 18 audit days provided to the New Forest National Park Authority under the current Service Level Agreement. The Council's budget for 2018-19 reflects these arrangements.

4. CRIME AND DISORDER IMPLICATIONS

- 4.1. There are no crime and disorder implications arising directly from this report, however inadequate audit coverage may result in areas of control weakness, unacceptable risks or governance failings as well as the increased potential for error and fraud.

5. ENVIRONMENTAL MATTERS & EQUALITY AND DIVERSITY IMPLICATIONS

5.1. There are no matters arising directly from this report.

6. RECOMMENDATION

6.1. The Audit Committee note the content of the progress report.

For Further Information Please Contact:

Antony Harvey
Deputy Head of Partnership (SIAP)
Tel: 01962 845701
E-mail: antony.harvey@hants.gov.uk

Background Papers:

Internal Audit Plan 18-19

Internal Audit Progress Report

December 2018

New Forest District Council



**Southern Internal
Audit Partnership**

Assurance through excellence
and innovation

Contents:

1.	Role of Internal Audit	3
2.	Purpose of report	4
3.	Performance dashboard	5
4.	Status of 'live' reports	6 – 8
5.	Executive summaries 'Limited' and 'No' assurance opinions	9
6.	Planning and resourcing	10
7.	Rolling work programme	10 - 13
Annex A	Audit assurance opinion definitions in place prior to SIAP	14

1. Role of Internal Audit

The requirement for an internal audit function in local government is detailed within the Accounts and Audit (England) Regulations 2015, which states that a relevant body must:

‘Undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector internal auditing standards or guidance.’

The standards for ‘proper practices’ are laid down in the Public Sector Internal Audit Standards [the Standards - updated 2017].

The role of internal audit is best summarised through its definition within the Standards, as an:

‘Independent, objective assurance and consulting activity designed to add value and improve an organisations operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes’.

The Council is responsible for establishing and maintaining appropriate risk management processes, control systems, accounting records and governance arrangements. Internal audit plays a vital role in advising the Council that these arrangements are in place and operating effectively.

The Council’s response to internal audit activity should lead to the strengthening of the control environment and, therefore, contribute to the achievement of the organisation’s objectives.

2. Purpose of report

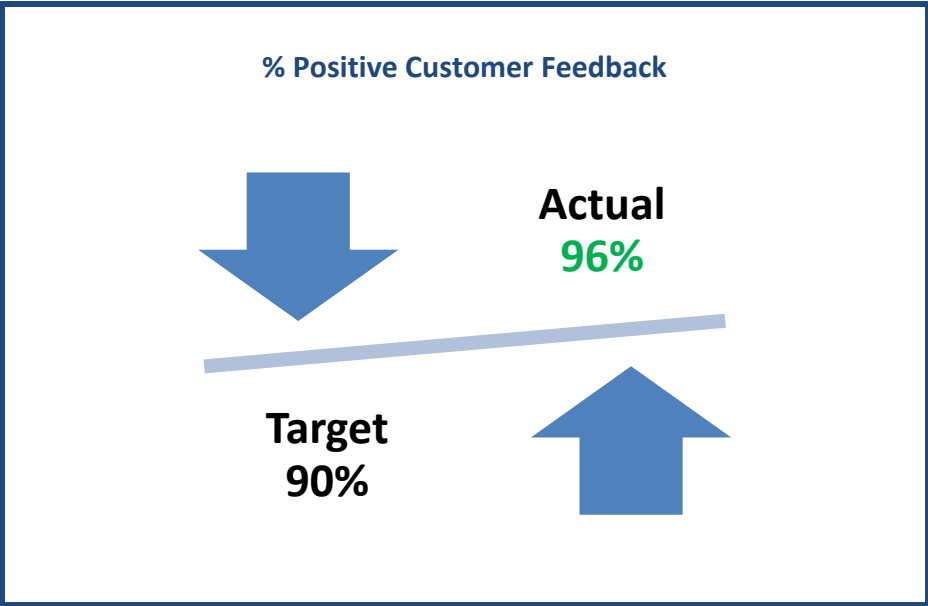
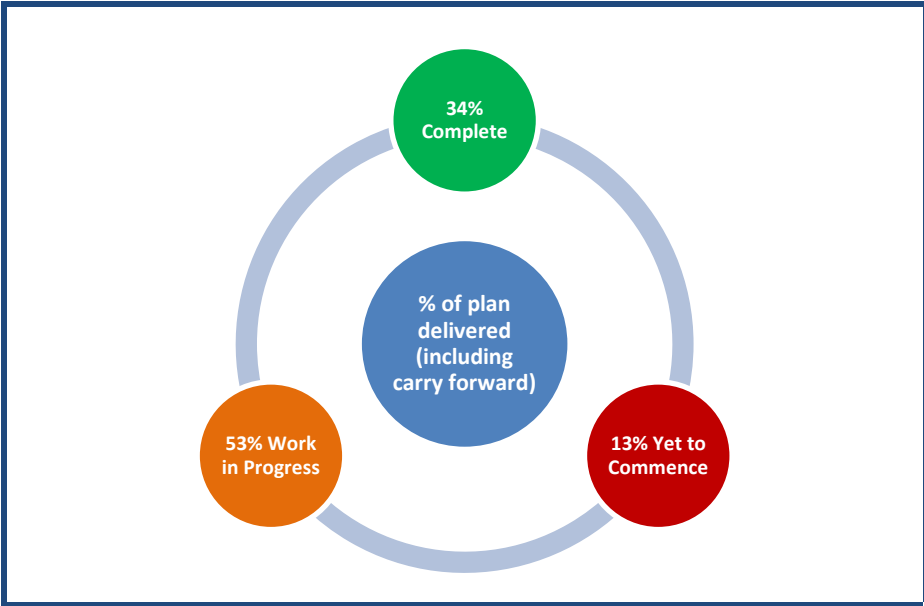
In accordance with proper internal audit practices (Public Sector Internal Audit Standards), and the Internal Audit Charter the Chief Internal Auditor is required to provide a written status report to ‘Senior Management’ and ‘the Board’, summarising:

- The status of ‘live’ internal audit reports;
- an update on progress against the annual audit plan;
- a summary of internal audit performance, planning and resourcing issues; and
- a summary of significant issues that impact on the Chief Internal Auditor’s annual opinion.

Internal audit reviews culminate in an opinion on the assurance that can be placed on the effectiveness of the framework of risk management, control and governance designed to support the achievement of management objectives of the service area under review. Assurance opinions are categorised as follows:

Substantial	A sound framework of internal control is in place and operating effectively. No risks to the achievement of system objectives have been identified
Adequate	Basically a sound framework of internal control with opportunities to improve controls and / or compliance with the control framework. No significant risks to the achievement of system objectives have been identified
Limited	Significant weakness identified in the framework of internal control and / or compliance with the control framework which could place the achievement of system objectives at risk
No	Fundamental weaknesses identified in the framework of internal control or the framework is ineffective or absent with significant risk to the achievement of system objectives.

3. Performance dashboard



Page 75

Compliance with Public Sector Internal Audit Standards / Local Government Application Note



An 'External Quality Assessment' of the Southern Internal Audit Partnership was undertaken by the Institute of Internal Auditors (IIA) in September 2015. The report concluded:

*'It is our view that the Southern Internal Audit Partnership 'generally conforms' (top grading) to **all** of the principles contained within the International Professional Practice Framework (IPPF); Public Sector Internal Audit Standards (PSIAS); and the Local Government Application Note (LAGN).*

In accordance with PSIAS, a further self assessment was completed in April 2018 concluding that the Southern Internal Audit Partnership continues to comply with all aspects of the IPPF, PSIAS and LGAN.

4. Status of 'Live' Reports

Audit Review	Report Date	Audit Sponsor	Assurance Opinion	Management Actions ('High Priority')				
				Reported	Not Accepted	Pending	Cleared	Overdue
<p>There are 23 outstanding actions from 8 audits relating to reviews completed prior to the 2017/18 audit plan. These actions will be tracked through to completion or on occasion, obsolescence if, for example, they are superseded by alternative actions to address the issues identified. Of the 23 outstanding actions, four are high priority and relate to the following areas:-</p> <ul style="list-style-type: none"> • ICT – VM upgrade. Current progress - The servers are being replaced. In the interim, to address current issues, more memory has been added to the servers, which has increased stability and taken the pressure off for the short term. All servers are planned to be running on the new virtual environment by the end of Jan 2019. • Payment Card Industry Data Security Standards (PCI DSS) Compliance. Current progress – There are elements of the current financial system and telephony system that are non-compliant. These systems are due to be replaced in 2019. • Business Continuity. Current progress – An initial Business Impact Analysis (BIA) has been completed with Service Managers. A proposed critical activity list has been developed and discussed with EMT. The critical activity list will be reviewed and will inform an in-depth BIA process with the aim to test Business Continuity Plans and the Emergency Response Plan during an annual exercise planned during the Spring 2019. This will be followed up by Internal Audit as part of in 2019/20 audit plan. 								
(Housing) Estates Management 2017/18 **	Sep-17	SM (HM)	Reasonable*	3 (0)	0 (0)	0 (0)	3 (0)	0 (0)
VAT 2017/18 **	Nov-17	HoF	Reasonable*	4 (0)	0 (0)	0 (0)	4 (0)	0 (0)
Accounts Payable 2017/18 **	Dec-17	HoF	Reasonable*	3 (0)	0 (0)	0 (0)	3 (0)	0 (0)
Health and Leisure Centres 2017/18	Jan-18	SM (H&L)	Limited*	35 (5)	0 (0)	0 (0)	32 (5)	3 (0)
Resident Involvement 2017/18	Jan-18	SM (EM&S)	Reasonable*	4 (0)	0 (0)	1 (0)	3 (0)	0 (0)
Trees (Council Owned) 2017/18 **	Feb-18	SM (OP)	Reasonable*	9 (1)	0 (0)	0 (0)	9 (1)	0 (0)

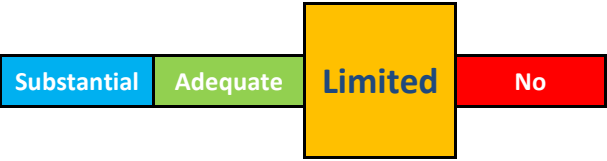

Audit Review	Report Date	Audit Sponsor	Assurance Opinion	Management Actions ('High Priority')				
				Reported	Not Accepted	Pending	Cleared	Overdue
Income 2017/18	Mar-18	SM (BI&CS)	Reasonable*	10 (0)	0 (0)	2 (0)	8 (0)	0 (0)
Asset Management 2017/18 **	Mar-18	SM (E&V)	Substantial*	1 (0)	0 (0)	0 (0)	1 (0)	0 (0)
Sundry Income (AR) 2017/18	Mar-18	HoF	Substantial*	5 (0)	0 (0)	1 (0)	4 (0)	0 (0)
Payroll (inc NFNPA testing, T&S Members, Allowances & Expenses) 2017/18	Jul-18	HoF / SM (HR)	Reasonable*	2 (0)	0 (0)	1 (0)	1 (0)	0 (0)
Vehicle and Plant Maintenance/Transport & Fleet Management System 2017/18	Jul-18	SM (W&T)	Reasonable*	3 (0)	0 (0)	1 (0)	2 (0)	0 (0)
Disabled Adaptation Funding **	Oct-18	SM (E&R)	Adequate	5 (0)	0 (0)	0 (0)	5 (0)	0 (0)
Environmental Services - Trade Waste	Oct -18	SM (W&T)	Limited	18 (5)	0 (0)	18 (5)	0 (0)	0 (0)
Accounts Payable	Nov- 18	HoF	Adequate	3 (0)	0 (0)	1 (0)	2 (0)	0 (0)
NNDR **	Nov- 18	SM (R&B's)	Substantial	1 (0)	0 (0)	0 (0)	1 (0)	0 (0)
Council Tax **	Nov- 18	SM (R&B's)	Substantial	1 (0)	0 (0)	0 (0)	1 (0)	0 (0)

* Please see Annex A for the audit assurance opinion definitions in place prior to SIAP

** Denotes audits where all actions have been completed since the last progress report

Audit Sponsor	
Service Manager (Business Improvement & Customer Services)	SM (BI&CS)
Head of Finance	HoF
Service Manager (Estates & Valuation)	SM (E&V)
Service Manager (Human Resources)	SM (HR)
Service Manager (Legal)	SM(L)
Service Manager (Democratic Services & Member Support)	SM (DS&MS)
Service Manager (Estate Management & Support)	SM (EM&S)
Service Manager (Revenues & Benefits)	SM (R&B)
Service Manager (ICT)	SM (ICT)
Service Manager (Housing Options)	SM (HO)
Service Manager (Housing Maintenance)	SM (HM)
Service Manager (Environmental & Regulation)	SM (E&R)
Service Manager (Health & Leisure)	SM (H&L)
Service Manager (Waste & Transport)	SM (W&T)
Service Manager (Coastal & Public Facilities)	SM (C&PF)
Service Manager (Open Spaces)	SM (OS)

5. Executive Summaries of new reports published concluding a ‘Limited’ or ‘No’ assurance opinion

Environmental Services – Trade Waste		
<p>Audit Sponsor: Chris Noble, Service Manager, Waste and Transport</p> <p>Key Contacts: Hannah Neale, Trade Waste Administrator Samantha Marrache, Administration Supervisor.</p> <p>Final Report Issued: 26/10/2018</p>	<p>Assurance opinion:</p> 	<p>Management Actions:</p> 
<p>Summary of key observations: Following both management and service administration staffing changes, the new Service Manager identified areas of weakness and requested Internal Audit complete an end to end process review, with a specific focus on the costing elements, to help inform a Service review and the development of a new Service Plan.</p> <p>There are known issues with the accuracy of disposal data which informs the charges paid to Hampshire County Council. The Service Manager is keen to address the issue and had initiated a sound sampling process/methodology to enhance data accuracy (e.g. average weight of bags/bins) which was still in progress at the time of the review. The accuracy of data and practice of co-collection with domestic waste has resulted in the costs of the service not being fully understood. Although uplifted annually, charges have not been reviewed to ensure they cover costs therefore it is not clear whether the service is making a surplus or loss.</p> <p>The customer database does not link to other systems, such as finance and stock control, and, as a consequence, some issues were identified with invoicing, debtors, and the availability and accuracy of management information. Trade Waste customers are not issued with contracts or any terms and conditions and as such, often start, change or cease services without notice and at a potential cost to the Council. The review found some sales of trade waste sacks to unregistered traders.</p>		

6. Planning & Resourcing

The Internal Audit Plan provides the mechanism through which the Chief Internal Auditor can ensure the most appropriate use of internal audit resources to provide a clear statement of assurance on risk management, internal control and governance arrangements.

The Internal Audit Plan for 2018-19 was discussed by EMT on 20 February 2018 and approved by the Audit Committee on 23 March 2018. The audit plan remains fluid to provide a responsive service that reacts to the changing needs of the Council. Progress against the plan is detailed within section 7.

7. Rolling Work Programme

Audit Review	Audit Sponsor	Scoping	Audit Outline Issued	Fieldwork	Draft Report Issued	Final Report Issued	Assurance Opinion	Tracker (✓ on schedule ✗ Delay)	Comment
Corporate / Cross Cutting									
Programme and Project Management	SM (BI&CS)	✓						✓	
Financial Stability	HoF	✓						✓	
Income Generation & Commercialisation	SM (E&V)							✓	Q4
Working in Partnership	SM (BI&CS)							✓	Q4
Corporate Governance									

Audit Review	Audit Sponsor	Scoping	Audit Outline Issued	Fieldwork	Draft Report Issued	Final Report Issued	Assurance Opinion	Tracker (✓ on schedule ✗ Delay)	Comment
Human Resources	SM (HR)	✓	✓					✓	
Fraud & Irregularities	HoF	✓	n/a	✓				✓	
Procurement	SM (L)	✓	✓					✓	
Contract Management	SM (L)	✓	✓					✓	
Information Governance	SM (L)	✓	✓	✓	✓			✓	
Ethical Governance	SM (DS&MS)	✓	✓	✓				✓	
Risk Management	SM (BI&CS)	✓	✓	✓				✓	
Financial Management									
Housing Rents	SM (EM&S)	✓	✓	✓	✓	✓	Substantial	✓	
Housing Benefits	SM (R&B)	✓	✓	✓	✓	✓	Substantial	✓	
Council Tax	SM (R&B)	✓	✓	✓	✓	✓	Substantial	✓	
Accounts Payable	HoF	✓	✓	✓	✓	✓	Adequate	✓	
Accounts Receivable / Debt Management	SM (R&B)	✓	✓	✓	✓	✓	Substantial	✓	

Audit Review	Audit Sponsor	Scoping	Audit Outline Issued	Fieldwork	Draft Report Issued	Final Report Issued	Assurance Opinion	Tracker (✓ on schedule ✗ Delay)	Comment
Main Accounting	HoF	✓	✓	✓				✓	
Treasury Management	HoF	✓	✓	✓	✓	✓	Substantial	✓	
NNDR	SM (R&B)	✓	✓	✓	✓	✓	Substantial	✓	
Payroll	HoF / SM (HR)	✓						✓	
Income Collection	SM (BI&CS)	✓	✓					✓	
Information Technology									
IT Strategy and assurance mapping	SM (ICT)	✓	n/a	✓	n/a	n/a	n/a	✓	
Business Continuity / Disaster Recovery Planning	SM (ICT)	✓	✓					✓	
ICT Programme / Project Management	SM (ICT)	✓	✓	✓	✓			✓	
PCI DSS (Kisoks)	SM (ICT)	✓	n/a	✓	n/a	n/a	n/a	✓	Advisory role
Portfolio Themes									
Homelessness & Affordable Housing	SM (HO)	✓	✓	✓				✓	

Audit Review	Audit Sponsor	Scoping	Audit Outline Issued	Fieldwork	Draft Report Issued	Final Report Issued	Assurance Opinion	Tracker (✓ on schedule ✗ Delay)	Comment
Housing Asset Management	SM (HM)							✓	Q4
Housing Finance	SM (EM&S)	✓						✓	
Disabled Adaptation Funding	SM (E&R)	✓	✓	✓	✓	✓	Adequate	✓	
Health & Leisure Facilities	SM (H&L)							✓	Q4
Environmental Services - Trade Waste	SM (W&T)	✓	✓	✓	✓	✓	Limited	✓	
Development / Building Control	SM (C&PF)	✓						✓	

Plan variations:-

Licensing – Defer the audit to 2019/20 due to pending legislative changes and staffing changes within the team.

Establishment Reviews – Defer the audit – use the outcomes of 2018/19 audit work to inform potential scope or assess whether a review is necessary.

Annex A

Audit Assurance Opinion Definitions in place prior to SIAP

Substantial - A strong system of internal controls, designed and operating effectively.

Reasonable - A sound system of internal controls; but one where minor weaknesses were found in the system design, or lack of compliance to the design;

Limited - Some weakness was identified in the overall system of controls, or the level of compliance resulted in risk to the achievement of system objectives;

No - Fundamental weakness was identified within one or more key controls, or controls were not operating effectively which may put at risk the achievement of the corporate control objective.

AUDIT COMMITTEE – 25 JANUARY 2019

THE REGULATION OF INVESTIGATORY POWERS ACT 2000

1. INTRODUCTION

- 1.1 The purpose of this report is to provide the Audit Committee with a summary of the Council's use of its powers under the Regulation of Investigatory Powers Act 2000 (RIPA).
- 1.2 RIPA provides a statutory framework whereby certain surveillance and information gathering activities can be authorised and conducted by the Council in a lawful manner where they are carried out for the prevention and detection of crime and, in some cases, for the prevention of disorder.
- 1.3 The Council has two policies ('the policies') relating to its use of RIPA:
 - 1.3.1 Surveillance Policy – updated 15 January 2019 (**Appendix 1**)
 - 1.3.2 Policy for the Acquisition of Communications Data – updated 15 January 2019 (**Appendix 2**)
- 1.4 In accordance with these policies the Legal Services Manager is required to report to the Audit Committee every two years on the Council's use of RIPA unless the specific powers have been used in the first of the two years, in which case a report will be made to the next Audit Committee following use of the powers.
- 1.5 The policies were updated to reflect changes to the management structure of the Council and to minor updates to legislation and the government Codes of Practice.

2. BACKGROUND

- 2.1 When the Human Rights Act 1998 came into force in 2000 it made the fundamental rights and freedoms contained in the European Convention on Human Rights (ECHR) enforceable in the UK.
- 2.2 Article 8 of the ECHR provides that individuals have the right to respect for private and family life and Article 6 of the ECHR provides that individuals have the right to a fair trial.
- 2.3 The use of covert surveillance techniques is considered to be an interference with this Article 8 right and therefore RIPA provides a framework to render lawful surveillance activities which might otherwise be in breach of the ECHR. It is also aimed at ensuring that evidence obtained against a person to be used in criminal proceedings is obtained in a fair manner.
- 2.4 RIPA regulates three surveillance techniques available to local authorities, namely:
 - 2.4.1 Directed surveillance - covert surveillance which is carried out as part of a specific investigation and is likely to involve the obtaining of private information about the person under investigation;

- 2.4.2 Covert Human Intelligence Sources (CHIS) – use of a person who establishes and maintains a relationship with the person under investigation in order to obtain and disclose information; and
 - 2.4.3 The acquisition and disclosure of communications data - obtaining information from communication service providers (e.g. the postal service, telephone companies and internet companies) about the use made of a service (e.g. itemised billing, internet connections or records of registered post) and user information (e.g. subscriber names, addresses or other customer information).
- 2.5 RIPA provides that the above activities may be authorised by local authorities but must be necessary and proportionate.

3. THE COUNCIL'S USE OF RIPA

- 3.1 The Council uses its powers under RIPA infrequently.
- 3.2 The Council did not authorise any surveillance activities under RIPA since the last report to the Audit Committee in March 2017.

4 TRAINING

- 4.1 In accordance with the policies, all staff with responsibilities related to RIPA will be trained by Legal Services during the course of January/ February 2019.

5 INVESTIGATORY POWERS COMMISSIONER INSPECTION

- 5.1 The Investigatory Powers Commissioner's Office (IPCO) provides independent oversight of the use of investigatory powers by public authorities and the Council was due for inspection by the IPCO at the end of 2018.
- 5.2 On 19 December 2018, a completed remote assessment questionnaire was returned to the IPCO detailing the Council's policies, training and use of RIPA since the last inspection in October 2015.
- 5.3 On 20 December 2018, Mr Graham Horne, Inspector at the IPCO confirmed that the questionnaire submitted "demonstrates a level of compliance that removed the need for a physical inspection." The next inspection will be due in 2021.

6. ENVIRONMENTAL IMPLICATIONS

- 6.1 There are no environmental implications arising from this report.

7. CRIME AND DISORDER IMPLICATIONS

- 7.1 The Council's use of RIPA relates to the prevention and detection of crime and, in some cases, the prevention of disorder. It is essential the Council complies with RIPA if covert surveillance techniques are used in order to prevent legal challenge and ensure that evidence obtained is admissible in criminal proceedings. As stated above, the Council rarely uses its powers under RIPA.

8. CONCLUSION

- 8.1 RIPA provides the Council with a statutory framework to follow so that it may carry out various covert investigatory activities in a lawful manner.

8.2 The Council uses its powers under RIPA infrequently, but when use is made of such powers it is essential that this is done in accordance with the law and the Council's policies.

9. RECOMMENDATION

It is recommended that:-

9.1 Members note the use made by the Council of its powers under RIPA.

Further Information

Andrew Kinghorn
Legal Services Manager
Telephone: 02380 285588
Email: andrew.kinghorn@nfdc.gov.uk

Background Papers

Published documents

Amanda Wilson
Solicitor
Telephone: 02380 285588
Email: amanda.wilson@nfdc.gov.uk

This page is intentionally left blank



SURVEILLANCE POLICY

Human Rights Act 1998

Regulation of Investigatory Powers Act 2000

Protection of Freedoms Act 2012

Investigatory Powers Act 2016

THIS POLICY MUST BE READ IN CONJUNCTION WITH THE REVISED HOME OFFICE CODES OF PRACTICE: "COVERT SURVEILLANCE AND PROPERTY INTERFERENCE" AND "COVERT HUMAN INTELLIGENCE SOURCES" (AUGUST 2018) AND ANY GUIDANCE ISSUED BY THE INVESTIGATORY POWERS COMMISSIONER'S OFFICE

CONTENTS**Page**

1.	Background	3
2.	Definitions	4
3.	Directed Surveillance	5
4.	CCTV	7
5.	Private Information	8
6.	Control and Use of Covert Human Intelligence Sources	8
7.	Online Covert Activity	12
8.	Authorisations, Renewals, Reviews and Cancellations	12
9.	Application Forms	15
10.	The Necessity and Proportionality Test	16
11.	Confidential Material	18
12.	Activities By Other Public Authorities	18
13.	Joint Investigations	18
14.	Data Protection	18
15.	Destruction of Wholly Unrelated Material	19
16.	Training	20
17.	Records of Authorisations	20
18.	Monitoring	21
19.	Senior Responsible Officer	22
20.	Policy and Implementation	22
21.	Appendices Appendix 1: Functions that may be undertaken by Authorised Officers Appendix 2: Application & Authorisation Checklist Appendix 3: Legal Services Manager & Senior Responsible Officer	23

1 BACKGROUND

- 1.1 When the Human Rights Act 1998 came into force in 2000 it made the fundamental rights and freedoms contained in the European Convention on Human Rights enforceable in UK Courts and Tribunals.
- 1.2 Article 8 of the Convention reads as follows: -
- “Everyone has the right to respect for his private and family life his home and his correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of public safety, for the protection of order, health or morals, or for the rights and freedoms of others.”
- 1.3 Investigating Officers of the Council may, from time to time, engage in activities which interfere with a person’s right under Article 8 of the Convention to respect for their private and family life. Such interference is only permissible where it complies with the exceptions set out in Article 8.
- 1.4 The Regulation of Investigatory Powers Act 2000 (“RIPA”) provides a statutory framework whereby certain surveillance activities can be authorised and conducted compatibly with Article 8 by public bodies. RIPA is also supplemented by the relevant provisions of the Investigatory Powers Act 2016.
- 1.5 Officers of New Forest District Council (“the Council”) may seek authorisation under RIPA to engage in the following types of surveillance: -
- Directed surveillance
 - Use of a Covert Human Intelligence Source
- 1.6 These surveillance techniques can **only** be authorised under RIPA where the use of the surveillance is necessary for the **prevention or detection of crime**, or (in some cases) for the **prevention of disorder**. Since **1 November 2012**, it is **only** possible to authorise directed surveillance under RIPA where the matter under investigation constitutes a **criminal offence** for which the courts could impose a maximum term of at least six months’ imprisonment, **or** where the surveillance is in connection with the sale of alcohol or tobacco to children.
- 1.7 The Council can only authorise surveillance under RIPA in connection with the performance of the specific public functions which it carries out. It cannot use RIPA to authorise surveillance in connection with the ordinary functions (e.g., employment issues) which are carried out by all public authorities.
- 1.8 This Surveillance Policy explains what is involved in each of these two types of surveillance. The policy sets out the relevant responsibilities of the Council and its officers, and is designed to ensure that any such surveillance is conducted in a manner that will comply with the safeguards embodied in the Human Rights Act 1998 and RIPA.
- 1.9 All Investigating Officers and Authorising Officers should be familiar with RIPA, this Surveillance Policy, the Codes of Practice issued by the Home Office relating to the Use of Covert Human Intelligence Sources and Covert Surveillance and Property

2 DEFINITIONS:

2.1 Confidential Information

This includes:

- Matters subject to legal privilege: Information relating to communications between a professional legal advisor and their client for the purposes of giving advice, in contemplation of legal proceedings or relating to legal proceedings.
- Confidential personal information: Information which relates to the physical or mental health, or spiritual counselling of a person (living or dead) who can be identified from it. For example, information about medical consultations/medical records.
- Confidential constituent information: Information relating to communications between a Member of Parliament and constituent in respect of constituency matters.
- Confidential journalistic information

2.2 Collateral Intrusion

Collateral Intrusion is the likely effect of the use of surveillance on the private and family life of persons who are not the intended subjects of the activity.

2.3 Surveillance

Surveillance includes

- 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.
- surveillance by, or with, the assistance of a surveillance device.

Surveillance can be **overt** or **covert**.

2.4 Overt Surveillance

Overt surveillance is surveillance which is not secretive or hidden. It includes surveillance where the subject has been told it will happen.

2.5 Covert Surveillance

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

2.6 Directed Surveillance

Directed surveillance is **covert** but **not intrusive** and is undertaken:

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

2.7 Intrusive surveillance

Intrusive Surveillance occurs when surveillance:

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

Intrusive surveillance cannot be carried out or approved by the Council.

2.8 The conduct and use of covert human intelligence sources (CHIS)

The conduct and use of covert human intelligence sources occurs when a person establishes or maintains a personal or other relationship with a person:

- For the covert purpose of using the relationship to obtain information or to provide access to any information to another person or

To covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

3 DIRECTED SURVEILLANCE

- 3.1 This paragraph should be read in conjunction with the Revised Home Office Code of Practice “Covert Surveillance and Property Interference” which can be found at <https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice>

- 3.2 Directed surveillance is surveillance which meets **all** of the following criteria:

i. It is covert, but not intrusive surveillance

Surveillance will be covert if it is carried out in a way calculated to ensure that the subject of the surveillance is unaware that it is taking place.

The Council **cannot** engage in intrusive surveillance.

ii. It is conducted for the purposes of a specific investigation or operation

iii. It is likely to result in the obtaining of private information about a person (whether or not specifically identified for the purposes of the investigation or operation)

“Private information” includes any information relating to a person’s private or family life, including their relationships with others, their family, and professional or business relationships.

For more information about what constitutes “private information”, see paragraph 5 below.

iv. 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 reasonable for an authorisation under RIPA to be sought.

For example, if an officer happens to spot an offence taking place, they may stop and take photographs as evidence of that offence, without requiring prior authorisation under RIPA.

3.3 Any officer intending to conduct directed surveillance must seek prior authorisation of that surveillance under RIPA (see paragraphs 8,9 & 10 below, regarding applications and authorisations).

3.4 Since **1 November 2012**, it is **only** possible to authorise directed surveillance under RIPA where the matter under investigation constitutes a **criminal offence** for which the courts could impose a maximum term of at least six months’ imprisonment, **or** where the surveillance is in connection with the sale of alcohol or tobacco to children.

3.5 Examples

3.5.1 Since 1 November 2012, it is no longer possible to authorise directed surveillance under RIPA for the following offences:

- Dog fouling
- Littering
- Planning offences
- Noise abatement notices

As the courts **cannot** impose a maximum term of at least six months’ imprisonment.

3.5.2 It is possible to authorise directed surveillance under RIPA for some offences under the following categories:

- Fly tipping

- Benefit fraud
- Trading standards offences
- Financial offences
- Dangerous dogs
- Listed building offences

As the courts **can** impose a maximum term of at least six months' imprisonment.

- 3.6 It is possible that on rare occasions, officers may need to carry out covert surveillance which falls outside the scope of RIPA, either because it falls outside of the Council's core functions (i.e. its specific public functions) and is therefore an ordinary function undertaken by all authorities (e.g., disciplinary investigations) or because the matter under investigation does not pass the imprisonable crime threshold. Such surveillance may not be unlawful, but would take place without the protection afforded by RIPA. In these situations, officers would normally be expected to use similar procedures and forms to those used for RIPA operations, applying the same tests of necessity and proportionality, in order to protect the Council from allegations that it has acted unfairly. Should you wish to conduct such covert surveillance, advice must first be sought from Legal Services.

4 CCTV

- 4.1 The Council operates a close circuit television system within certain towns in the New Forest District. Use of this system by the council or third parties such as the police for directed surveillance would require authorisation under RIPA.
- 4.2 Overt CCTV cameras which are permanently sited for the purposes of, for example, monitoring traffic flow or public safety will not generally require RIPA authorisation, since the public will be aware that such systems are in use. However, there may be occasions when the Council wishes to use such CCTV cameras for the purposes of a specific investigation or operation or to target a specific person. In such circumstances (unless as an immediate response to events) consideration must be given as to whether authorisation for directed surveillance is required.
- 4.3 For example, authorisation for directed covert surveillance is likely to be required if the Council wishes to make use of permanently sited overt CCTV cameras in circumstances where Officers have received reports of unlawful trading at a specific location, and wish to use those existing CCTV systems to keep watch for such activities.
- 4.4 If another agency – eg the Police – wishes to use the Council's CCTV cameras for one of their investigations, this must be agreed by the Head of Public Health and Community Safety, or by the Civil Contingencies and CCTV Manager. A copy of the other agency's RIPA authorisation form must be obtained and the details held with the Council's central register. In such circumstances, as long as there is a Police RIPA authorisation, there is no separate need for one of the Council's Authorised Officers to authorise the use of the cameras.

4.5 Deployable CCTV

The deployment of mobile surveillance cameras is likely to be directed surveillance in all cases and appropriate RIPA authorisation will be required. Additionally, applicants will be required to complete a “Mobile CCTV Deployment Form”, in accordance with the Council’s Deployable (Mobile) CCTV Camera Policy. This form should be submitted to the Council’s CCTV Manager.

5 PRIVATE INFORMATION

- 5.1 The 2000 Act states that private information includes any information relating to a person’s private or family life. Private information should be taken generally to include any aspect of a person’s private or personal relationships with others, including family and professional or business relationships. Private information may include personal data, such as names, telephone numbers and addresses.
- 5.2 Whilst a person may have a reduced expectation of privacy when in a public place, 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. For example, two people holding a conversation on a public street or bus may have a reasonable expectation of privacy, even though they are in a public place.
- 5.3 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. For example, where an officer drives past a restaurant to take a photograph of the exterior, this is unlikely to require authorisation under RIPA, as the officer is not collecting private information. However, if the officer wishes to revisit the restaurant on a number of occasions to try to establish occupancy of the premises, this is likely to result in the obtaining of private information about the occupier, and authorisation for directed surveillance will usually be required.

6 CONDUCT AND USE OF COVERT HUMAN INTELLIGENCE SOURCES (“CHIS”)

- 6.1 This paragraph should be read in conjunction with the Home Office Revised Code of Practice “Covert Human Intelligence Sources” which can be found at <https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice>
- 6.2 The conduct and use of covert human intelligence sources occurs when a person establishes or maintains a personal or other relationship with a person:
- For the covert purpose of using the relationship to obtain information or to provide access to any information to another person **or**
 - To covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

A person who uses a relationship to obtain information which they then pass to the Council could be a CHIS, even if the Council hasn’t asked them to use their relationship in this way (see paragraph 6.5 below).

- 6.3 The conduct or use of a CHIS may be authorised under RIPA where it is **necessary** for the **prevention or detection of crime, or for the prevention of disorder**.
- 6.4 A relationship is established or maintained for a covert purpose if it is conducted in a manner to ensure that one of the parties is unaware of its purpose. A relationship will only be used covertly and information will only be disclosed covertly if it is used or disclosed in a way which will ensure that one of the parties is unaware of the use or disclosure.
- 6.5 The use of such sources by the Council is essentially the manipulation of a relationship to gain information and can amount to the use of an informant.. It should be noted that the use or conduct of a CHIS is a particularly intrusive and high risk covert technique. Therefore, where the use of a CHIS is envisioned there should be sufficient resources dedicated to the oversight and management of the operation. The Council is only likely to use a CHIS in very exceptional circumstances.
- 6.6 The CHIS will be the person who establishes or maintains the relationship as set out in paragraph 6.2 above.
- The provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the Council that is within their personal knowledge, without being induced, asked or tasked by the Council. Therefore, the public can continue to provide information as part of their normal civic duties, or to contact numbers set up by the Council to receive information.
 - However, a member of the public providing information **may** be a CHIS if their information is obtained in the course of, or as a consequence of, the existence of a personal or other relationship and they covertly pass that information to the Council. For example, where a member of the public gives repeat information about a suspect and it becomes apparent that the member of the public may be obtaining that information in the course of a family or neighbourhood relationship, it should be considered by the Investigating Officer whether that person is in reality a CHIS.
 - This is known as a “status drift”. The Council accordingly needs to be alert to the fact that a public informant may in reality be a CHIS even if not tasked to obtain information covertly.
 - Where such a “status drift” occurs, advice must be sought from Legal Services before any information received from this member of the public is relied on.

6.7 Examples

6.7.1 The following **will not** be a CHIS:

- A member of the public volunteers a piece of information to the Council regarding something he has witnessed in his neighbourhood. He will not be a CHIS as he is not passing on information as a result of a relationship which has been established or maintained for a covert purpose.
- A person complains about excessive noise coming from their neighbour’s house and the Council ask them to keep a noise diary. They will not be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose.

6.7.2 The following **will** be a CHIS:

- Intelligence received by the Council suggests that a local public house will sell alcohol to minors if they are familiar with them. A person under the age of 18 is engaged and trained by the Council and deployed to attend the licensed premises on a number of occasions and then try and purchase alcohol. In this situation a relationship has been established and maintained for the covert purpose and therefore a CHIS authorisation will be required.
- Without being asked, a person provides regular information to the Council about their neighbours' working hours and income as they believe their neighbour is committing benefit fraud. The person regularly visits their neighbour and engages in conversations about their work for the purpose of obtaining this information and passing it to the Council.

6.8 If a CHIS is used, both the use of the CHIS and their conduct require prior authorisation.

- **Conduct** is establishing or maintaining a personal or other relationship with a person for the covert purpose of (or incidental to) obtaining and passing on information.
- **Use** includes actions inducing, asking or assisting a person to act as a CHIS.

6.9 The Investigating Officer should apply for such authorisation as soon as the conduct or use of a CHIS is contemplated (see paragraphs 8,9 & 10 below, regarding authorisations and applications).

6.10 Handling and Controlling the CHIS

6.10.1 If an authorisation is provided the Investigating Officer must ensure that they are aware of the extent and limits of what the CHIS is allowed to do and make sure that the CHIS is advised of this.

6.10.2 The Investigating Officer will be responsible for the day to day handling of the CHIS (they will be the "handler"). This will involve dealing with the CHIS on behalf of the Council, directing the day to day activities of the CHIS, recording information supplied by the CHIS and monitoring the CHIS's security and welfare.

6.10.3 The safety and welfare of a CHIS both during the operation and after the authorisation has been cancelled should be taken into account by the investigating officer. Every application for authorisation should therefore include a detailed risk assessment of the risk to the CHIS and the likely consequences should the role of the CHIS become known.

6.10.4 The line manager of the "handler" will be the CHIS "controller" and they will be responsible for the management and supervision of the "handler" and the general oversight of the use of the CHIS.

6.10.5 A record must also be made of the use made of the CHIS (see paragraph 17 below for the information which must be held in the Central Log).

6.11 **Records**

Records of relevant documentation relating to every CHIS should be kept for a period of at least five years in accordance with paragraph 17 of this Policy.

6.12 **Special considerations**

6.12.1 Special care should be taken where the use of CHIS may involve confidential information (see paragraphs 2.1 & 11).

6.12.2 Special safeguards should be put in place where the CHIS is under the age of 18. A child under the age of 16 may not be authorised to give information against his parents. The Regulation of Investigatory Powers (Juveniles) Order 2000 contains the special provisions which should be followed where the CHIS is a minor. In such cases the only Authorising Officer is the Chief Executive (or in his absence an Executive Head).

6.12.3 Special safeguards should also be used where the CHIS is a vulnerable individual. A vulnerable individual is defined by the Code of Practice as “a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.” The use of a vulnerable individual is only permitted in exceptional circumstances. In such cases the only Authorising Officer is the Chief Executive (or in his absence an Executive Head).

7 ONLINE COVERT ACTIVITY

- 7.1 The extent of the information that is now available online, presents new opportunities to view or gather information which may assist in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public.
- 7.2 It is important that the Council is able to make full and lawful use of this information for its statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered.
- 7.3 The use of the internet (including social and business networking sites) may be required to gather information prior to and/or during an operation (including a CHIS operation). This may amount to directed surveillance.
- 7.4 In addition, a CHIS may communicate online.
- 7.5 Even if something is posted on a publicly-accessible networking site, it may still be private information. Where the use of the internet is intended as part of an investigation, the investigating officer must consider whether the proposed activity is likely to interfere with a person's Article 8 right to private and family life. The potential for collateral intrusion should also be considered. Such activity should only be contemplated if it is necessary and proportionate to the specific operation. If private information is likely to be obtained a directed surveillance authorisation must be obtained.
- 7.6 Advice should be sought from Legal Services on the use of the internet as part of an investigation.

8 AUTHORISATIONS, RENEWALS, REVIEWS AND CANCELLATIONS

- 8.1 Prior authorisation is required for the use of **directed surveillance** or the **conduct or use of a CHIS**.
- 8.2 **Procedure for Authorisations**
- 8.2.1 Each officer who undertakes investigations on behalf of the Council must seek authorisation in **writing** for any directed surveillance or the conduct and use of a CHIS.
- 8.2.2 A full list of Authorising Officers, is shown at **Appendix 1**. Authorising Officers **must not** delegate their powers under RIPA.
- 8.2.3 A checklist for the respective duties of the Investigating Officer and the Authorising Officer is set out in **Appendix 2**. Further detail is provided on some of these duties in this Policy.

- 8.2.4 All applications for authorisations should be made on the applicable standard form (See paragraph 9).
- 8.2.5 The Authorising Officer must describe explicitly in the authorisation what is being authorised. This should be in the Authorising Officer's own words rather than merely by reference to the terms of the application.
- 8.2.6 The Authorising Officer may add a proposed activity to the application if it is deemed necessary, and the Authorising Officer may authorise only some of what is being requested by the Investigating Officer. Where only part of the application is being authorised, the Authorising Officer should state the reason for this decision.
- 8.2.7 Authorising Officers should not normally be responsible for authorising operations in which they are directly involved as the Authorising Officer should be independent of the investigations. Where this is unavoidable this must be highlighted on the authorisation.
- 8.2.8 Every authorisation must state the rank of the person providing it.

8.3 Authorisations Requiring Judicial Approval

- 8.3.1 Since **1 November 2012**, where an authorisation has been granted for directed surveillance or the conduct or use of a CHIS, that authorisation shall not have effect until it has been **approved** by a justice of the peace at the local Magistrates Court. **No directed surveillance or the use of a CHIS can take place until this approval has been obtained.**
- 8.3.2 Legal Services should be instructed to prepare the application to the justice of the peace.

8.4 Duration

- 8.4.1 The time limit for a standard **written** authorisation for directed surveillance is 3 months from the day of the authorisation.
- 8.4.2 The time limit for a standard **written** authorisation for a CHIS is 12 months from the day of the authorisation.
- 8.4.3 It should be noted that even if an authorisation is only required for a limited time, it must still be for the statutory periods outlined above. However, the authorisation can be reviewed and/or cancelled if it is no longer necessary and proportionate.
- 8.4.4 No further operations can be carried out after the expiry of the relevant authorisation unless it has been renewed.
- 8.4.5 It will be the responsibility of the Investigating Officer to ensure that direct surveillance or the conduct or use a CHIS is only undertaken under an appropriate and valid authorisation. It will be the Investigating Officer's responsibility to diarise when the authorisation expires.

8.5 Reviews

- 8.5.1 The Authorising Officer will be responsible for reviewing each authorisation at regular intervals. The Authorising Officer shall determine how often a review should take place at the outset and each review should be conducted by the predetermined date. As a guide, reviews should take place on a monthly basis. However, the Authorising Officer may determine that they should take place more or less frequently (if so, the reasons should be recorded).
- 8.5.2 Reviews should take place as often as necessary and practicable and this will need to be determined on a case by case basis. More frequent reviews should take place where surveillance results in collateral intrusion or access to confidential information. (see paragraphs 2.1, 2.2 & 11).
- 8.5.3 Reviews should also be held in response to changing circumstances and must take into account any subsequent action by the Council arising from the product of the surveillance, which may be in the form of the issue of notices, orders, or determinations by the Council, or the bringing of criminal or civil proceedings, or any other action.
- 8.5.4 It will be the responsibility of the Authorising Officer to diarise when reviews should be held.
- 8.5.5 All reviews should be recorded on the correct form (See paragraph 9).

8.6 Renewal

- 8.6.1 An authorisation may be renewed **before** it ceases to have effect if an Authorising Officer considers it necessary for the authorisation to continue. The renewal takes effect at the time at which the authorisation would have ceased to have effect. If necessary a renewal can be made more than once.
- 8.6.2 Before a renewal of an authorisation for the conduct or use of a CHIS the Authorising Officer must be satisfied that a review has taken place of:
- the use made of the source in the period since the grant or, as the case may be, latest renewal of the authorisation; and
 - the tasks given to the source during that period and the information obtained from the conduct or the use of the source.
- 8.6.3 Since **1 November 2012**, where renewal of an authorisation has been granted for directed surveillance or a CHIS that renewal shall not have effect until it has been **approved** by a justice of the peace at the local Magistrates Court.
- 8.6.4 Where the renewal relates to the conduct or use of a CHIS the Justice of the Peace will need to be satisfied that a review has taken place of the matters listed in paragraph 7.6.2.
- 8.6.5 All renewals must be made on the correct form. (See paragraph 9).

8.7 Cancellations

- 8.7.1 All authorisations must be cancelled **as soon as** they are no longer required.
- 8.7.2 Even if an authorisation has expired it will not lapse and should be formally cancelled.
- 8.7.3 The Authorising Officer who granted or last renewed the authorisation must cancel the authorisation if the grounds for granting the authorisation no longer apply e.g. the aims have been met; risks have changed and authorisation is no longer appropriate.
- 8.7.4 If the Authorising Officer is not available, this duty will fall on one of the other Authorising Officers.
- 8.7.5 When cancelling an authorisation, the Authorising Officer should (where applicable):
- Record the date and times (if at all) that surveillance took place, and that the order to cease the activity was made.
 - Record reason for the cancellation.
 - Ensure that surveillance equipment has been removed and returned.
 - Provide directions for the management of the material obtained as a result of the investigation.
 - Ensure that the detail of persons subjected to surveillance since the last review or renewal is properly recorded.
 - Record the value of the surveillance and interference (i.e. whether the objectives as set out in the authorisation were met.)
- 8.7.6 Authorisations may be cancelled orally. When and by whom this was done should be endorsed on the cancellation form when it is completed and recorded on the central record of authorisations. However, best practice will be for the authorisation to be cancelled in writing.
- 8.7.7 The Authorising Officer should also advise those involved in the surveillance or the CHIS to stop their actions with immediate effect.
- 8.7.8 Where necessary, when cancelling the use of a CHIS, the Authorising Officer should consider the safety and welfare of the CHIS, and should satisfy themselves that all safety and welfare matters are addressed.
- 8.7.9 All cancellations must be completed on the correct form (See paragraph 9).

9 APPLICATION FORMS

- 9.1 The standard forms can be found at <https://www.gov.uk/government/collections/ripa-forms--2>
- 9.2 The person completing the form is responsible for ensuring that the form used is the most up-to-date version issued by the Government.
- 9.3 The forms for applications, renewals, reviews and cancellations should be completed in as much detail as possible.

- 9.4 For guidance on what should be included in the application for authorisation the Investigating Officer should refer to paragraph 5.6 of the 2018 Covert Surveillance and Property Interference Revised Code of Practice (for direct surveillance) or paragraph 5.11 in the 2018 Covert Human Intelligence Sources Revised Code of Practice (for CHIS).
- 9.5 Each investigation or operation should be given a unique reference number (“URN”) on the application form by the Legal Services Manager. Any reviews, renewals or cancellation forms should be identified by the same URN.
- 9.6 The URN should be obtained from the Legal Services Manager (see paragraph 18).
- 9.7 Any application (or other) form which is not completed in full will be rejected by the Authorising Officer.
- 9.8 The role of the Investigating Officer is to present the facts and evidence to the Authorising Officer. They must also set out in detail why they consider the directed surveillance/use of a CHIS to be **necessary** and **proportionate** (see paragraph 10). The application should include consideration of any potential collateral intrusion (see paragraph 2.2) and measures taken to limit this. The application must state whether the Investigating Officer expects the investigation to result in the obtaining of confidential information (see paragraphs 2.1 & 11).
- 9.9 Having reviewed the application, the Authorising Officer must decide whether they consider the activities applied for are **necessary** and **proportionate** (see paragraph 10). If so, they should decide whether to authorise some or all of the activities applied for. If they decide to authorise the application, they must record in detail the reasons that they have reached this decision, including the reasons that they have concluded the activities are necessary and proportionate.

10 THE NECESSITY AND PROPORTIONALITY TEST

- 10.1 No directed surveillance or use of a CHIS can be authorised under RIPA unless it can be demonstrated that it is necessary and proportionate.
- 10.2 The Authorising Officer must be satisfied that the proposed surveillance is **necessary and proportionate**.
- 10.3 **Necessary**
- 10.3.1 The use of the directed surveillance or conduct and use of a CHIS must be **necessary** for the **purpose of preventing or detecting crime or of preventing disorder**.
- 10.3.2 In order for the Authorising Officer to be satisfied that the surveillance is necessary, the Investigating Officer must clearly identify in the application the conduct that it is aimed to prevent or detect, and an explanation of why covert techniques are required.
- 10.4 **Proportionate**

- 10.4.1 The intrusion into the private and family life of the subject of the operation must be **balanced** against what the activity seeks to achieve. The intrusion must not be excessive or arbitrary.
- 10.4.2 The authorisation should therefore demonstrate how the Authorising Officer reached the conclusion that the act is proportionate
- 10.4.3 The activities will not be proportionate if the activities are excessive in the circumstances of the case or if the information could be obtained by a less intrusive means.
- 10.4.4 The following elements of proportionality must be considered by the Authorising Officer and should be addressed in the authorisation:
- 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 conduct to be authorised will have any implications for the privacy of others, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation

 - 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.
- 10.4.5 When authorising a CHIS, the Authorising Officer must also:
- be satisfied that the conduct and/or use of the CHIS is proportionate to the objective sought to be achieved;
 - be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS. These arrangements must address health and safety issues by the carrying out of a formal and recorded risk assessment;
 - consider the likely degree of intrusion for all those potentially affected;
 - consider any adverse impact on community confidence that may result from the use or conduct of the CHIS or the information obtained; and
 - ensure that records contain the required particulars of the CHIS and that these are not available except on a 'need to know' basis.

10.4.6 Risk of Collateral Intrusion

The Authorising Officer should consider the likely effect of the use of the direct surveillance or the conduct and use of a CHIS on the private and family life of persons who are not the intended subjects of the activity. The Authorising Officer must consider the risk of collateral intrusion and have a plan for managing any such risk.

If the impact on other persons cannot be avoided altogether, then any collateral intrusion must be proportionate.

The person carrying out the surveillance must inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals not covered by the authorisation. The Authorising Officer must then consider whether the authorisation ought to continue or whether a new authorisation is required.

11 CONFIDENTIAL MATERIAL

- 11.1 Particular care should be taken where the subject of the investigation or operation might reasonably expect a high degree of privacy and where it is envisaged that the investigation may cause the Council to come into possession of Confidential Information (see definition at paragraph 2.1). In these cases, the surveillance can only be authorised by the Chief Executive (or in his absence an Executive Head). Applications which are calculated to obtain confidential information will only be authorised in very exceptional and compelling circumstances.
- 11.2 Where an Investigating Officer comes into possession of confidential material during the course of an investigation, s/he should seek legal advice from a member of the Council's Legal Services before taking any action in connection with that material.
- 11.3 Where it is envisaged that surveillance may cause the Council to come into possession of material which is subject to legal privilege, the Investigating Officer must seek legal advice from a member of the Council's Legal Services Section before the application for authorisation is made.

12 ACTIVITIES BY OTHER PUBLIC AUTHORITIES

The Investigating Officer must make enquiries of other public authorities whether they are carrying out similar activities, if he considers that there is such a possibility, in order to ensure that there is no conflict between the activities of the Council and those other public authorities.

13 JOINT INVESTIGATIONS

- 13.1 From time to time, Council officers may carry out investigations with officers from another public authority, for example:
- The police;
 - The Department of Work and Pensions;

- The Environment Agency;
- The Food Standards Agency; or
- The Health and Safety Executive

13.2 Where one authority is acting on behalf of another, the tasking authority should normally obtain the RIPA authorisation. If an authorisation has been obtained by another agency, who wish the Council to carry out surveillance in accordance with that authorisation, an Authorising Officer must view that authorisation to ensure that Council officers, and the activities which they are being asked to carry out, are covered by that authorisation.

14 DATA PROTECTION

Private information collected as a result of surveillance may include personal data. It is the responsibility of the Authorising Officer to ensure that personal data is processed (including handling, dissemination, storage, retention and destruction) in accordance with the General Data Protection Regulation, the Data Protection Act 2018 and the Council's Data Protection Policy, Law Enforcement (Data Protection) Policy and the Protection of Special Category Data Policy.

15 DESTRUCTION OF WHOLLY UNRELATED MATERIAL

15.1 Surveillance may result in officers obtaining the following categories of material:

- i. material which is wholly unrelated to the investigation (for example, information about persons who are not the subject of the surveillance, and have no relevant involvement with the subject of the surveillance);
- ii. material regarding the subject(s) of the surveillance, which is unlikely to be used in connection with the investigation or any subsequent proceedings;
- iii. material which is relevant to the investigation, and may be used in connection with subsequent proceedings

15.2 Material which is **wholly unrelated** to the investigation (category i. above) should be destroyed promptly and securely. As the material will have been collected in connection with the investigation of a criminal offence, advice should be sought from the Council's Legal Services section prior to the destruction of evidence.

15.3 All other material should be retained until the investigation is concluded and a decision is taken regarding what action, if any, will be taken in connection with the investigation. At that stage, the Authorising Officer will determine which materials are to be retained, and for how long.

15.4 Where criminal proceedings are contemplated, all material (save for wholly unrelated material) is potentially relevant. It must therefore be retained and will be disclosable in those proceedings.

16 TRAINING

- 16.1 Each officer of the Council with responsibilities for the conduct of an investigation, operation or authorisation under RIPA, will undertake training every three years to ensure that any such investigations, operations and authorisations undertaken are conducted according to the statutory requirements and the Codes of Practice. However, where a RIPA investigation is contemplated, the relevant officers are required to contact Legal Services in advance so an update training session can be provided.
- 16.2 Each officer who undertakes training in connection with their responsibilities under RIPA must keep a personal training record, and must send a copy of this training record every two years to the Legal Services Manager.

17 RECORDS OF AUTHORISATIONS

- 17.1 A centrally retrievable record of all authorisations will be held by the Legal Services Manager. This will contain the following information:
- the type of authorisation
 - the URN
 - the dates that the authorisation was granted, reviewed, renewed or cancelled.
 - details of attendances at the Magistrates' Court to include date of attendances, the determining Magistrate, the decision of the Court and the time and date of that decision.
 - the name and rank of the Authorising Officer for the initial authorisation and any reviews, renewals or cancellations.
 - whether the Authorising Officer is involved in the investigation.
 - the file reference for the investigation.
 - whether the authorisation was likely to result in the obtaining of confidential material.
- 17.2 This centrally retrievable record will be stored in a manner which is confidential and secure. It will be retained for a period of at least **three years** from the date of cancellation of the authorisation for directed surveillance, and at least **five years** from the date of cancellation of the authorisation of a CHIS.
- 17.3 In addition, the Legal Services Manager will keep the following documents, where applicable, for a period of at least **three years** from the date of cancellation of the authorisation for directed surveillance, and at least **five years** from the date of cancellation of the authorisation of a CHIS:
- The application, authorisation, reviews, renewals, cancellations and the approval from the Magistrates Court.
 - The frequency of the reviews prescribed by the authorising officer.

- The date and time when any instruction to cease directed surveillance or use of a CHIS was given.
- The date and time when any other instruction was given by an Authorising Officer.

17.4 In relation to the use of a CHIS the Legal Services Manager will also maintain the following documents:

- Any risk assessment in relation to the CHIS.
- The circumstances in which tasks were given to the CHIS.
- The value of the CHIS to the Council.

17.5 Investigating Officers and Authorising Officers may keep copies of relevant documentation but any such copies should be stored in a manner which is confidential and secure.

18 MONITORING

18.1 The Legal Services Manager will have responsibility for overseeing the authorising process to ensure good quality control of RIPA and will be referred to as the Legal Services Manager for the purposes of this Policy (see **Appendix 3**).

18.2 The Legal Services Manager will be responsible, along with the Senior Responsible Officer, for ensuring corporate awareness of RIPA.

18.3 The Legal Services Manager will be responsible for issuing each application with a URN.

18.4 All completed RIPA forms; applications (whether granted or refused), authorisations, reviews, renewals and cancellations, and approvals from the Magistrates' Court should be forwarded to the Legal Services Manager within **five working days** of the relevant decision. The Legal Services Manager will hold these documents securely.

18.5 The Legal Services Manager will also be responsible for the day to day management of the authorising process, and any initial queries from Investigating Officers or Authorising Officers should be addressed to the Legal Services Section.

18.6 Adherence to the requirements of RIPA, the Codes of Practice and this Policy should reduce the scope for making errors. The Legal Services Manager will conduct a regular review of errors and a record must be made of each review.

19 SENIOR RESPONSIBLE OFFICER

- 19.1 The Senior Responsible Officer will be the Chief Executive (see **Appendix 3**).
- 19.2 The Senior Responsible Officer will be responsible for the following:
- The integrity of the process in place within the Council for the management of CHIS and Directed Surveillance.
 - Compliance with RIPA and with the Codes of Practice.
 - Ensuring all Authorising Officers are of an appropriate standard.
 - Oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors.
 - Engagement with the Investigatory Powers Commissioner's Office (IPCO) inspectors when they conduct their inspections, where applicable.
 - Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

20 POLICY AND IMPLEMENTATION

- 20.1 The Policy is operational from **15 January 2019** and replaces any previous policies and procedures relating to surveillance.
- 20.2 The Legal Services Manager will report every two years to the Audit Committee regarding the use made by the Council of its powers under RIPA, unless RIPA powers have been used in the first of the two years, in which case a report will be taken to the first Audit Committee following use of the powers.
- 20.3 The Audit Committee will review the Council's Surveillance Policy every two years.

21 APPENDICES

Appendix 1 – Functions that may be undertaken by Authorising Officers

Appendix 2 - Application and Authorisation Checklist

Appendix 3 – Monitoring and Senior Responsible Officers

APPENDIX 1

FUNCTIONS THAT MAY BE UNDERTAKEN BY AUTHORISING OFFICERS:

1. Authorise an **application** for authority to carry out directed surveillance or for the conduct or the use of a CHIS.
2. **Review** an authorisation to carry out directed surveillance or the conduct or use of a CHIS on or before the specified date.
3. Authorise **renewal** of an application for authority to carry out directed surveillance or for the conduct or use of a CHIS.
4. Authorise **cancellation** of an application for authority to carry out directed surveillance or for the conduct or use of a CHIS.
5. Authorise **destruction** of wholly unrelated material arising from surveillance or from the conduct or use of a CHIS, with advice from the Legal Services Section where appropriate.
6. **Monitor** the produce of the surveillance or from the conduct or use of a CHIS.
7. Authorise an application where the likely consequence of directed surveillance or conduct or use of a CHIS would be intrusion on another person other than the target (**collateral intrusion**).
8. Authorise an application where the likely consequence of the directed surveillance or conduct or use of a CHIS would result in Council obtaining **confidential material**.
9. Authorise the use of a CHIS who is a minor.
10. Authorise the use of a CHIS who is a vulnerable person.

RANK/TITLE	AUTHORISED FUNCTIONS
Chief Executive	1-10
Executive Heads	1-7 (8,9,10 in Chief Executive's absence)
Service Managers for: Planning Environmental and Regulation Street Scene Revenue and Benefits Housing Estates Management & Support.	1-7

APPLICATION AND AUTHORISATION CHECKLIST

Investigating Officer must:

Read the Surveillance Policy document and be aware of any other relevant guidance.	
Determine that directed surveillance and/or a CHIS is required.	
For directed surveillance , assess whether the authorisation will be in accordance with Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 and be able to demonstrate that the suspected offence is subject to a custodial sentence of 6 months or more or that the surveillance is in connection with the sale of alcohol or tobacco to children (see paragraph 3.4 of this Policy).	
Assess whether authorisation is necessary under RIPA and whether the surveillance could be done overtly.	
Consider whether surveillance will be proportionate.	
Consider all less intrusive options which may be available and practicable and use that option first.	
If authorisation is necessary and proportionate , request a URN from the Legal Services Manager, prepare and submit an application to carry out directed surveillance or conduct or use of a CHIS to an Authorising Officer.	
REVIEW REGULARLY and submit to Authorising Officer on date set.	
If operation is no longer necessary or proportionate, complete cancellation form and submit to Authorising Officer.	

Authorising Officer must:

Consider in detail whether all options have been duly considered, including taking into account the Surveillance Policy document and any other relevant guidance.	
---	--

For directed surveillance, confirm that the offence is subject to a custodial sentence of 6 months or more or the surveillance is in connection with the sale of alcohol or tobacco to children (see paragraph 3.4 of this Policy).	
Consider whether surveillance can be considered to be in accordance with the law and is necessary and proportionate to the offence being investigated.	
Authorise only if an overt or less intrusive option is not practicable.	
Ensure the relevant judicial authority has made an order approving the grant of the authorisation.	
If surveillance is necessary and proportionate: <ul style="list-style-type: none"> • Review authorisation • Set review timetable (at least monthly) 	
Cancel authorisation when it is no longer necessary or proportionate.	

ESSENTIAL:

- Officers must use the correct RIPA forms (which can be found on the Home Office website www.homeoffice.gov.uk).
- A URN must be obtained from the Legal Services Manager before submitting an application for authorisation.
- Once authorised, approval must be obtained from a Magistrates Court before any surveillance commences.
- All RIPA application forms (whether authorised or rejected) must be sent to the Legal Services Manager **within 5 working days**. This must include reviews, renewals and cancellations
- If in any doubt, seek advice from the Legal Services Manager or the Senior Responsible Officer **before** any directed surveillance and/or CHIS is authorised, renewed, cancelled, or rejected.

MONITORING AND SENIOR RESPONSIBLE OFFICERS

Name	Job Title	RIPA Role
Bob Jackson	Chief Executive	Senior Responsible Officer
Andrew Kinghorn	Legal Services Manager	Monitoring

This page is intentionally left blank



POLICY FOR THE ACQUISITION OF COMMUNICATIONS DATA

Human Rights Act 1998,

Regulation of Investigatory Powers Act 2000

Protection of Freedoms Act 2012

Investigatory Powers Act 2016

THIS POLICY MUST BE READ IN CONJUNCTION WITH THE CURRENT HOME OFFICE CODE OF PRACTICE: "ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA".

CONTENTS	Page
1. Background.....	3
2. National Anti-Fraud Network.....	4
3. What types of data can be acquired?.....	4
4. Authorisations and Notices.....	5
5. Different Roles:.....	5
Applicant	
Single Point of Contact (SPoC)	
Designated Peron	
Senior Responsible Officer	
6. Necessity and Proportionality.....	7
7. Applications and Authorisations:.....	7
Application form	
SPoC Review	
Authorisation by Designated Person	
8. Judicial Approval.....	9
9. Data Protection and Handling the data acquired.....	10
10. Duration, renewal and cancellation.....	10
11. Record keeping.....	12
12. Errors.....	12
13. Policy and Implementation.....	12

1 BACKGROUND

- 1.1 When the Human Rights Act 1998 came into force in 2000 it made the fundamental rights and freedoms contained in the European Convention on Human Rights enforceable in UK Courts and Tribunals.
- 1.2 Article 8 of the Convention reads as follows: -

“Everyone has the right to respect for his private and family life his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of public safety, for the protection of order, health or morals, or for the rights and freedoms of others.”
- 1.3 Investigating Officers of the Council may, from time to time, engage in activities which interfere with a person’s right under Article 8 of the Convention to respect for their private and family life. Such interference is only permissible where it complies with the exceptions set out in Article 8.
- 1.4 The Regulation of Investigatory Powers Act 2000 (“RIPA”) provides a statutory framework whereby certain investigations can be carried out in a lawful, regulated and proportionate manner so that an individual’s Article 8 rights are not infringed.
- 1.5 This Policy is concerned with the provision in RIPA enabling certain communications data to be acquired by public authorities in a manner which is compatible with Article 8. This Policy sets out the relevant responsibilities of the Council and its officers, and is designed to ensure that any acquisition of communications data is conducted in a manner that will comply with the safeguards embodied in the Human Rights Act 1998 and RIPA. (The Council has a separate Surveillance Policy which deals with Directed Surveillance and Covert Human Intelligence Sources).
- 1.6 The acquisition of communications data can **only** be authorised by the Council under RIPA where the use of the surveillance is necessary for the **prevention or detection of crime** or for the **prevention of disorder**.
- 1.7 All officers who apply for communications data to be obtained or disclosed should be familiar with RIPA, this Policy, and the Home Office “Code of Practice for the Acquisition and Disclosure of Communications Data” which can be found at <https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and-disclosure-of-communications-data>.
- 1.8 Acquiring communications data without authorisation or outside the scope of an authorisation will mean that the “protective umbrella” of RIPA is unavailable, and could expose the Council to the risk of legal action. It may also result in disciplinary action being taken against the officer/officers involved.

2 NATIONAL ANTI-FRAUD NETWORK

- 2.1 The Council uses the National Anti-Fraud Network (“NAFN”) to deal with all applications for the acquisition of communications data. The application process, and NAFN’s role in this process, is detailed below under “Applications and Authorisations”.
- 2.2 NAFN provides a service whereby all applications are checked by an accredited individual (a “Single Point of Contact” or “SPoC”) to ensure compliance with RIPA. NAFN has direct access to the databases of a number of Communications Service Providers (“CSPs”). This means that if an authorisation is granted to allow a person to engage in conduct required to obtain communications data (see paragraph 4.1.1 below), and NAFN has access to the database of the relevant CSP, the NAFN SPoC will be able to obtain that data directly.
- 2.3 In order to access the NAFN secure website to make an application for communications data, an Applicant will require a username, password and PIN.
- 2.4 Should a manager consider that it is necessary for a Council employee to use the NAFN secure website to make applications for communications data, this must be authorised in writing by the employee’s Service Manager. Where the Service Manager has provided their authorisation, the manager should notify NAFN of the details of the employee who requires log in details for the system.

3 WHAT TYPES OF DATA CAN BE ACQUIRED?

- 3.1 “Communications data” is generated, held or obtained by CSPs and may relate to use of the following services:-
 - 3.1.1 Postal service
 - 3.1.2 Email
 - 3.1.3 Landline telephone
 - 3.1.4 Mobile telephone
 - 3.1.5 Internet
- 3.2 Local authorities may **NOT** acquire any information about the content of communications (eg, what was said, or what data was passed on), or the location of a mobile device used to make a call.
- 3.3 Local authorities may acquire communications data of the following types: -
 - 3.3.1 **‘Service use information’**. This is information about the services provided to an individual. It will include information about:
 - a) the use made by any person of any postal service or communications service;

- b) the use made by any person of any part of a telecommunications system, in connection with the provision to or use of any telecommunications service.

Service information might include, for example, information regarding itemised billing (numbers called, timing and duration of service usage), use of call diversions/forwarding, itemised records of connections to internet services, information about amounts of data downloaded or uploaded, information about selection of preferential numbers or discount calls, records of registered post and parcel consignment.

- 3.3.2 **'Subscriber information'**. This is information about the person who uses a service. It will include any information held by the provider of a postal or telecommunications service, regarding the persons to whom they provide the service.

This might include subscriber details, including names, addresses and other customer information, for example, the identity of the subscriber to telephone number 01234 567891, or email address example@example.co.uk, or who is entitled to post to web space www.example.co.uk.

- 3.4 The above examples are not exhaustive lists of the communications data which may be acquired. If officers are in any doubt about the types of data which they may be able to acquire, or the ways in which this might be acquired, they should seek advice from a SPoC (see paragraph 5.3 below).
- 3.5 Applicants and Designated Persons (see paragraph 5.4 below) should bear in mind that it may be appropriate to obtain subscriber information (ie, to check that the person who subscribes to a service is a person relating to their investigation) before they can determine whether it is necessary and proportionate to go on to acquire service use information, such as itemised billing.

4 AUTHORISATIONS AND NOTICES

- 4.1 Communications data can be acquired in two ways: by Authorisation or by Notice:
 - 4.1.1 An Authorisation enables the authorised person (generally the SPoC) to engage in conduct required to obtain the communications data;
 - 4.1.2 A Notice requires a CSP to disclose the data in their possession, or to obtain and disclose the data.
- 4.2 The SPoC will be able to advise which of these methods will be most appropriate in relation to a particular investigation. In the majority of cases, the Council will use an Authorisation, authorising the SPoC to obtain the data required from the relevant CSP.

5 DIFFERENT ROLES

- 5.1 There are four key roles relevant to the acquisition of communications data:

- Applicant
- Single Point of Contact (SPoC)
- Designated Person
- Senior Responsible Officer

5.2 Applicant

The Applicant will generally be the investigating officer, who will complete the application form, setting out for consideration by the Designated Person the necessity and proportionality of acquiring the communications data.

5.3 Single point of contact

A SPoC must have formal accreditation, and is trained to facilitate the lawful acquisition of communications data and effective cooperation between a public authority and CSPs. In this way, the SPoC provides a “guardian and gatekeeper” function. The SPoC provides objective judgement and advice to both the Applicant and Designated Person.

The Council does not have an internal Single Point of Contact (SPoC), but uses the SPoCs at NAFN, who hold the necessary accreditation.

5.4 Designated Person

The Designated Person is the person within the Council who reviews the application and authorises the grant of an Authorisation, or the giving of a Notice, where they consider the acquisition to be necessary and proportionate.

Designated Persons must be independent from the operation or investigation to which the application relates, ie, they should have had no prior involvement with the operation or investigation. If the Designated Person is an Executive Head, they should not authorise applications from within their own Services.

In an exceptional, urgent situation (for example, if there is an immediate threat to life, or an urgent operational requirement for the prevention or detection of serious crime), if there is no independent Designated Person available, the involvement of a non-independent Designated Person must be recorded, and the justification for their involvement explained in their recorded considerations. The involvement of a non-independent Designated Person must be reported to the Commissioner at their next inspection, and the details and reasons may be published by the Commissioner.

The Council’s Designated Persons are currently the Chief Executive and Executive Heads.

5.5 Senior Responsible Officer

The Senior Responsible Officer is responsible for: -

- 5.5.1 Ensuring the integrity of the processes in place within the authority to acquire communications data;

- 5.5.2 Ensuring compliance with RIPA and with the Code of Practice;
- 5.5.3 Oversight of the reporting of errors to the Investigatory Powers Commissioner's Office (IPCO), the identification of the reasons for the errors, and the implementation of processes to minimise repetition of errors;
- 5.5.4 Engagement with IPCO inspectors, and oversight of the implementation of any post-inspection plans.

The Council's Senior Responsible Officer is currently the Chief Executive.

6 NECESSITY AND PROPORTIONALITY

The obtaining or disclosure of communications data (by Authorisation or Notice) should only be authorised if the Designated Person is satisfied that:

- 6.1 The action is **NECESSARY** for the prevention or detection of crime or the prevention of disorder. An application should cover three main points, and should demonstrate the link between these three aspects:

- The event under investigation (ie, the crime or disorder);
- the person (eg, the suspect) and how they are linked to the event; and
- the communications data, and how this relates to the person and the event.

- 6.2 The action is **PROPORTIONATE**. It should: -

- 6.2.1 be no more than is required in the circumstances;
- 6.2.2 impinge as little as possible on the rights and freedoms of the individual concerned and of innocent third parties;
- 6.2.3 be carefully designed to meet the objectives in question;
- 6.2.4 not be arbitrary, unfair or based on irrational considerations.

7 APPLICATIONS AND AUTHORISATIONS

7.1 APPLICATION FORM

- 7.1.1 The Applicant must complete the NAFN application form, which is a standard form approved by the Home Office. As the Council uses the NAFN application process, the Applicant will access the application form by logging onto the NAFN website using their username, password and PIN.
- 7.1.2 The Applicant should have reference to the Home Office document: "Acquisition and Disclosure of Communications Data; Guidance for the Layout

of a Chapter II Application Form and Guidance for Applicants and Designated Persons Considering Necessity and Proportionality”.

7.1.3 The application form must include the following information: -

- i) name, rank and position of the Applicant;
- ii) a unique reference number (which will be generated automatically by the NAFN website);
- iii) the operation name, if applicable;
- iv) specify that the communications data is required in connection with the purpose of **preventing or detecting crime or disorder**;
- v) describe the communications data required, specifying the time periods for which the data is sought, including (where relevant) any historic or future dates. Any time period specified should be the shortest period in which the objective for which the data is sought can be achieved;
- vi) describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- vii) explain why the acquisition of the communications data is **necessary** and **proportionate** (see paragraph 6 above);
- viii) consider and, where appropriate, describe any collateral intrusion (ie, explain the extent to which the privacy of an individual not under investigation may be infringed, and why that infringement is justified in the circumstances);
- ix) consider and, where appropriate, describe any potential unintended consequences of the application;
- x) identify and explain the timescale within which the data is required.

7.2 SPoC REVIEW

- 7.2.1 Once the Applicant has completed the application form, this must be submitted electronically to the SPoC, who will check that the application is compliant with RIPA, that the acquisition intended is practical and lawful, and that the tests of proportionality and necessity have been properly considered and detailed.
- 7.2.2 If the SPoC considers that there are any problems with the application, or that further information is required, he will provide advice to the Applicant about the application. This may include, for example, advice about whether it is lawful, possible, or practical to obtain communications data of the nature sought by the applicant, and whether the tests of necessity and proportionality have been properly applied and explained. Where appropriate, the Applicant can make amendments to the application, and can re-submit the application to the SPoC.

- 7.2.3 Once the SPoC is satisfied with the application, he will complete the relevant sections of the application form, identifying the data to be acquired, and how it may be acquired. The SPoC will then notify the Designated Persons at the Council by email that there is an application pending which requires review.

7.3 AUTHORISATION BY DESIGNATED PERSON

- 7.3.1 The Designated Person must review the application in detail, before deciding whether to: -

- a) authorise the application;
- b) reject the application;
- c) request further information.

- 7.3.2 Before deciding whether to authorise an application, the Designated Person should have reference to the Home Office document: "Acquisition and Disclosure of Communications Data; Guidance for the Layout of a Chapter II Application Form and Guidance for Applicants and Designated Persons Considering Necessity and Proportionality".

- 7.3.3 The Designated Person should consider the proportionality and necessity of the Authorisation/Notice applied for (see paragraph 6 above), and the potential for collateral intrusion. The Designated Person should not simply "rubber stamp" the application. Their reasons for authorising/declining the application should be clear and detailed, and demonstrate that they have considered the substantive merits of the application. If the Designated Person requires further information in order to decide whether to approve an application, they should notify the SPoC that more information is required.

- 7.3.4 The standard form requires the Designated Person to tick a box to confirm whether they are authorising a person to engage in conduct to acquire communications data, or whether they are authorising a Notice to be served on a CSP, requiring them to obtain/disclose data. The Notice or Authorisation documents themselves will be completed by the SPoC.

- 7.3.5 The authorised or rejected Application is then submitted back to the SPOC via the NAFN secure website.

8 JUDICIAL APPROVAL

- 8.1 From 1 November 2012 a person may not engage in the conduct authorised, or serve a Notice on a CSP requiring them to provide communications data, unless and until the Authorisation/Notice has been approved by a Justice of the Peace.

- 8.2 Before approving an Authorisation or Notice, a Justice of the Peace must be satisfied that: -

At the time of granting the Authorisation, or giving the Notice: -

- i) There were reasonable grounds for believing that the Authorisation/Notice was necessary and proportionate;

- ii) The person who granted the Authorisation/Notice was an appropriate Designated Person; and
- iii) At the time when the Justice of the Peace is considering the matter, there remain reasonable grounds for believing that the Authorisation/Notice is necessary and proportionate.

8.3 The procedure for obtaining judicial approval is as follows: -

- i) After the Designated Person has completed the authorisation on the NAFN secure website, NAFN will send an application pack to the Applicant;
- ii) The application pack should be forwarded to the Legal Services Manager;
- iii) A member of Legal Services will prepare the Magistrates' Court application, and will represent the Council at the Magistrates' Court hearing. The Applicant may be asked to prepare a witness statement and may be required to attend the hearing;
- iv) If the Authorisation/Notice is approved, Legal Services will pass the approval to the Applicant. The Applicant will then liaise with the SPoC who will obtain the communications data from the CSP.
- v) If the Authorisation/Notice is not approved, or is quashed by a Justice of the Peace, Legal Services will inform the Applicant. The Applicant must inform the SPOC and Designated Person that the Authorisation/Notice was not approved, or was quashed.

8.4 **No action may be taken under the Authorisation or Notice unless and until it has been approved by a Justice of the Peace.**

9 DATA PROTECTION AND HANDLING THE DATA ACQUIRED

- 9.1 When the communications data has been acquired, it will be made available to the Applicant on the NAFN secure website.
- 9.2 Information collected through acquisition of communications data may include personal data. It is the responsibility of the Applicant to ensure that personal data is processed (including handling, dissemination, storage, retention and destruction) in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and the Council's Data Protection Policy, Law Enforcement (Data Protection) Policy and the Protection of Special Category Data Policy . In particular, the information obtained must be handled and stored securely. Any queries regarding an officer's obligations under the Data Protection Act or the GDPR should be directed to the Council's Data Protection Officer. .

10 DURATION, RENEWAL AND CANCELLATION

Duration

- 10.1 All Authorisations and Notices should specify the time period in relation to which the communications data are to be obtained. For example, it might authorise the SPOC to obtain information regarding all calls made from a specified number to another specified number in the two weeks immediately following the Authorisation. Or a Notice might require a CSP to confirm the subscriber details for a specific email account between two specified dates in the past. An authorisation: -
- 10.1.1 Cannot authorise or require any data to be obtained more than one month after the Authorisation or Notice is granted; and
- 10.1.2 In the case of a Notice, cannot authorise or require any disclosure of data not already in the possession of the CSP after the end of one month from the date of the grant of the Notice or Authorisation.

Renewal

- 10.2 RIPA provides that an Authorisation or Notice may be renewed for a period of up to one month by the grant of a further Authorisation or the giving of a further Notice. A renewed Authorisation or Notice takes effect upon the expiry of the Authorisation or Notice it is renewing.
- 10.3 Where the Applicant believes that a renewal is necessary and proportionate, they should complete an addendum to the original application, setting out their reasons for seeking renewal. They should then submit this to the SPoC, who will review it in the same way as a new application. Once the SPoC is happy with the application for renewal, they will notify the Designated Person that an application requires review.
- 10.4 Where a Designated Person is granting a further Authorisation or giving a further Notice to renew an earlier Authorisation or Notice, they should: -
- 10.4.1 consider and record in writing the reasons that it is necessary and proportionate to continue with the acquisition of the data being generated; and
- 10.4.2 record the date (and where appropriate the time) when the Authorisation or Notice is renewed.
- 10.5 A renewal **must** be approved by a Justice of the Peace before it will take effect. Any renewal must therefore be submitted to the SPOC in plenty of time to enable it to be reviewed and forwarded to the Designated Person for approval, and for approval to be sought from a Justice of the Peace. Where a renewal has been approved by a Designated Person, Legal Services must be notified at least **seven** working days before expiry of the original Authorisation or Notice, so that they have sufficient time to seek approval from a Justice of the Peace.
- 10.6 In practice, given the requirement to obtain the approval of a Justice of the Peace and the time constraints this imposes, it will often be more practical to begin a new application, rather than to renew an existing Authorisation or Notice. Applicants who have not obtained, or do not expect to obtain, the data required within one month of grant of the Authorisation or Notice should discuss with the SPoC the best way to deal with this.

Cancellation

- 10.7 Where a Notice has been given to a CSP, and a Designated Person determines that it is no longer necessary or proportionate for the CSP to comply with the Notice, the Designated Person shall cancel the Notice,, and must ensure that the CSP is notified of the cancellation.
- 10.8 Where an Authorisation has been given and a Designated Person determines that it should cease to have effect because the conduct authorised is no longer necessary or proportionate, the Designated Person shall withdraw the Authorisation, and inform the person authorised by the Authorisation of the withdrawal.
- 10.9 The cancellation or withdrawal must: -
- 10.9.1 be in writing;
 - 10.9.2 identify, by reference to its unique reference number, the Notice or Authorisation being cancelled;
 - 10.9.3 record the date (and, where appropriate the time) when the Notice or Authorisation was cancelled;
 - 10.9.4 record the name, office and rank/position held by the Designated Person.
- 10.10 Normally, it will be the Applicant who realises that a Notice or Authorisation is no longer necessary or proportionate (for example, because they have obtained the information required from elsewhere, or because the investigation has concluded for some reason). In this situation, the Applicant should notify the SPoC immediately. The SPoC will then alert the Designated Person that the Authorisation or Notice should be cancelled. The Designated Person should log on to the NAFN secure website to cancel the Authorisation or Notice. Where necessary, the SPoC will notify the CSP that the Authorisation or Notice has been cancelled.
- 10.11 Where the Designated Person who authorised the Application is unavailable, one of the other Designated Persons should cancel or withdraw the Authorisation or Notice so that no undue delay is caused.

11 RECORD KEEPING

NAFN keeps a full, electronic record of all applications on the Council's behalf, in accordance with the requirements of RIPA.

12 ERRORS

- 12.1 Where an error occurs in the grant of an Authorisation, the giving of a Notice, or as a consequence of any authorised conduct, or conduct undertaken to comply with a Notice, a record must be kept.
- 12.2 There are two types of error: -
- i) an error which results in communications data being wrongly acquired or disclosed. This type of error is known as a "Reportable Error".
 - ii) an error which is identified after the Authorisation or Notice is given, but without data being wrongly obtained or disclosed. This type of error is known as a "Recordable Error".

- 12.3 If an Applicant or Designated Person identifies a Reportable or Recordable Error, they must notify the SPoC immediately.
- 12.4 A Reportable Error must be reported to the IPCO. This report will be made by the SPoC at NAFN. It is **essential** that the Council's Senior Responsible Officer and the SPoC is informed about any Reportable Error **immediately**, as the error must be investigated, the facts ascertained and the report made to the IPCO within five working days of discovery of the error. If a SPoC requests assistance from the Applicant or another Council officer in connection with the investigation of an error, all reasonable assistance should be provided promptly.
- 12.5 If the Council receives material from a CSP which has no relevance to any investigation or operation by the Council, the material should be securely destroyed as soon as the report to the IPCO has been made.
- 12.6 A record of all Recordable Errors will be held by NAFN, and made available for inspection by the IPCO on request. The record will contain details of the error, how the error occurred, and an indication of what steps have been or will be taken to prevent the error from occurring again. The SPoC will notify the Designated Person and the Council's Senior Responsible Officer of all Recordable and Reportable Errors.

13 POLICY AND IMPLEMENTATION

- 13.1 The Policy is operational from 15 January 2019 and replaces any previous policies and procedures relating to the acquisition of communications data.
- 13.2 The Legal Services Manager will report to the Audit Committee every two years regarding the use made by the Council of its powers under RIPA.

This page is intentionally left blank

Audit Committee Work Plan 2019/20

DATE	WORK / REPORTS
	(Provisional Dates)
29 March 2019	External Audit Planning Report 2018/19 Internal Audit Progress Report 2018/19 Internal Audit Plan 2019/20 Internal Audit Charter 2019/20 Fraud Update Report Risk Update Risk Register
31 May 2019	Treasury Management Out-turn Report 20/08/19 Local Code of Good Governance Review Draft Annual Governance Statement Draft Annual Financial Report Final Accounts Bad Debts Write-offs 20/08/19 Procurement Waivers 2018/19 Annual Internal Audit and Opinion Report 2018/19
26 July 2019	Audit Results Report 2018/19 Annual Governance Statement 2018/19 Annual Financial Report 2018/19

This page is intentionally left blank