

AGENDA

AUDIT AND RISK MANAGEMENT COMMITTEE

MONDAY, 12 FEBRUARY 2024

4.00 PM

**COUNCIL CHAMBER, FENLAND HALL,
COUNTY ROAD, MARCH**

Committee Officer: Jo Goodrum
Tel: 01354 622285
e-mail: memberservices@fenland.gov.uk

- 1 To receive apologies for absence.
- 2 Appointment of Vice-Chairman for the Municipal Year
- 3 Previous Minutes. (Pages 3 - 6)

To confirm the minutes of 20 November 2023.
- 4 To report additional items for consideration which the Chairman deems urgent by virtue of special circumstances to be now specified.
- 5 Members to declare any interests under the Local Code of Conduct in respect of any item to be discussed at the meeting.
- 6 Treasury Management Strategy Statement, Capital Strategy, Minimum Revenue Provision Policy Statement and Annual Investment Strategy 2023/24 (Pages 7 - 26)

The purpose of this report is to provide Members with information on the proposed Treasury Management Strategy Statement, Minimum Revenue Provision (MRP) Policy Statement and Annual Investment Strategy for 2024/25.

7 Internal Audit Plan 2023/24 - Progress Report Quarter 3 (Pages 27 - 38)

To report progress against the Internal Audit Plan 2023/24 for the third quarter of 1 October until 31 December 2023 and the resulting level of assurance from the planned work undertaken, and to provide an update to members on the resourcing situation within the Internal Audit team.

8 RIPA Policy (Pages 39 - 116)

This report is intended to provide members of the Audit and Risk Management Committee with an update on Fenland District Council's use of the Regulation of Investigatory Powers Act 2000 (RIPA) and to seek approval of a revised RIPA Policy.

9 Corporate Risk Register - quarterly update (Pages 117 - 148)

To provide an update to the Audit and Risk Management Committee on the Council's Corporate Risk Register.

10 Audit and Risk Management Committee Work Programme (Pages 149 - 152)

For information purposes.

11 Items of Topical Interest.

12 Items which the Chairman has under item 4 deemed urgent.

Friday, 2 February 2024

Members: Councillor K French (Chairman), Councillor G Booth, Councillor G Christy, Councillor S Harris, Councillor J Mockett and Councillor S Tierney

AUDIT AND RISK MANAGEMENT COMMITTEE

MONDAY, 20 NOVEMBER 2023 - 4.00 PM



PRESENT: Councillor K French (Chairman), Councillor G Booth and Councillor J Mockett

APOLOGIES: Councillor S Harris (Vice-Chairman), Councillor G Christy and Councillor S Tierney

Officers in attendance: Amy Brown (Assistant Director), Mark Saunders (Chief Accountant), Stephen Beacher (Head of ICT Digital & Resilience), David Thacker (Interim Internal Audit Manager) and Helen Moore (Member Services and Governance Officer)

ARMC19/23 PREVIOUS MINUTES.

The minutes of the meeting held 26 September 2023 were confirmed and signed as an accurate record.

ARMC20/23 AUDITOR'S ANNUAL REPORT 2021/22.

Members considered the Auditor's Annual Report 2021/22 report presented by Mark Saunders, Chief Accountant.

Members asked questions, made comments, and received responses as follows:

- Councillor Booth expressed surprise at the increase in fees as the majority of the work had been completed in previous years, particularly the land valuations. Mark Saunders agreed with Councillor Booth and stated there will be justification why the work was required and why the figures have increased, with the Council having to undertake another pension valuation due to the time scale of the audit which meant the OS19 was out of date and has added to the rise in cost.
- Councillor Booth stated pension figures can have an effect on the overall cost as they fluctuate and asked if the Covid crisis had any input regarding the increased fee due to administering grants on behalf of the Government? Mark Saunders responded it was additional work and costs were similar for 2020/21 and the PSAA will determine whether the costs are justified.
- Councillor Booth asked if the PSAA ask for the Council's feedback on the fees to see if the Council feel it is justified? Mark Saunders responded that they do not ask for any input on the determination of the fee.
- Councillor Nawaz commended the report and the prudent and fiscal management and this Council, if it is compared to some others in the country, appears to be in safe hands, which is a credit to note. He asked for elaboration on Page 7, Paragraphs 2 and 3, as whilst he understands how these figures are arrived at, where were the savings made and where it says including staff vacancies what has been undertaken to alleviate the issue and has that led to any under delivery of services? Mark Saunders responded that there has been no under delivery of services and the breakdown of those figures are detailed in the financial statements and Cabinet outturn report. He referred to staff vacancies, when a post becomes vacant it can take a while to get a new person into post and it depends upon what type of vacancy it is as to whether the Council recruits a temporary person so there can often be a saving to be had by staff salaries and the cost of replacing this vacancy but it depends upon the job as to whether agency staff are required. Councillor Nawaz asked what the current

position is relating to vacancies? Mark Saunders responded that there are still some vacancies in several areas which the Council is addressing in a difficult and challenging environment, acknowledging that agency costs are significantly more than what would be paid for a permanent member of staff. Councillor Nawaz made the point that this is a Council that has not raised Council Tax so the financial performance should be commended.

- Councillor Booth stated planning has the biggest staffing shortage and asked if this is where a lot of the agency staff have been needed? Mark Saunders responded that for the past two years there has been shortages, but things are improving.

Members noted the Auditor's Annual Report 2021/22.

ARMC21/23 TREASURY MANAGEMENT STRATEGY STATEMENT AND ANNUAL INVESTMENT STRATEGY MID YEAR REVIEW

Members considered the Treasury Management Strategy Statement and Annual Investment Strategy Mid-Year Review report presented by Mark Saunders, Chief Accountant.

Members asked questions, made comments, and received responses as follows:

- Councillor Booth stated that the property funds have not delivered and asked what the situation was with property funds in general, are they not performing as strongly as they have in the past as for example the uncertainty over the viability of the High Street or that office blocks are becoming a thing of the past due to flexible working? Mark Saunders responded that when it was decided which property fund to invest in there was a wide range of property funds and they all had a very different, diverse portfolio that they invest in. He stated that the two decided upon were ones which were specifically more towards the industrial sector and did not have any great focus on retail, although they do have some commercial exposure, and the returns are holding up similar to what they were when they were taken out but it is the capital value of the property fund, due to what has happened in the property market in general, which has suffered in terms of the value and it is not something the Council will be looking to get out of or sell soon until such time as capital appreciation is seen, which will hopefully be before the end of the five years.
- Councillor Booth stated there is normally a clause with these funds about withdrawals and asked if this applied and if there was a crash in the market would the Council be stuck with it? Mark Saunders responded that nobody is permitted to take any massive withdrawals out at any one time and the Council is committed for the long haul.
- Councillor Booth asked about the properties being purchased for the resettlement of families from the Ukraine and Afghan and is this fully funded by the Government? Mark Saunders responded 40% of the property price is funded by the Government and the Council is funding the difference, this is detailed in the capital programme, with the costs predicted to generate a return for the Council and help the homelessness situation by avoiding putting people into temporary accommodation and should have a positive impact on that service. He advised that each authority was given a grant for these properties which the Council took up to help with homelessness and the lack of accommodation, with the Council being under no obligation to take this up, but it was seen as a good opportunity to address the shortage of accommodation for the homeless within the Fenland area.
- Councillor Nawaz asked if the 29 properties the Council are purchasing would be available for tenants to purchase at a discounted rate? Mark Saunders responded the housing regulations are different, so the houses are not part of the right to buy regulations. Councillor Nawaz asked if there are savings to be made elsewhere as had these properties not been available the Council legally would have been obliged to house people? Mark Saunders stated this is what the Council is expecting that it will alleviate the pressure on the homelessness budget by not using bed and breakfast accommodation. He added that there are issues around homelessness and how it impacts on housing benefit which is quite complicated.

- Councillor Nawaz asked where the housing benefit comes from, the Government or the Council? Mark Saunders responded that housing benefit comes from the Government, and it is a limited amount the Council can claim back.
- Councillor Nawaz asked is there a fixed period the families can stay in these properties? Mark Saunders responded that they are meant to be temporary accommodation and are placed in these properties until alternative more permanent suitable accommodation can be found.
- Councillor Nawaz asked when it comes to housing local indigenous homeless people, how do the needs of the group equate? Mark Saunders responded that in the Homelessness Reduction Act there is a process that has to be followed to identify what the Council's liability is, but rough sleepers are part of the mix that the Council has had to house over the past few years along with other homeless people. Councillor Miss French recommended Councillor Nawaz saved any further housing questions for Dan Horn as they did not relate to this item of business and would enable the correct response to be given.

Members noted the Treasury Management Strategy Statement and Annual Investment Strategy Mid-Year Review.

ARMC22/23 INTERNAL AUDIT PLAN 2023/24 - PROGRESS REPORT Q2

Members considered the Internal Audit Plan 2023/24 presented by David Thacker, Interim Internal Audit Manager.

Members asked questions, made comments, and received responses as follows:

- Councillor Booth stated that he would like to have a copy of the executive summary report to help the panel provide assurance as he feels councillors should get an overview of the findings before the meeting takes place. David Thacker responded this is not something that has been raised directly with him and he has worked at other councils where it is not normal for councillors to receive the report. However, if Councillor Booth would like further information before the meetings, he is happy to have a conversation with him regarding this matter. Councillor Booth asked for this to be looked at as something for the future to enable members to fulfil their roles as a critical friend.
- Councillor Booth asked about the high-risk valuables in relation to public health funerals contained in the report. David Thacker responded Audit findings are labelled using various risk factors from high to medium to low and this was put into the high-risk factor because the contents of the safe were valued at £5000 and there were multiple accesses to the safe, but a second safe has now been purchased purely for public health deceased assets and procedures put in place to record an inventory.
- Councillor Booth questioned licensing and why this is a medium risk. David Thacker responded there was no proactivity to see what businesses were operating without a licence as the process was focused on renewals of existing licences, and it could be missed additional income for the Council.
- Councillor Booth stated he would like to know more about the transparency code as it appears the Council has not been complying with the code and asked how long there has been an issue in this area as some past reports seem out of date. David Thacker responded that due to the pandemic some reports were out of date, but they are now up to date, apart from one item which will be dealt with by next year, so positive progress is being made. Councillor Booth asked how often the code should be checked and complied with? David Thacker stated that this should be checked annually.
- Councillor Nawaz stated he would like to understand more about the housing options and the £1.2m spent on bed and breakfast, asking if these 34 properties are part of the 29 houses that were mentioned in an earlier report or is this separate and how much could the Council save? Mark Saunders responded the 29 houses are part of the 34 houses in the report, with the other 5 houses leased from Clarion Housing. He added that the costing is being looked at as part of the budget process.

- Councillor Booth stated that the purchase of these properties goes through the Overview and Scrutiny Panel call-in process and asked if these purchases are an ongoing situation. Mark Saunders responded the Council has received two tranches of money from the Government which had to be committed by the end of this financial year, with the Council currently having completed on 6 properties. There are more in the pipeline, with deposits being placed and they are now going through the completion process.
- Councillor Booth asked with David Thacker due to leave in March what are the plans to replace him moving forward? Amy Brown responded there are plans in place to advertise the position and find the right person for the position.

Members noted the activity and performance of the Internal Audit Plan 2023/24.

ARMC23/23 CORPORATE RISK REGISTER UPDATE

Members considered the Corporate Risk Register update presented by Stephen Beacher, Head of ICT, Digital and Resilience.

Members asked questions, made comments, and received responses as follows:

- Councillor Booth referred to the health and safety risks and feels there has been a 'deep dive' in this area, with a lot of commentary added and it is said that none of the current risk values have changed but if there are a lot more actions being taken that would suggest either that it was at the wrong level to start with or it will move to a different level once those actions are delivered and asked if it is correct that it was a 'deep dive' and why has this area been looked at specifically? Stephen Beacher responded he was not aware that it was a 'deep dive', it was just a rewording of the existing risk and having looked at this at the Risk Management Group and following procedures it was not felt it took the Council into a different risk level for mitigation. Councillor Booth responded that it is good that actions are being raised to mitigate but is it an accepted risk or are there concerns that further measures are required as the number of actions he believes makes it seem that more actions are required to control the risk. Stephen Beacher assured Councillor Booth there was nothing to be concerned about and the actions added are mostly minor in nature and day to day activities. Councillor Booth assumed the collation of the risk register assessment would be ongoing anyway? Stephen Beacher responded these are more operational risk assessments and managed by each of the services.
- Councillor Booth referred to delivery dates and the voluntary cyber security scrutiny and asked when this was going to be completed, with it being useful to have a completion date for 8 actions so members can keep a track of when things are delivered or are overdue. Stephen Beacher advised the security scrutiny was completed and passed in October.
- Councillor Booth expressed surprise that no risk have actually moved as he would have expected some movement with a full review.

Members APPROVED the updated Corporate Risk Register.

ARMC24/23 AUDIT & RISK MANAGEMENT COMMITTEE WORK PROGRAMME

Members considered the Audit and Risk Management Committee Work Programme.

Members AGREED to note the contents of the work programme.

ARMC25/23 ITEMS OF TOPICAL INTEREST.

There were no items of topical interest.

Agenda Item No:	6	
Committee:	Audit and Risk Management Committee	
Date:	12 February 2024	
Report Title:	Treasury Management Strategy Statement, Minimum Revenue Provision Policy Statement and Annual Investment Strategy 2024/25	

Cover sheet:

1 Purpose / Summary

The purpose of this report is to provide Members with information on the proposed Treasury Management Strategy Statement, Minimum Revenue Provision (MRP) Policy Statement and Annual Investment Strategy for 2024/25.

2 Key issues

- The prudential and treasury indicators detailed in paragraphs 2-13, show that the Council's capital investment plans are affordable, prudent and sustainable.
- The MRP policy sets out how the Council will make prudent provision for the repayment of borrowing needs over the medium-term forecast.
- The Treasury Management Strategy has been organised so that the Council will have sufficient cash resources to meet capital expenditure plans and operational cash flows.
- Total external interest payments which include finance lease interest payments; revised estimate for 2023/24 is £618,000 and the estimate for 2024/25 is £905,100.
- Link Group forecast that Bank Rate has now peaked at 5.25%.
- The current Medium Term Financial Strategy assumes that some external borrowing will be required over the four-year period to 31 March 2027.
- The aim of the Council's annual investment strategy is to provide security of investments whilst managing risk appropriately; investment returns are commensurate with the Council's historic low risk appetite although we are in the process of transition as a Council from a low risk policy to an appropriate managed risk policy. The Council achieves these objectives through differentiating between "specified" and "non-specified" investments and through the application of a creditworthiness policy.
- The council holds £4m in Property Funds which are long term investments. Although the returns from these investments can be higher than short term investments there is an increased risk that capital values will rise and fall.
- Total investment income from temporary investments is estimated at £1,090,000 for 2023/24 and £750,000 for 2024/2025. Income from pooled property funds is estimated at £130,000 in 2023/24 and £150,000 in 2024/25.

- The Council's Capital Strategy is currently being updated to take account of the latest developments in respect of the Council's Commercial and Investment Strategy and relevant sector guidance. The final version will be incorporated in the papers which Council considers at its meeting on 26 February 2024.

3 Recommendations

It is recommended that: -

- Audit and Risk Management Committee endorses the strategy detailed in this report to be included in the final budget report for 2024/25.

Wards Affected	All
Portfolio Holder(s)	Cllr Chris Boden, Leader and Portfolio Holder, Finance
Report Originator(s)	Peter Catchpole, Corporate Director and Chief Finance Officer (S.151 Officer) Mark Saunders, Chief Accountant
Contact Officer(s)	Peter Catchpole, Corporate Director and Chief Finance Officer (S.151 Officer) Mark Saunders, Chief Accountant
Background Paper (s)	Link Group template Budget working papers

Report:

1 Introduction

CIPFA Treasury Management Code and Prudential Code (Revised 2021)

1.1 CIPFA published the revised codes on 20 December 2021 and has stated that revisions need to be included in the reporting framework from the 2023/24 financial year. This Council has to have regard to these codes of practice when it prepares the Treasury Management Strategy Statement and Annual Investment Strategy, and also related reports during the financial year, which are taken to Full Council for approval.

1.2 The revised codes will have the following implications:

- a requirement for the Council to adopt a new debt liability benchmark treasury indicator to support the financing risk management of the capital financing requirement;
- clarify what CIPFA expects a local authority to borrow for and what they do not view as appropriate. This will include the requirement to set a proportionate approach to commercial and service capital investment;
- address Environmental, Social and Governance (ESG) issues within the Capital Strategy;
- require implementation of a policy to review commercial property, with a view to divest where appropriate;
- create new Investment Practices to manage risks associated with non-treasury investment (similar to the current Treasury Management Practices);
- ensure that any long term treasury investment is supported by a business model;
- a requirement to effectively manage liquidity and longer term cash flow requirements;
- amendment to Treasury Management Practice 1 to address ESG policy within the treasury management risk framework;
- amendment to the knowledge and skills register for individuals involved in the treasury management function - to be proportionate to the size and complexity of the treasury management conducted by each council;
- a new requirement to clarify reporting requirements for service and commercial investment, (especially where supported by borrowing/leverage).

1.3 In addition, all investments and investment income must be attributed to one of the following three purposes: -

Treasury management

Arising from the organisation's cash flows or treasury risk management activity, this type of investment represents balances which are only held until the cash is required for use. Treasury investments may also arise from other treasury risk management activity which seeks to prudently manage the risks, costs or income relating to existing or

forecast debt or treasury investments. The Council's investment in property funds falls into this category.

Service delivery

Investments held primarily and directly for the delivery of public services including housing, regeneration and local infrastructure. Returns on this category of investment which are funded by borrowing are permitted only in cases where the income is "either related to the financial viability of the project in question or otherwise incidental to the primary purpose".

Commercial return

Investments held primarily for financial return with no treasury management or direct service provision purpose. Risks on such investments should be proportionate to a council's financial capacity – i.e., that 'plausible losses' could be absorbed in budgets or reserves without unmanageable detriment to local services. An authority must not borrow to invest primarily for financial return. This does not preclude the Council from taking forward investments as part of its Commercial and Investment Strategy so long as financial return is not the primary reason for taking forward the scheme. This particularly applies in the case of projects relating to housing where service delivery objectives can be achieved as well as a financial return.

- 1.4 As this Treasury Management Strategy Statement and Annual Investment Strategy deals solely with treasury management investments, the categories of service delivery and commercial investments will be dealt with as part of the Capital Strategy report
- 1.5 These changes are now fully adopted within the 2024/25 TMSS report.

2 Background

- 2.1 The Council is required to operate a balanced budget, which broadly means that cash raised during the year will meet cash expenditure. Part of the treasury management operation is to ensure that this cash flow is adequately planned, with cash being available when it is needed. Surplus monies are invested in low risk counterparties or instruments commensurate with the Council's assessment of its risk appetite, providing adequate liquidity initially before considering investment return.
- 2.2 The second main function of the treasury management service is the funding of the Council's capital plans. These capital plans provide a guide to the borrowing need of the Council, essentially the longer term cash flow planning to ensure that the Council can meet its capital spending obligations. This management of longer term cash may involve arranging long or short term loans or using longer term cash flow surpluses. On occasion, when it is prudent and economic, any debt previously drawn may be restructured to meet Council risk or cost objectives.
- 2.3 The contribution the treasury management function makes to the authority is critical, as the balance of debt and investment operations ensure liquidity or the ability to meet spending commitments as they fall due, either on day-to-day revenue or for larger capital projects. The treasury operations will see a balance of the interest costs of debt and the investment income arising from cash deposits affecting the available budget. Since cash balances generally result from reserves and balances, it is paramount to ensure adequate security of the sums invested, as a loss of principal will in effect result in a loss to the General Fund Balance.

CIPFA defines treasury management as:

"The management of the local authority's borrowing, investments and cash flows, its banking, money market and capital market transactions; the effective control of the risks associated with those activities; and pursuit of optimum performance consistent with those risks."

- 2.4 Whilst any commercial initiatives or loans to third parties will impact on the treasury function, these activities are generally classed as non-treasury activities, (arising usually from capital expenditure), and are separate from the day-to-day treasury management activities.

3 The Capital Strategy Reporting Requirements

- 3.1 The CIPFA revised 2021 Prudential and Treasury Management Codes require all local authorities to prepare an additional document, a Capital Strategy which will provide the following:
- a high-level long-term overview of how capital expenditure, capital financing and treasury management activity contribute to the provision of services;
 - an overview of how the associated risk is managed; and
 - the implications for future financial sustainability.
- 3.2 The aim of the Capital Strategy is to ensure that all elected members on full Council fully understand the overall long-term policy objectives and resulting capital strategy requirements, governance procedures and risk appetite.

4 Treasury Strategy Reporting Requirements

- 4.1 The Council is required to receive and approve, as a minimum, three main treasury reports each year, which incorporate a variety of policies, estimates and actuals. These reports are required to be adequately scrutinised by the Audit and Risk Management Committee and Cabinet before being recommended to the Council.
- 4.2 **Prudential and Treasury Indicators and Treasury Strategy** (this report), the first and most important report is forward looking and covers:
- the capital plans (including prudential indicators);
 - a Minimum Revenue Provision policy (how residual capital expenditure is charged to revenue over time);
 - the Treasury Management Strategy (how investments and borrowings are to be organised) including treasury indicators; and
 - an Investment Strategy (the parameters on how investments are to be managed).

A Mid-Year Treasury Management Report - This will update Members with the progress of the capital position, amending prudential indicators as necessary and whether any policies require revision.

An Annual Treasury Report - This is a backward looking review document and provides details of actual prudential and treasury indicators and actual treasury operations compared to the estimates within the strategy.

- 4.3 The Strategy covers two main areas:

Capital issues

- the capital expenditure plans and associated prudential indicators;
- the MRP policy.

Treasury management issues

- the current treasury position;
- treasury indicators which limit the treasury risk and activities of the Council;
- prospects for interest rates;
- the borrowing strategy;

- policy on borrowing in advance of need;
- debt rescheduling;
- the investment strategy;
- creditworthiness policy; and
- policy on use of external service providers.

These elements cover the requirements of the Local Government Act 2003, the CIPFA Prudential Code, DLUHC MRP Guidance, the CIPFA Treasury Management Code and the DLUHC Investment Guidance.

4.4 **IFRS16 - Leases** The CIPFA Local Authority Accounting Code Board has deferred implementation of IFRS16 until 1 April 2024, the 2024/25 financial year. IFRS 16 defines a lease as a contract or part of a contract, which conveys the right to use an asset (the underlying asset) for a period of time in exchange for a consideration. Under the new standard the distinction between finance leases and operating leases under the previous leasing standard is removed and all leases are treated in the way the finance leases currently are. A 'right of use' asset is shown on the balance sheet with a corresponding liability of the discounted value of the future lease payments. There are exceptions for short, dated leases (under a year, or with less than a year remaining at transition) and low value leases (low value to be determined by the council using its approach to determining de minimus items). This means that all leases that do not meet the exceptions will be treated as capital expenditure from 2024/25 and form part of the Capital Financing Requirement. Although legally the Council doesn't own the asset during the lease duration, International Accounting Standards require that the Council capitalise the asset and liability on its balance sheet, much like a loan. Whilst this increases the CFR, the nature of the finance lease agreement doesn't require the Council to separately borrow to fund the asset.

4.5 **Training** - The CIPFA Treasury Management Code requires the responsible officer to ensure that members with responsibility for treasury management receive adequate training in treasury management. This especially applies to members responsible for scrutiny.

The training needs of treasury management officers and members are periodically reviewed.

5 **Capital Prudential Indicators 2024/25 to 2026/27**

5.1 The Council's capital expenditure plans are the key driver of treasury management activity. The output of the capital expenditure plans is reflected in the prudential indicators, which are designed to assist Members' overview and confirm capital expenditure plans are prudent, affordable and sustainable.

5.2 The capital expenditure prudential indicator is a summary of the Council's capital expenditure plans, both those agreed previously and those forming part of this budget cycle. Commercial activities/non-financial investments relate to areas such as capital expenditure on investment properties, loans to third parties etc.

5.3 The table below summarises the capital expenditure plans and how these are being financed by capital or revenue resources. Any shortfall of resources results in a funding borrowing need.

Capital Programme	2023/24 Revised Estimate £000	2024/25 Estimate £000	2025/26 Estimate £000	2026/27 Estimate £000
Forecast Capital Expenditure	14,634	6,695	3,097	1,829
Commercial and Investment Strategy Schemes	7,389	2,730	6,000	7,972
TOTAL	22,023	9,425	9,097	9,801
Financed by:				
Capital Grants	12,541	2,754	1,194	1,194
Capital Receipts	155	250	250	250
Reserves used in year to fund Capital	2,674	730	0	0
Section 106 and Other Contributions	1,025	45	38	35
Total Financing	16,395	3,779	1,482	1,479
Net Financing Need for The Year (Borrowing)	5,628	5,646	7,615	8,322

- 5.4 The second prudential indicator is the Council's Capital Financing Requirement (CFR). The CFR is simply the total historic outstanding capital expenditure which has not yet been paid for from either revenue or capital resources. It is essentially a measure of the Council's indebtedness, its underlying borrowing need. Any capital expenditure shown above, which has not immediately been paid for will increase the CFR.
- 5.5 The CFR does not increase indefinitely, as each year the Council is required to pay off an element of the capital spend (including finance leases) through a statutory revenue charge (MRP). In the case of schemes taken forward as part of the Council's capital programme this has the effect of reducing the Council's (CFR) broadly over the asset's life.
- 5.6 In the case of capital expenditure incurred in accordance with the Council's Commercial and Investment Strategy the MRP charge cannot be determined until such time that the Investment Board approves a scheme. Where the projected Capital Financing Requirement is disclosed in this report the figures used reflect the impact of borrowing to fund the full allocation of the remaining £16.972m over the next 4 years but no assumptions have been made regarding how MRP might reduce the CFR attributable to these schemes. This approach is considered reasonable until such time that any new schemes are formally approved by the Investment Board. In accordance with the current Minimum Revenue Policy, a provision for MRP in relation to the investment and residential property acquired in previous financial years is incorporated into the information in this report and the Council's Medium Term Financial Strategy.
- 5.7 In this context, it is also important to note that, as well as the statutory MRP charge, the Council is permitted to make additional voluntary payments to reduce the CFR. These voluntary payments will typically reduce the statutory charge that would have been due in future years. Voluntary payments can be funded from capital resources. This is particularly significant in the context of the Council's Commercial and Investment Strategy. As a result of investments undertaken, the Council may receive significant capital receipts and/or repayments of amounts due under the terms of loan agreements with third parties, including the Local Authority Trading Company. These amounts may be received before the maturity date of the external borrowing used to undertake the initial

investment. Any assumptions regarding the anticipated use of capital resources to reduce the CFR will be reported as part of future treasury management reporting.

5.8 The CFR includes any other long term liabilities (finance leases).

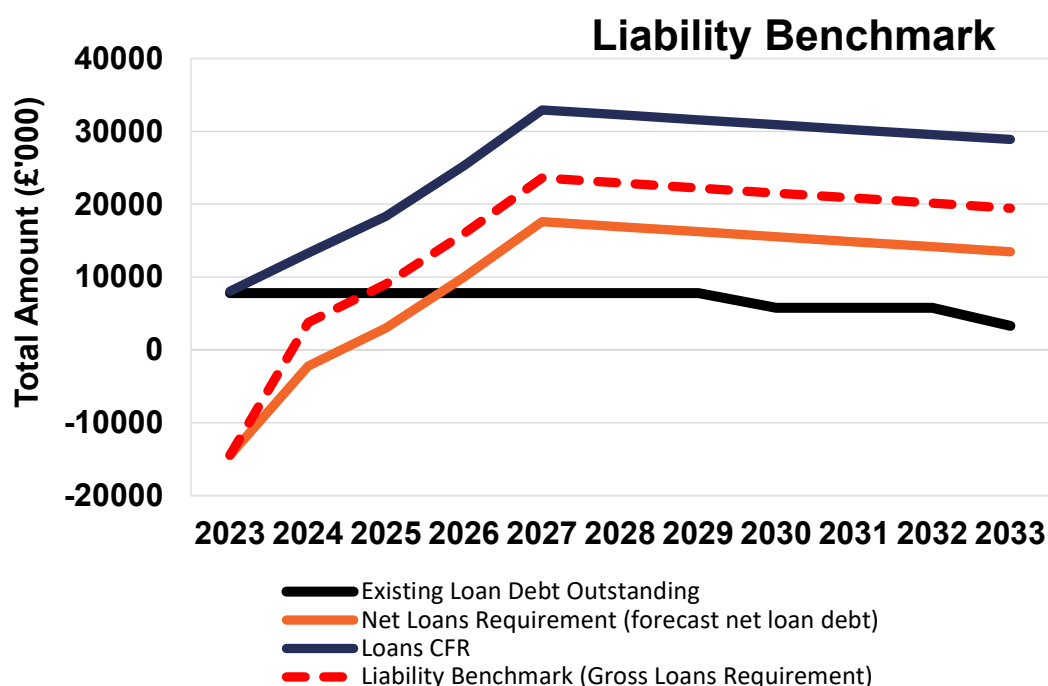
Capital Financing Requirement (CFR)	2023/24 Revised Estimate £000	2024/25 Estimate £000	2025/26 Estimate £000	2026/27 Estimate £000
CFR – as at 31 March				
Opening CFR	8,052	13,296	18,354	25,295
Movement in CFR	5,244	5,058	6,941	7,646
Closing CFR	13,296	18,354	25,295	32,941
Movement in CFR represented by				
Net financing need for the year	5,628	5,646	7,615	8,322
Less MRP and other Financing Movements	(384)	(588)	(674)	(676)
Movement in CFR	5,244	5,058	6,941	7,646

5.9 The third prudential indicator is the Liability Benchmark (LB). The liability benchmark is a measure of how well the existing loans portfolio matches the authority's planned borrowing needs.

5.10 The purpose of this prudential indicator is to compare the authority's existing loans outstanding (the black line) against its future need for loan debt, or liability benchmark (the red line).

5.11 The liability benchmark below indicates a future borrowing requirement over the life of this strategy.

5.12 The timing of actual borrowing arranged may differ from the liability benchmark depending on actual cash balances, the rate at which the capital programme is delivered and actual use of reserves and working capital.



6 Minimum Revenue Provision (MRP) Policy Statement

- 6.1 The Council is required to pay off an element of the accumulated general fund capital spend each year (the CFR) through a revenue charge (the minimum revenue provision), although it is also allowed to undertake additional voluntary payments if required (voluntary revenue provision).
- 6.2 DLUHC regulations have been issued which require the Council to approve an MRP statement in advance each year. A variety of options are provided to Councils within the guidance. Councils are permitted under the guidance to establish their own approach to setting MRP, and different approaches can be applied for different types of assets. The Council's principal responsibility is to ensure that it can demonstrate that whatever approach they adopt across their asset base it is prudent. Given the Council's decision to adopt a Commercial and Investment Strategy it was necessary to revise the MRP policy in 2020/21 to take account of investments which might feasibly be taken forward in accordance with the Commercial and Investment Strategy. The policy applicable for the current financial year onwards is as follows:
- (1) For unsupported borrowing (including finance leases) undertaken to fund the Council's capital programme, excluding any capital expenditure approved by the Council's Investment Board for Investment Properties, MRP will be based on the estimated useful life of the assets to be purchased or acquired. Repayments made under the terms of finance leases shall be applied as MRP.
 - (2) For Investment Properties purchased or constructed (following a decision taken by the Council's Investment Board) the MRP charge shall be based on the difference between the value of the asset and the value of any outstanding unsupported borrowing secured to fund the original purchase of the asset. A calculation shall be undertaken at the end of each financial year to identify the difference between the value of the asset and the amount borrowed. Where a difference exists MRP shall be charged over a period commensurate with the period the Council expects to hold the asset as set out in reports presented to the Investment Board.
 - (3) For any loans made to third parties, including those made to the Local Authority Trading Company, no MRP shall be charged where the loan requirement requires the third party to make repayments on at least an annual basis over the life of the loan. In the unlikely event of the Council providing a maturity loan to a third party, MRP shall be charged in equal amounts over the life of the loan.
 - (4) Should the Council acquire an equity stake in any third party, the MRP charge will be for the lower of twenty years or the scheduled completion date of any projects funded by the third party using the proceeds from selling an equity stake to the Council.
 - (5) For investment in Property Funds which the Council, following consultation with its Treasury Advisors, assesses as meeting the definition of capital expenditure MRP shall be charged over the period the Council expects to hold the investment. The period over which MRP can be charged for this type of investment shall not be permitted to exceed 20 years. The property funds referred to elsewhere in this document do not meet the definition of capital expenditure.
- 6.3 It is important to note that DLUHC are currently consulting on potential changes to the guidance relating to setting the Minimum Revenue Provision. One potential outcome of the consultation is that government could bring forward changes to the regulations.

7 The Use of Council's Resources and the Investment Position

- 7.1 The application of resources (capital receipts, reserves etc) and temporary use of 'surplus cash balances' to both finance capital expenditure and other budget decisions to support the revenue budget reduces cash investment balances held (see below). Unless resources are supplemented with new sources (asset sales, capital grants, etc) then new borrowing will be required to fulfil the objectives as set in the Council's Business Plan. Detailed below are estimates of the year end balances for each resource.

Year End Resources	2023/24 Revised Estimate £000	2024/25 Estimate £000	2025/26 Estimate £000	2026/27 Estimate £000
Fund balances / reserves	13,000	12,600	11,600	11,500
Expected investments	14,600	14,800	14,500	15,000

8 Affordability Prudential Indicators

- 8.1 The previous sections cover the overall capital and control of borrowing prudential indicators; also within this framework prudential indicators are required to assess the affordability of the capital investment plans. These provide an indication of the impact of the capital investment plans on the Council's overall finances. The Council is asked to approve the following indicators.
- 8.2 This indicator identifies the trend in the cost of capital (borrowing and other long term obligation costs net of investment income) against the net revenue stream.

Financing Costs to Net Revenue Stream	2023/24 Revised Estimate %	2024/25 Estimate %	2025/26 Estimate %	2026/27 Estimate %
General Fund	5.94	8.25	9.75	10.65
Net Revenue Stream	£16.857m	£18.097m	£17.405m	£17.466m

- 8.3 Net Income from Commercial and Service Investments as % of net revenue stream. This indicator identifies the authority's reliance on income from Commercial and Service Investments such as rents from the Council's long-standing portfolio of non-operational assets managed to secure rental income and income from fees and charges earned from providing facilities for conferences and meetings (economic estates) and one commercial investment property.

Ratio of Income from Commercial and Service Investments to net revenue stream	2023/24 Revised Estimate %	2024/25 Estimate %	2025/26 Estimate %	2026/27 Estimate %
General Fund	6.8	6.7	7.0	7.0
Net Revenue Stream	£16.857m	£18.097m	£17.405m	£17.466m

9 Treasury Management Strategy

- 9.2 The capital expenditure plans set out in section 5 provide a summary of future level of spend. The treasury management function ensures that the Council's cash is organised in accordance with the relevant professional codes, so that sufficient cash is available to

meet service activity and the Council's capital strategy. This will involve both the organisation of cash flow and where capital plans require, the organisation of appropriate borrowing facilities. The strategy covers the relevant treasury / prudential indicators, the current and projected debt positions and the annual investment strategy.

- 9.3 The Council's treasury portfolio as at 31 March 2023 for borrowing and investments was £7.823m and £22.550m respectively. As of 31 December 2023, investments are £21.720m (see Appendix A attached) and borrowing £7.823m.
- 9.4 The Council's forward projections for borrowings are summarised below. The next table shows the actual external debt, against the underlying capital borrowing need (the Capital Financing Requirement - CFR).

	2023/24 Revised Estimate £000	2024/25 Estimate £000	2025/26 Estimate £000	2026/27 Estimate £000
Debt at 1 April	7,800	13,430	19,080	26,700
Expected change in debt to fund capital programme (excluding Commercial and Investment Strategy schemes)	4,630	3,650	1,620	350
Borrowing to fund Commercial and Investment Strategy Schemes	1,000	2,000	6,000	7,970
Other long term liabilities (OLTL)	23	0	0	0
Expected change in OLTL	(23)	0	0	0
Actual gross debt at 31 March	13,430	19,080	26,700	35,020
Capital financing requirement (CFR) at 31 March	13,296	18,354	25,295	32,941
Borrowing less CFR – 31 March	134	726	1,405	2,079

- 9.5 At 1 April 2023 the Council's Debt position comprised other long-term liabilities relating to finance leases of £23k and external borrowing of £7.8m. These loans were taken out at prevailing market rates between 1994 and 2004. The term of these loans is between 25 and 50 years. Following the transfer of the Council's Housing Stock in 2007, which generated a significant capital receipt for the Council, the Council has retained investment balances which exceed the amounts borrowed. However, changes in prevailing interest rates since the loans were taken out mean that a high premium would be payable by the Council if it were to seek to repay the PWLB loans (£4.5m) early. The premiums to be applied are considered to be prohibitively high for early redemption to be regarded as a reasonable treasury management decision. Repaying the Barclays market rate loan of £3.3m may be considered whilst premature redemption rates remain elevated but only if there is surplus cash available to facilitate any repayment. The Council continues to keep this situation under review with the support of its appointed treasury management advisors. However, for the purposes of this strategy, it has been assumed that external borrowing of £7.8m brought forward, as at 1 April 2023, will continue to be carried forward.
- 9.6 Within the prudential indicators there are a number of key indicators to ensure that the Council operates its activities within well-defined limits. One of these is that the Council needs to ensure that its gross debt, does not, except in the short term, exceed the total of

the CFR in the preceding year plus the estimates of any additional CFR for 2024/25 and the following two financial years. This allows some flexibility for limited early borrowing for future years but ensures that long term borrowing is not undertaken for revenue or speculative purposes (in the sense of anticipating future upward movements in interest rates), other than where the borrowing fits in with the Council's approved Investment Strategy.

9.7 The Council notes that the Prudential Code published by CIPFA prohibits local authorities from borrowing in advance of need. This prohibition has been recently re-affirmed by DLUHC in its Statutory Guidance on Local Authority Investments which states that this prohibition extends to undertaking borrowing to fund the purchase of financial and non-financial investments, including investment properties. This is on the basis that in such circumstances local authorities would be borrowing 'purely in order to profit from investment of the extra sums borrowed'. Section 4 of the Council's Capital Strategy explains how the Council has had regard for this guidance and notes the Council's approach to determining whether the motivation behind any proposed investment is purely to profit from investment of any sums borrowed.

9.8 Interest repayments associated with the external debt (including finance leases) above are shown below.

YEARS	INTEREST DUE £000
2023/24	618,000
2024/25	905,100
2025/26	1,023,700
2026/27	1,183,000

9.9 The operational boundary is the limit beyond which external debt is not normally expected to exceed. In most cases this would be a similar figure to the CFR but may be lower or higher depending on the levels of actual debt.

Operational Boundary	2023/24 Revised Estimate £000	2024/25 Estimate £000	2025/26 Estimate £000	2026/27 Estimate £000
Debt	12,430	16,080	17,700	18,050
Other long term liabilities	1,000	1,000	1,000	1,000
Commercial Activities / Non Financial Investments	1,000	3,000	9,000	16,970
Total	14,430	20,080	27,700	36,020

9.10 The authorised limit is a key prudential indicator, which represents a control on the maximum level of borrowing. This represents a legal limit beyond which external debt is prohibited and this limit needs to be set or revised by full Council. It reflects the level of external debt which, while not desired, could be afforded in the short term but is not sustainable in the longer term.

9.11 This is a statutory limit determined under section 3 (1) of the Local Government Act 2003. The Government retains an option to control either the total of all council's plans, or those of a specific council, although this power has not yet been exercised. The Council is asked to approve the following authorised limit.

Authorised Limit	2023/24	2024/25	2025/26	2026/27
-------------------------	----------------	----------------	----------------	----------------

	Revised Estimate £000	Estimate £000	Estimate £000	Estimate £000
Debt	17,430	21,080	22,700	23,050
Other long term liabilities	1,000	1,000	1,000	1,000
Commercial Activities / Non Financial Investments	1,000	3,000	9,000	16,970
Total	19,430	25,080	32,700	41,020

10 Prospects for Interest Rates

- 10.1 The Council has appointed Link Group as its treasury advisor and part of their service is to assist the Council to formulate a view on interest rates. The following table gives Link Assets Service's central view.

	Mar-24	Jun-24	Sep-24	Dec-24	Mar-25	Jun-25	Sep-25	Dec-25	Mar-26	Jun-26	Sep-26	Dec-26	Mar-27
BANK RATE	5.25	5.25	4.75	4.25	3.75	3.25	3.00	3.00	3.00	3.00	3.00	3.00	3.00
3 month ave earnings	5.30	5.30	4.80	4.30	3.80	3.30	3.00	3.00	3.00	3.00	3.00	3.00	3.00
6 month ave earnings	5.20	5.10	4.60	4.10	3.70	3.30	3.10	3.10	3.10	3.10	3.10	3.10	3.10
12 month ave earnings	5.00	4.90	4.40	3.90	3.60	3.20	3.10	3.10	3.10	3.10	3.10	3.20	3.20
5 yr PWLB	4.50	4.40	4.30	4.20	4.10	4.00	3.80	3.70	3.60	3.60	3.50	3.50	3.50
10 yr PWLB	4.70	4.50	4.40	4.30	4.20	4.10	4.00	3.90	3.80	3.70	3.70	3.70	3.70
25 yr PWLB	5.20	5.10	4.90	4.80	4.60	4.40	4.30	4.20	4.20	4.10	4.10	4.10	4.10
50 yr PWLB	5.00	4.90	4.70	4.60	4.40	4.20	4.10	4.00	4.00	3.90	3.90	3.90	3.90

- 10.2 Links central forecast for interest rates was updated on 7 November and reflected a view that the MPC would be keen to further demonstrate its anti-inflation credentials by keeping Bank Rate at 5.25 until at least summer 2024. They then expect rate cuts to start when both the CPI inflation and wage/employment data are supportive of such a move, and when there is a likelihood of the overall economy enduring at least a slowdown or mild recession over the coming months (although most recent GDP releases have surprised with their on-going robustness).
- 10.3 Naturally, timing on this matter will remain one of fine judgment: cut too soon, and inflationary pressures may well build up further; cut too late and any downturn or recession may be prolonged.
- 10.4 In the upcoming months, forecasts will be guided not only by economic data releases and clarifications from the MPC over its monetary policies and the Government over its fiscal policies, but also international factors such as policy development in the US and Europe, the provision of fresh support packages to support the faltering recovery in China as well as the on-going conflict between Russia and Ukraine, and Gaza and Israel.
- 10.5 Gilt Yields and PWLB Rates - The overall longer-run trend is for gilt yields and PWLB rates to fall back over the timeline of our forecasts, as inflation continues to fall through 2024.
- 10.6 Links target borrowing rates are set two years forward (as they expect rates to fall back) and the current PWLB (certainty) borrowing rates are set out below: -

PWLB debt	Current borrowing rate as at 08.01.24 p.m.	Target borrowing rate now (end of Q4 2025)	Target borrowing rate previous (end of Q3 2025)

5 years	4.53%	3.70%	3.80%
10 years	4.67%	3.90%	3.80%
25 years	5.19%	4.20%	4.20%
50 years	4.97%	4.00%	4.00%

- 10.7 Borrowing advice: Links long-term (beyond 10 years) forecast for Bank Rate remains at 3% and reflects Capital Economics' research that suggests AI and general improvements in productivity will be supportive of a higher neutral interest rate. As all PWLB certainty rates are currently significantly above this level, borrowing strategies will need to be reviewed in that context. Overall, better value can be obtained at the shorter end of the curve and short-dated fixed LA to LA monies should be considered. Temporary borrowing rates will remain elevated for some time to come but may prove the best option whilst the market continues to factor in Bank Rate reductions for 2024 and later.
- 10.8 The current forecast shown in paragraph 10.1, includes a forecast for Bank Rate to have peaked at 5.25%. The Council continues to benefit from what is a higher interest rate environment than has been the case in recent years. The Medium Term Financial Strategy (MTFS) reflects expected investment rate income in future years. This is expected to reduce from that observed in 2023/24 as existing cash balances are used to fund capital expenditure and the base rate begins to reduce.
- 10.9 As there are so many variables at this time, caution must be exercised in respect of all interest rate forecasts.

11 Borrowing Strategy

- 11.1 As noted above in paragraph 9.5 the Council recognises that statutory guidance indicates that whilst the Council has the necessary powers to borrow in advance of need the government and CIPFA state it should refrain from doing so where such borrowing takes place purely in order to profit from investment of the extra sums borrowed. None of the Council's current borrowing was undertaken in advance of need.
- 11.2 The Council has previously maintained an under-borrowed position. This means that the capital borrowing need, (the Capital Financing Requirement), has not been fully funded with loan debt as cash supporting the Council's reserves, balances and cash flow have been used as an alternative funding measure. This strategy is considered prudent whilst investment returns are lower than the cost of borrowing and counterparty risk remains an issue to be considered.
- 11.3 The current MTFS assumes that external borrowing will be required over the four-year period to 31 March 2027. Assumptions about the level of external interest payable are reflected as part of the prudential indicators included in this document. Responsibility for deciding when to borrow externally, together with details of the amount to borrow and the term and type of any loan, rests with the Chief Finance Officer. The Chief Finance Officer's decision will be informed by advice from the Council's treasury management advisors and information regarding the progress of schemes set out in the capital programme. Any borrowing decisions will be reported to Cabinet through either the mid-year or annual treasury management reports.
- 11.4 When the Council borrows externally it will ordinarily do so using funds borrowed from the Public Works Loan Board, though this does not preclude the Council considering other sources of lending.

11.5 Maturity structure of borrowing. These gross limits are set to reduce the Council's exposure to large, fixed rate sums falling due for refinancing and are required for upper and lower limits.

11.6

Maturity structure of fixed interest rate borrowing 2024/25	Lower %	Upper %
Under 12 months	0	100
12 months to 2 years	0	100
2 years to 5 years	0	100
5 years to 10 years	0	100
10 years and above	0	100

Maturity structure of variable interest rate borrowing 2024/25	Lower %	Upper %
Under 12 months	0	100
12 months to 2 years	0	100
2 years to 5 years	0	100
5 years to 10 years	0	100
10 years and above	0	100

12 Debt Rescheduling / Repayment

12.1 Rescheduling of current borrowing in our debt portfolio may be considered whilst premature redemption rates remain elevated but only if there is surplus cash available to facilitate any repayment, or rebalancing of the portfolio to provide more certainty is considered appropriate.

12.2 If rescheduling was done, it will be reported to the Cabinet at the earliest meeting following its action.

13 Annual Investment Strategy - management of risk

13.1 The Department of Levelling Up, Housing and Communities (DLUHC) and CIPFA have extended the meaning of 'investments' to include both financial and non-financial investments. This report deals solely with treasury (financial) investments, (as managed by the treasury management team). Non-financial investments, essentially the purchase of income yielding assets, are covered in the Capital Strategy, (a separate report).

13.2 The Council's investment policy has regard to the following: -

- DLUHC's Guidance on Local Government Investments ("the Guidance");
- CIPFA Treasury Management in Public Services Code of Practice and Cross Sectoral Guidance Notes 2021 ("the Code"); and
- CIPFA Treasury Management Guidance Notes 2021.

13.3 The Council's investment priorities will be security first, portfolio liquidity second and then yield, (return). The Council will aim to achieve the optimum return (yield) on its investments commensurate with proper levels of security and liquidity and with the Council's risk appetite

13.4 The above guidance from the DLUHC and CIPFA, place a high priority on the management of risk. The Council has adopted a prudent approach to managing risk and defines its risk appetite by the following means.

13.5 Minimum acceptable credit criteria are applied in order to generate a list of highly creditworthy counterparties which also enables diversification and thus avoidance of

concentration risk. The key ratings used to monitor counterparties are the Short Term and Long Term ratings.

- 13.6 Ratings will not be the sole determinant of the quality of an institution; it is important to continually assess and monitor the financial sector on both a micro and macro basis and in relation to the economic and political environments in which institutions operate. The assessment will also take account of information that reflects the opinion of the markets. To achieve this consideration the Council will engage with its advisors to maintain a monitor on market pricing such as “credit default swaps” and overlay that information on top of the credit ratings.
- 13.7 Investment instruments identified for use in the financial year are listed below under the ‘specified’ and ‘non-specified’ investments categories. Counterparty limits will be as set through the Council’s treasury management practices – schedules.
- 13.8 **Specified Investments** - These investments are sterling investments (meeting the minimum ‘high’ quality criteria where applicable) of not more than one year maturity, or those which could be for a longer period but where the Council has the right to repay within 12 months if it wishes. These are considered low risk assets where the possibility of loss of principal or investment income is small. Investment instruments identified for use in the financial year are as follows:
- term deposits with part nationalised banks and local authorities;
 - term deposits with high credit criteria deposit takers (banks and building societies);
 - callable deposits with part nationalised banks and local authorities;
 - callable deposits with high credit criteria deposit takers (banks and building societies);
 - money market funds (CNAV) / (LVNAV) / (VNAV);
 - Debt Management Agency Deposit Facility (DMADF); and
 - UK Government gilts, custodial arrangement required prior to purchase.
- 13.9 **Non-Specified Investments** - These are any other type of investment (i.e. not defined as specified above). Investment instruments identified in both “specified” and “non-specified” categories are differentiated by maturity date and classed as non-specified when the investment period and right to be repaid exceeds one year. Non-specified investments are more complex instruments which require greater consideration by members and officers before being authorised for use. Investment instruments identified for use in the financial year are as follows:
- term deposits with high credit criteria deposit takers (banks and building societies);
 - term deposits with part nationalised banks and local authorities;
 - callable deposits with part nationalised banks and local authorities;
 - callable deposits with high credit criteria deposit takers (banks and building societies);
 - Debt Management Agency Deposit Facility (DMADF);
 - UK Government gilts, custodial arrangement required prior to purchase; and
 - Property funds.
- 13.10 As a result of the change in accounting standards for 2023/24 under IFRS 9, this Authority will consider the implications of investment instruments which could result in an adverse movement in the value of the amount invested and resultant charges at the end of the year to the General Fund. (In November 2018, the MHCLG, concluded a consultation for a temporary override to allow English local authorities time to adjust their

portfolio of all pooled investments by announcing a statutory override to delay implementation of IFRS 9 for five years ending 31.3.23. More recently, a further extension to the over-ride to 31.3.25 has been agreed by Government.

- 13.11 At present, fluctuations in the value of the external property funds do not impact on the council's revenue account, because they are held in an unusable reserve via the statutory override arrangements set out in IFRS9. The override was extended in early 2023 to 31 March 2025. It is unclear if the override will be extended beyond that date.
- 13.12 Investments will be made with reference to the core balance and cash flow requirements and the outlook for short-term interest rates (i.e. rates for investments up to 12 months). Greater returns are usually obtainable by investing for longer periods. Short term cash flow requirements (up to 12 months) include payments such as, precepts, business rate retention, housing benefits, salaries, suppliers, interest payments on debt etc.
- 13.13 The current forecast shown in paragraph 10.1, includes a forecast for Bank Rate to have peaked at 5.25%.
- 13.14 The suggested budgeted investment earnings rates for returns on investments placed for periods up to about three months during each financial year are as follows:

Average earnings in each year	
2023/24 (residual)	5.30%
2024/25	4.55%
2025/26	3.10%
2026/27	3.00%

- 13.15 Estimated investment income is £1,090,000 2023/24 and £750,000 in 2024/25. These estimates assume that none of the existing cash balances held by the Authority will be utilised to fund schemes approved by the Investment Board.
- 13.16 £4m of the Council's investments are held in externally managed pooled property funds where short-term security and liquidity are lesser considerations, and the objectives instead are regular revenue income and long-term price stability.
- 13.17 As the Council's externally managed 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 medium to long-term investment objectives are regularly reviewed. Although the returns from these investments can be higher than short term investments there is an increased risk that capital values will rise and fall. The 2023/24 projected outturn for property fund income is £130,000 and the estimate for 2024/25 is £150,000.
- 13.18 **Investment treasury indicator and limit** - total principal funds invested for greater than 365 days. These limits are set with regard to the Council's liquidity requirements and to reduce the need for early sale of an investment and are based on the availability of funds after each year end.

	2024/25 £000	2025/26 £000	2026/27 £000
Maximum principal sums invested > 365 days	10,000	10,000	10,000

- 13.19 For its cash flow generated balances, the Council will seek to utilise its call accounts and short dated deposits (overnight to 180 days) in order to benefit from the compounding interest.
- 13.20 At the end of the financial year, the Council will report on its investment activity as part of its Annual Treasury Report.

14 Creditworthiness Policy

14.1 The Council applies the creditworthiness service provided by Link Group. This service employs a sophisticated modelling approach utilising credit ratings from the three main credit rating agencies - Fitch, Moody's and Standard & Poor's. The credit ratings of counterparties are supplemented with the following overlays:

- "watches" and "outlooks" from credit rating agencies;
- Credit Default Swaps spreads to give early warning of likely changes in credit ratings;
- sovereign ratings to select counterparties from only the most creditworthy countries.

14.2 This modelling approach combines credit ratings, Watches and Outlooks in a weighted scoring system, which is then combined with an overlay of CDS spreads for which the end product is a series of colour coded bands which indicate the relative creditworthiness of counterparties. These colour codes are used by the Council to determine the suggested duration for investments. The Council will therefore use counterparties within the following durational bands:

- yellow 5 years;
- dark pink 5 years for ultra-short dated bond funds with a credit score of 1.25;
- light pink 5 years for ultra-short dated bonds funds with a credit score of 1.5;
- purple 2 years;
- blue 1 year (only applies to nationalised or semi nationalised UK banks);
- orange 1 year;
- red 6 months;
- green 100 days
- no colour not to be used.

14.3 The Link creditworthiness service uses a wider array of information than just primary ratings and by using a risk weighted scoring system does not give undue preponderance to just one agency's ratings.

14.4 Typically, the minimum credit ratings criteria the Council will use will be short term rating (Fitch or equivalents) of F1 and a long-term rating of A-. There may be occasions when the counterparty ratings from one rating agency are marginally lower than these ratings but may still be used. In these instances consideration will be given to the whole range of ratings available, or other topical market information, to support their use

14.5 The Council's own bank currently meets the creditworthiness policy. However, should they fall below Link Group creditworthiness policy the Council will retain the bank on its counterparty list for transactional purposes, though would restrict cash balances to a minimum.

14.6 All credit ratings are monitored weekly. The Council is alerted to changes to ratings of all three agencies through its use of the Link Group creditworthiness service.

- If a downgrade results in the counterparty / investment scheme no longer meeting the Council's minimum criteria, its further use as a new investment will be withdrawn immediately.
 - In addition to the use of credit ratings the Council will be advised of information in movements in credit default swaps against the iTraxx European Senior Financials benchmark and other market data on a weekly basis. Extreme market movements may result in downgrade of an institution or removal from the Council's lending list.
- 14.7 Sole reliance will not be placed on the use of Link Group Creditworthiness policy. In addition, this Council will also use market data and market information, information on any external support for banks to justify its decision making process.
- 14.8 To further mitigate risk the Council has decided that where counterparties form part of a larger group, group limits should be used in addition to single institutional limits. Group limits will be as set through the Council's Treasury Management Practices – schedules.
- 14.9 In relation to financial institutions, the Council currently only invests in UK banks and building societies, which provides sufficient high credit quality counterparties to meet investment objectives. It should be noted that in some cases these banks are subsidiaries of foreign banks, but these are of the highest credit quality.


15 External Service Providers

- 15.1 The Council uses Link Group as its external treasury management advisors. The Council recognises that responsibility for treasury management decisions remains with the authority at all times and will ensure that undue reliance is not placed upon our external service providers. All decisions will be undertaken with regards to available information, including, but not solely, our treasury advisors.
- 15.2 It also recognises that there is value in employing external providers of treasury management services in order to acquire access to specialist skills and resources. The Council will ensure that the terms of their appointment and the methods by which their value will be assessed are properly agreed and documented and subjected to regular review.
- 15.3 The scope of investments within the Council's operations now includes both conventional treasury investments, (the placing of residual cash from the Council's functions), and more commercial type investments, such as investment properties. The Council will engage specialist advisers for commercial-type investments.

INVESTMENTS AS AT 31/12/2023

BORROWER	AMOUNT £000	START DATE	MATURITY DATE	PERIOD IN DAYS	CURRENT INTEREST RATE %
Short Term Investments					
Barclays Bank*	3,450	16/06/14		Flexible Interest	4.85
National Westminster Bank	1,000	11/07/23	18/01/24	191	5.86
Lloyds Bank	1,000	20/07/23	18/01/24	182	5.59
Leeds Building Society	4,500	26/09/23	04/01/24	100	5.31
UK Debt Management Office	3,500	15/11/23	18/01/24	64	5.18
Yorkshire Building Society	3,000	01/12/23	22/02/24	83	5.11
Yorkshire Building Society	2,000	18/12/23	18/01/24	31	5.12
Total Short Term Investments	18,450				
Long Term Investments					
Property Funds (valuation at 31.12.23)	3,270	28th & 31/03/2022	N/A	N/A	3.87
Total Investments at 31/12/2022	21,720				

* Barclays Bank Call Account is operated on the basis of meeting more immediate/very short term needs of the Council eg. payment of salaries, suppliers, benefits etc. Therefore a level of balance is maintained dependent on the immediate and very short-term requirements of the Council.

Agenda Item No:	7	
Committee:	Audit and Risk Management	
Date:	12 February 2024	
Report Title:	Internal Audit Plan 2023-24 Progress Report Q3	

1 Purpose / Summary

- To report progress against the Internal Audit Plan 2023/24 for the third quarter of 1 October until 31 December 2023 and the resulting level of assurance from the planned work undertaken.
- To provide an update to members on the resourcing situation within the Internal Audit team.

2 Key issues

- The Council's Internal Audit Plan is produced on an annual basis. It is an estimate of the work that can be performed over the financial year. Potential areas of the Council for audit are prioritised based on a risk assessment, enabling the use of Internal Audit resources to be targeted at areas of emerging corporate importance and risk.
- The format of the plan reflects the Public Sector Internal Audit Standards (PSIAS) which were introduced in April 2016 and applicable from April 2017. It also incorporates the governance and strategic management arrangements of Internal Audit resources.
- Performance Standard 2060 of the PSIAS requires the Internal Audit Manager to report to the Committee on the Internal Audit activity and performance relative to this Plan.
- Audit and Risk Management Committee approved the Internal Audit Plan 2023/24 on 20 March 2023. It was updated following a detailed review in early Q2 and submitted and approved by the Committee on 26 September 2023.
- Members of the Audit and Risk Management Committee are keen to receive proactive performance reporting in relation to progress against the Internal Audit Plan on a quarterly basis.

- Proactive quarterly monitoring of the Internal Audit plan will enable the Committee to understand the Internal Audit activity which has successfully taken place and the associated assurance level.

3 Recommendations

For Members of Audit and Risk Management Committee to consider and note the activity and performance of the Internal Audit function.

Wards Affected	All
Forward Plan Reference	N/A
Portfolio Holder(s)	Councillor Chris Boden – Leader and Finance Portfolio Holder Councillor Kim French - Audit and Risk Management Committee Chairperson
Report Originator(s)	David Thacker – Interim Internal Audit Manager
Contact Officer(s)	Amy Brown – Assistant Director, Legal and Governance abrown@fenland.gov.uk 01354 622450 Peter Catchpole - Corporate Director & s151 Officer pcatchpole@fenland.gov.uk 01354 622201 David Thacker – Interim Internal Audit Manager
Background Paper(s)	Annual Risk-Based Internal Audit Plan 2023/24 Internal Audit Outturn and Quality Assurance Review 2022/23

1 Background / Introduction

- 1.1 This report includes details of the Internal Audit activity undertaken for the third quarter of 1 October to 31 December 2023.
- 1.2 The annual Internal Audit Plan is formulated in advance, following an assessment of risks inherent to services and systems of the Council based on Internal Audit and Management knowledge at that time. During the period that follows, changes in the control environment may occur due to, for example:
- introduction of new legislation/regulations;
 - changes of staff;
 - changes in software;
 - changes in procedures and processes; and
 - changes in service demand.
- 1.3 In respect of Internal Audit resources, the current situation is that there are three staff. The Head of Internal Audit and the full-time Auditor positions are currently filled by contractors, via agencies, with the contracts expiring on 31 March 2024. The other Auditor position is held by a part-time (term-time only) FTE, who has been with the Council since 2001 and in Internal Audit since 2008.
- 1.4 The Council intends to re-advertise the vacant Head of Audit and full-time Auditor positions in the new year. Management continues to review resourcing options including requesting assistance from other surrounding authorities, although it is understood that there is a shortage of suitable candidates in the area.

2 Monitoring

- 2.1 On completion of each audit a formal report is issued to the relevant Service Manager and Corporate Director. A copy is also sent to the Corporate Director – Finance (S151 Officer). Each report contains a management action plan, with target dates, that has been agreed with Service Managers to address any observations and recommendations raised by the Internal Auditor. Progress on recommendations is monitored on a regular basis and no less frequent than quarterly.
- 2.2 The following audits have been completed up to end of Q3 2023/24. (Appendix A)
- Public Health Funerals (22/23)
 - Licences – Animal Welfare (22/23)
 - Licences – Other (22/23)

- Corporate Assurance – Transparency
- Housing Options (22/23)
- Trading Operations – Cemetery Income
- Freedom of Information
- Safeguarding – Follow Up

2.3 The following audits are in progress and will be reported to the committee in future progress reports:

- Debtors & Collection Agency – being finalised.
- Port Berthings (Special Audit) – being finalised.
- ICT Cyber Security.
- Development – Planning (combined with Fee Income).
- Corporate Assurance – Information & Data Management.
- Emergency Planning & Business Continuity Planning.

2.4 In the third quarter of the year other work that Internal Audit has been involved to assist with and to provide additional assurance are detailed below:

- National Fraud Initiative work
- Risk Management Group
- Major Project support and advice
- Corporate Governance
- Following up outstanding recommendations

2.5 In respect of the last point, Appendix B shows the number of outstanding Audit issues from 2021/22 to 2023/23 to date. Internal Audit is working with Service Managers to ensure that recommendations are implemented by the agreed target dates or, if not, that requested date extensions can be justified. Status updates have been included where relevant.

Appendix A – Completed Audits 2023/24

Audit	Overall Opinion	High	Medium	Low	Issue Summary & Status (<i>in italics</i>)
<p>Public Health Funerals (2022/23)</p> <p>To gain assurance that the Council is fulfilling its obligation to provide a public health funeral as required and that robust policies and procedures are in place to ensure a recourse of public funds.</p>	Adequate	1	1	-	<p>The high-risk issue relates to unlimited access to the shared safe at the BASE where the small contents from the deceased are stored, e.g., cash, along with other service's items. <i>Completed.</i></p> <p>The medium risk relates to no updated procedures, a key person risk and no record of possessions removed from a deceased person's property. <i>An inventory is in place now. Key person risk and procedures will be addressed by February 2024.</i></p>
<p>Licensing – Animal Welfare (2022/23)</p> <p>To gain assurance that the Council has robust procedures for the licensing of activities involving animals.</p>	Substantial	-	-	-	No issues raised.
<p>Licensing – Other (2022/23)</p> <p>To gain assurance that the Council has robust procedures and guidance in place demonstrating appropriate issuance and monitoring of other licenses, such as scrap metal dealers and small lotteries.</p>	Adequate	-	1	-	<p>The medium risk issue relates to no control check in place for potential members of public or businesses operating without a licence for scrap metal, small society lotteries, street collections, house to house collections and gambling. <i>The process will be in place by January 2024.</i></p>

Appendix A – Completed Audits 2023/24

<p>Corporate Assurance – Transparency</p> <p>To gain assurance that the Council complies with the Local Government Transparency Code 2015.</p>	<p>Adequate</p>	<p>-</p>	<p>2</p>	<p>-</p>	<p>The medium risk issues relate to:</p> <ul style="list-style-type: none"> • A lack of updated information on the Council’s website that is not in compliance with the Local Government Transparency Code 2015. <i>Ten of the eleven data sets are now up to date. The only outstanding one is the Senior Salaries – last published as part of the Statement of Accounts 21/22 (awaiting publishing of the draft 22/23 accounts).</i> • Raising the profile of compliance with service managers for timely updates. <i>This will be completed by March 2024.</i>
<p>Housing Options (2022/23)</p> <p>To gain assurance that there are adequate controls and procedures in place for the monitoring, recording and payment of housing option services.</p>	<p>Adequate</p>	<p>-</p>	<p>4</p>	<p>-</p>	<p>The medium risk issues relate to:</p> <ul style="list-style-type: none"> • High usage of B&B and a considerable increase in hotel/hostel spend – over £1.2m since April 2020 – with no evidence of value for money. <i>6 properties have been leased from Clarion since June 2023 and 28 of the 29 LAHF properties have been purchased or are in the process of being purchased. All properties will be owned and occupied by June 2024.</i> • Non-compliance with the Council’s Code of Procurement in relation to services including accommodation, removal and storage and cleaning. <i>We are currently getting 3 quotes for storage and have a tender draft being finalised to go out to procure for emergency interim accommodation. Also, any accommodation</i>

Appendix A – Completed Audits 2023/24

					<p><i>provider in the area and neighbouring is welcome to offer accommodation during the interim of the procurement exercise for emergency interim accommodation as advertised openly on our website. Procurement for cleaning could be part of the corporate cleaning contract.</i></p> <ul style="list-style-type: none"> • <i>At the time of the audit fieldwork in 2022, there was a potential time limit breach of DLUHC guidance for housing 8 families over 6 weeks in B&B. However, the number reduced by 2023. There has only been one quarter where we were close to a breach, and we managed to work collectively to reduce that. With increased new delivery, improved RP void performance and a big increase in new tenancy agreements, this should be addressed.</i> • <i>An outdated homelessness strategy and guidance. To be implemented by September 2024.</i>
--	--	--	--	--	--

Appendix A – Completed Audits 2023/24

<p>Trading Operations – Cemetery Income</p> <p>To gain assurance that the administration of cemetery income is monitored and managed efficient and effectively.</p>	<p>Adequate</p>	<p>-</p>	<p>2</p>	<p>-</p>	<p>The medium risk issues relate to:</p> <ul style="list-style-type: none"> Disjointed invoice and debtors’ management between the Bereavement Team and Finance. <i>To be completed by February 2024.</i> A lack of updated procedures. <i>To be completed by February 2024.</i>
<p>Freedom of Information Act Requests</p> <p>To gain assurance that the Council has a robust framework in place demonstrating compliance with the Freedom of Information Act 2000.</p>	<p>Adequate</p>	<p>-</p>	<p>4</p>	<p>1</p>	<p>The medium risk issues relate to:</p> <ul style="list-style-type: none"> Outstanding and overdue FOI requests exceeding statutory timeframe. <i>Monitoring and escalation to be improved by March 2024.</i> Lack of Publication Scheme. <i>To be implemented by March 2024.</i> Lack of formal training and awareness. <i>To be implemented by December 2024.</i> Lack of performance reporting. <i>Completed.</i>
<p>Safeguarding Children & Vulnerable Adults – Follow Up</p> <p>A follow-up of the recommendations agreed in the systems-based review of Safeguarding Children and Vulnerable Adults performed in 2021/22.</p>	<p>Substantial</p>	<p>-</p>	<p>2</p>	<p>1</p>	<p>The medium risk issues both relate to relevant staff training for the revised policy – one at induction and the second every two years. <i>To be completed once the new HR platform has been implemented in April 2024.</i></p>

Appendix A – Completed Audits 2023/24

An assurance rating is applied, when a system or process is reviewed, which reflects the effectiveness of the control environment.

The text below is an indication of the different assurance ratings used:

Assurance	Description
Full	There is a sound system of control designed to proactively manage risks to objectives.
Substantial	There is a sound system of control, with further opportunity to improve controls which mitigate minor risks.
Adequate	There is a sound system of control, with further opportunity to improve controls which mitigate moderate risks.
Limited	There are risks without effective controls, which put the objectives at risk.
None	There are significant risks without effective controls, which put the objectives at risk. Fraud and/or error are likely to exist.

Appendix B – Recommendation Status 2020/21 to 2023/24

Total Recommendations 2020/21				
	High	Medium	Low	Total
Total Recommendations	3	21	23	47
Total Complete	3	20	23	46
Total Not Due	0	0	0	0
Overdue	0	1	0	1

NB. This data includes recommendations made from our ARP Audit Partners who conducted audits for the partnership. These have all been completed or superseded by the audits of 2021/22.

The overdue recommendation relates to CCTV. The Assistant Director stated that whilst the section 113 has been signed and completed, the Memorandum of Understanding (MOU) is in final draft and should be completed soon.

Total Recommendations 2021/22				
	High	Medium	Low	Total
Total Recommendations	4	31	34	69
Total Complete	4	26	30	60
Total Not Due	0	5	4	9
Overdue	0	0	0	0

NB. This table does not include the recommendations made in relation to the ARP audits, conducted by partner authorities as they are reported to their respective authorities at this stage.

The outstanding medium-risk issues relate to Safeguarding (training on the updated policy) and to Procurement (code of procurement & procurement strategy – awaiting new legislation later in 2024).

Total Recommendations 2022/23				
	High	Medium	Low	Total
Total Recommendations	5	13	13	31
Total Complete	3	12	13	28
Total Not Due	2	1	0	3
Overdue	0	0	0	0

NB. This table does not include the recommendations made in relation to the ARP audits, conducted by partner authorities as they are reported to their respective authorities at this stage.

The outstanding high-risk issues relate to Trading Operations – Port Commercial & Marine (no formal agreement with LCC for Cross Keys Marina, although the lease from LCC to FDC and sub- lease of part from FDC to EIFCA are in agreed form and ready to sign. This should be done by the end of February 2024) and the Construction

Appendix B – Recommendation Status 2020/21 to 2023/24

Industry Scheme – IR35 Compliance (the revised Recruitment COP was completed at the end of 2023 and is awaiting CMT approval).

The medium-risk issue relates to Cyber Security training, which is being reviewed again currently.

Total Recommendations 2023/24 (to date)				
	High	Medium	Low	Total
Total Recommendations	1	16	1	18
Total Complete	1	1	0	2
Total Not Due	0	15	1	16
Overdue	0	0	0	0

NB. This table does not include the recommendations made in relation to the ARP audits, conducted by partner authorities as they are reported to their respective authorities at this stage.

All outstanding issues are from current audits and are scheduled to be implemented in 2024.

This page is intentionally left blank

Agenda Item 8

Agenda Item No:	8	
Committee:	Audit and Risk Management Committee	
Date:	12th February 2024	
Report Title:	Regulation of Investigatory Powers Act (RIPA) – Update & Revised Policy	

Purpose / Summary

- This report is intended to provide members of the Audit and Risk Management Committee with an update on Fenland District Council's use of the Regulation of Investigatory Powers Act 2000 (RIPA) and to seek approval of a revised RIPA Policy.

Key issues

- Good practice suggests that the Councils Audit and Risk Management Committee (ARMC) should review the operational use of RIPA as well as undertaking any updates and amendments to the Council's RIPA Policy.
- The Council has used RIPA once since its activities were last reported to the ARMC on 22nd March 2023.
- The Council has completed a review of its RIPA Policy to ensure that it remains current and incorporates all recommended best practice.

Recommendations

That the Audit and Risk Management Committee is requested to:

- Note this annual report on the Council's use of RIPA; and
- Approve the amended RIPA Policy as set out at Appendix 1.

Portfolio Holder(s)	Cllr Chris Boden – Portfolio Holder for Finance
Report Originator(s)	Peter Catchpole – Corporate Director & s.151 Officer
Contact Officer(s)	Amy Brown – Assistant Director
Background Paper(s)	None

1 BACKGROUND

1.1 Local authorities exercise criminal investigation powers for numerous reasons e.g. fly tipping and planning enforcement. Officers are required to gather evidence to support their investigations and sometimes, it is necessary to do this via the use of surveillance.

1.2 RIPA and the Investigatory Powers Act 2016 (IPA2016) regulate the use of surveillance powers by public authorities including directed surveillance, the use of covert human intelligence sources (CHIS) and access to communications data.

1.3 Fenland District Council is a very rare user of these powers however, it is important that it has sufficient oversight of its activities to ensure that any considered use is compliant with the subject's human rights. Such surveillance is only lawful if the actions are necessary (to the required standard), proportionate, non-discriminatory, lawful and properly approved.

1.4 The types of activity regulated by RIPA and the IPA2016 include:

1.5 Directed Surveillance

1.6 This is covert surveillance conducted for the purpose of a particular investigation (which meets the relevant thresholds) or operation that is likely to result in the obtaining of private information about a person (and is not in immediate response to relevant events).

1.7 The relevant thresholds will be met if the covert surveillance is carried out for the purpose of preventing or detecting a criminal offence and it meets the serious crime test i.e. that the criminal offences which are sought to be prevented or detected are:

- Punishable whether on summary conviction or on indictment by a maximum term of at least 6 months of imprisonment; or
- Would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

1.8 Private information includes any aspect of a person's private or personal relationships with others including family and professional or business relationships. For example, covert surveillance might mean the use of CCTV to monitor an individual's movement or their actions. Whilst the CCTV camera itself is overt, it is the use of the camera to track that specific individual's actions without them knowing which makes it covert.

1.9 Directed surveillance is only permitted if authorised by a Justice of the Peace.

1.10 Covert Human Intelligence Sources

1.11 This is the practice of using an officer or 3rd party (such as adults and/or children in certain circumstances) for the purposes of establishing and maintaining a personal or other relationship with a person for the covert purpose of obtaining information. This could be an officer who builds a

relationship with an individual operating a business in order to gain evidence of an offence by that individual. It may also be the use of underage volunteers to purchase age restricted products.

- 1.12 The required criteria for the use of a CHIS to be authorised is for the 'prevention and detection of crime and the prevention of disorder'. The serious crime criteria do not apply to CHIS however their use also has to be approved by a Justice of the Peace at Magistrates Court.

1.13 Communications Data

- 1.14 Via the National Anti-Fraud Network (NAFN), the Council can require the release of communications data from communications service providers ("CSP") where appropriate circumstances exist. CSPs are anyone who provide a postal or telecommunications service e.g. Royal Mail, British Telecom, Vodafone etc.

- 1.15 Communications data is generated in the provision, delivery and maintenance of postal or telecommunications services but it does not include the content of the communication. For example, it is possible to obtain information which identifies the subscriber to a mobile phone and see the call history however, it is not possible to gain access to the actual content of the calls.

- 1.16 Councils only have the power to acquire the following data from CSP's:

- Billing, delivery and installation address;
- Contact telephone numbers;
- Periods of subscription use;
- Itemised telephone call records;
- Itemised records of connections to internet services;
- Provision, and use of forwarding/redirection services;
- Records of postal items, e.g. registered, recorded or special delivery postal items;
- Top up details for mobile phones, credit/debit card details and voucher top up details.

- 1.17 CSP's will only respond to requests from Council's via designated contacts who must have undertaken and passed a Home Office approved course. NAFN is a designated contact however, Fenland District Council does not currently subscribe to it and does not therefore directly acquire communications data however, the Anglian Revenues Partnership is a member of NAFN and can obtain data on our behalf in appropriate circumstances.

- 1.18 The ARP are required to report on their usage in support of this annual Report and in compliance with the Council's general record keeping requirements.

2 FENLAND DISTRICT COUNCIL AUTHORISED ACTIVITY

2.1 Details of the applications that Fenland District Council have made over the last 5 years are as follows:

2.2 **Directed Surveillance or Covert Human Intelligence Sources**

Description	2023/24	2019/20 – 2022/23
Number of Applications made	1	0
Number of Applications granted	1	0
Number of authorisations cancelled	1	0
Number of ongoing authorisations 2023/24.	0	0

2.3 Use of Acquisition and Disclosure of Communications Data

2.4 No applications for the disclosure of communications data were made during the municipal years 2019/20, 2020/21, 2021/22, 2022/23 and 2023/24.

2.5 There have been no reported instances of Fenland District Council having misused its powers under the relevant Acts.

3 INSPECTION AND REPORTING

3.1 The Council's continues to receive regular inspections from the Investigatory Powers Commissioner's Office (IPCO). The last inspection was carried out in March 2021 and the next inspection is due this year.

3.2 The Council takes account of IPCO's conclusions and recommendations when formulating and revising RIPA practice and Policy. The following recommendations were made at the conclusion of the last inspection:

- Implementation of a procedure for ensuring that all online activity is recorded and periodically scrutinised for oversight purposes; and
- Internal guidance, at practitioner level, to instruct staff on how to implement the safeguards in an operational context. This to be achieved by amplifying the existing instructions in the RIPA Policy.

3.3 All of the necessary preparation for the next inspection is underway and the proposed changes to the RIPA Policy as set out in this Report are designed to address the recommendations made following the previous inspection.

3.4 In addition to inspections, IPCO require the submission of annual statistical data each year for the purpose of compiling their annual report as well as for the Council to arrange for training to be carried out once in every three-year period:

3.5 IPCO's Annual Report is published on its website via the following link: [HC 910 – Investigatory Powers Commissioner's Office – Annual Report of the Investigatory Powers Commissioner 2021 \(ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com\)](https://www.ipco.gov.uk/annual-report) (the last report at the time of writing published 20 March 2023). Part 15 provides the findings in relation to local authorities.

Since the time of last reporting, updated training has been provided to all relevant officers. In that regard, training was provided to enforcement officers and heads of service during Autumn 2022 and SIRO/Authorising Officer took place on 15th March 2023. The Council has committed to a bi-annual training program and talks are already underway as regards the potential inclusion of updated training in the corporate plan for the municipal year 2024/25.

4 RIPA POLICY REVIEW

4.1 The Council's current RIPA Policy was approved in September 2019 and a revised version is attached to this Report at Schedule 1. The RIPA Policy has been the subject of a full review with input from investigating officer colleagues. The paragraphs of the RIPA Policy which have been significantly amended/added to have been highlighted in yellow and the following table also provides an overview:

Page	Description	Reason
3-5	Index	The Index has been updated where required to reflect the changes made within the main body of the document.
6	Codes of Practice	The Policy has been updated to make specific reference to the Codes of Practice which provide further practical guidance. A link to the most up-to-date version of the Codes has also been included for ease of access.
6-7	Defined Roles	Updated information has been included about the key responsibilities of each of the core roles required to support the lawful implementation of the Policy.
	Useful Websites	Updated links to useful websites has been included.
8	Scope – paragraph 2.3	Additional wording has been added to reflect updates to the Policy which incorporate information about the Council's position/expectations in relation to the use of surveillance which falls outside the scope of RIPA.
	Scope – paragraph 2.4	Updated legislative references.
	Scope – paragraph 2.5	Specific inclusion of a description and link to the Codes of Practice.
9	Consequences	Inclusion of additional wording to make very clear that it is a requirement of Fenland District Council to comply with the Policy

Page	Description	Reason
		regardless of the legal position.
10	Independent Oversight – paragraph 5.1	Full title of IPCO.
	Independent Oversight – paragraph 5.2	Inclusion of a link to IPCO’s website and useful guidance.
	Council Oversight – paragraph 6	Confirming that information relating to the use of RIPA and updates to the Policy etc will be presented to the ARMC and senior management.
	Training – paragraph 7	Inclusion of a paragraph which confirms the Council’s commitment to providing training/refresher training.
11	Basic Determination – Paragraph 9	Inclusion of a Q&A Table which provides a practical and straightforward means of identifying whether RIPA is likely to apply.
12	Overt Surveillance – paragraph 10.2.1	Inclusion of reference to data protection legislation.
	Covert Surveillance – paragraph 10.3	Inclusion of the specific Code reference where the definition of covert surveillance can be found.
13	Intrusive Surveillance – paragraph 11	Inclusion of wording to make absolutely clear the Council’s expectations with regard to intrusive surveillance and that it should not be used in any circumstance.
	Directed Surveillance -paragraph 12.1	Wording included to make clear that the use of directed surveillance is only permissible if it is compliant.
14	Private Information – paragraph 13.6	Inclusion of specific Code reference where the definition of non-private information can be found.
15-16	Confidential/Privileged Information	Updated paragraphs regarding the requirements in relation to confidential/privileged information and the additional requirements which will apply.
16	Lawful Grounds/Crime Threshold – paragraph 15	Inclusion of the words ‘Crime Threshold’ to link in with other wording included in the Policy.

Page	Description	Reason
	General Observation Activities – paragraph 16	Inclusion of a section about general observations and giving examples of how to distinguish when an authorisation may be required.
17	Test Purchases – paragraph 17.1	Inclusion of examples about when the use of a juvenile will require a CHIS organisation in a test purchase scenario.
	Test Purchases – paragraph 17.2	Inclusion of wording which makes clear that other means of obtaining the same information should first be considered.
18	Urgent Cases – paragraph 18.2	Confirming the process for urgent surveillance.
19-21	Internet and Social Media Investigations – paragraph 22.1 (in the context of direct surveillance)	This section of the policy has been further developed to provide more information about when the use of the internet/social media is more likely to require an authorisation or not. It also requires that the use of the internet/social media (whether or not an authorisation is required) is fully documented using the template form. This provision has been specifically included to meet the recommendations arising from the previous inspection.
21	Surveillance Outside RIPA – paragraph 23	A sentence has been added to make clear that officers should record and be able to demonstrate their thought processes as to how something is outside RIPA and therefore why an authorisation was not considered necessary.
22	Disciplinary Investigations – paragraph 24	A sentence has been included to confirm that advice should be sought and who that advice can be obtained from.
25	CHIS – Introduction – Paragraph 28.4	New paragraph inserted to confirm the required authorisations for a CHIS.
	Definition of CHIS – paragraph 29.1	Inclusion of specific Code reference which defines a CHIS.
26-27	Definition of CHIS – paragraph 29.4	Inclusion of a table which gives practical examples of when a CHIS authorisation may

Page	Description	Reason
		or may not be required.
27 – 28	Vulnerable and Juvenile CHIS – paragraph 30	Paragraphs included to provide additional guidance as to the use of vulnerable and juvenile CHIS; the steps that must be complied with, what is prohibited and the use of appropriate adults.
30-31	Risk Assessments, Security and Welfare – paragraph 36	Includes updated paragraphs about the need to risk assess CHIS arrangements at the outset and keep that risk assessment under review as appropriate.
32	Operation Involving Multiple CHIS – paragraph 39	Inclusion of guidance as to the ability to authorise multiple CHIS and when this may or may not be appropriate.
32-34	Social Media Consideration – paragraph 40 (in the context of CHIS)	This section of the policy has been further developed to provide more information about when a CHIS authorisation might be required for interactions via the internet/social media is more likely to require an authorisation or not and the authorisation requirements of such an arrangement including risk assessments. This provision has been specifically included to meet the recommendations arising from the previous inspection.
42	Other Factors – paragraph 50	Confirms the requirement not to undertake surveillance which would interfere with spiritual counselling (and defines this) as well as including a requirement to ensure that any other sensitivities are identified and considered as appropriate.
43	Duration of Authorisations – paragraph 52.3	Confirms again that more than one CHIS can be authorised via one authorisation provided the relevant requirements are met.
47	Renewal – paragraph 59	Paragraph included to confirm that an authorisation should not be allowed to lapse. A decision to either cancel or renew should be actively taken.
54-55	Handling of Retention Material – paragraph 66	Paragraphs updated to include confirmation that the storage and processing of data obtained under an authorisation must be

Page	Description	Reason
		compliant with information governance legislation and the Council's related policies and guidance. Must be retained where there are ongoing proceedings and must be kept securely. The retention and destruction of data to be kept routinely under review. Also to incorporate new Guidance which has been specifically included to meet the recommendations arising from the previous inspection.
55	Dissemination of Information – paragraph 68	Paragraph added to confirm the care that needs to be taken when sharing data with other individuals within the Council or other enforcement agencies.
59-60	Part I – Relevant Case Law	New section inserted to provide information about case-law which is relevant to decision making under the Policy.

4.2 The entries annotated in red incorporate into the RIPA Policy amendments reflecting the practices which have been developed to specifically meet the recommendations of the IPCO inspector following the last inspection.

5 REASONS FOR RECOMMENDATIONS

5.1 It is requested that members of the Audit and Risk Management Committee agree the recommendations set out in this Report in order to ensure that Fenland District Council is compliant with its responsibilities under the relevant legislation, associated Codes and guidance and IPCO inspection requirements.

6 CONSULTATION

6.1 There are no specific consultation requirements connected with the recommendations comprised within this Report however, in developing the revised RIPA Policy, input has been sought from relevant internal and external colleagues and advisors.

7 ALTERNATIVE OPTIONS CONSIDERED

7.1 It is a constitutional requirement reflecting recommended best practice for the Audit and Risk Management Committee to receive an annual report relating to the Council's activity under the relevant Acts as well as any proposed updates to the RIPA Policy and updated training etc. There are therefore no recommended alternatives to this requirement.

- 7.2 It is necessary to conduct routine updates of the RIPA Policy and there are various amendments/improvements which can be made at any one time. The current recommendations reflect best practice as it currently stands and as advised following the last inspection. The alternative of not amending the RIPA Policy is not advisable as it would inhibit a clear and consistent message being provided to all relevant stakeholders in the process.

8 IMPLICATIONS

8.1 Legal Implications

- 8.2 The legal implications are as set out in the main body of this Report and the associated RIPA Policy.

8.3 Financial Implications

- 8.4 There are no significant financial implications associated with the recommendations set out within this Report. The RIPA Policy requires an ongoing financial commitment to resourcing its operation by relevant officers and the associated training.

8.5 Equality Implications

- 8.6 In line with the Public Sector Equality Duty, public bodies must, in the exercise of their functions, give due regard to the need to eliminate discrimination, harassment, victimisation, to advance equality of opportunity and foster good relations between those who share a protected characteristic and those who do not.
- 8.7 The contents of this report do not directly impact on equality, in that it is not making proposals that will have a direct impact on equality of access or outcomes for diverse groups.

9 SCHEDULES

Schedule 1: Amended RIPA Policy

Regulation of Investigatory Powers Act 2000

(RIPA)

Policy and Guidance

Document Control

Purpose of document:	The approach to the use of RIPA powers and the process followed by Fenland District Council
Intended audience:	Officers who may use directed covert surveillance or covert human intelligence sources as part of an investigation
Type of document:	Policy and Procedure
Document lead/author	
Other documents that link to this one:	Data Protection Policy ICT Acceptable Use Policy Social Media Guidance for Members Social Media Guidance for Employees Data Retention Policy
Document ratified/approved by:	
Version number:	
Issue date:	
Dissemination method:	
Date due for review:	
Reviewers:	

DOCUMENT REVISION RECORD:

Description of amendments:	Version No.	Date of re-approval and re-issue

Contents

Table of Contents

PART A	Introduction & RIPA General	6
1.	Introduction	6
1.2	Who to contact for advice?	6
1.3	Useful Websites	7
2.	Scope of Policy	7
3.	Background to RIPA and Lawful Criteria	8
4.	Consequences of Not Following RIPA	9
5.	Independent Oversight	10
6.	Council oversight	10
7.	Training	10
PART B	Surveillance, Types and Criteria	11
8.	Introduction	11
9.	Basic determination of RIPA	11
10.	Surveillance Definition	12
10.2.	Overt Surveillance	12
10.3.	Covert Surveillance	12
11.	Intrusive Surveillance	13
12.	Directed Surveillance Definition	13
13.	Private Information	14
14.	Confidential or Privileged Material	15
15.	Lawful Grounds/Crime Threshold	16
17.	Test Purchases	17
18.	Urgent Cases	17
19.	Surveillance for Preventing Disorder	18
20.	CCTV	18
21.	Automatic Number Plate Recognition (ANPR)	19
22.	Internet and Social Media Investigations	19
23.	Surveillance Outside of RIPA	21
24.	Disciplinary Investigations	22
25.	Joint Agency Surveillance	23
26.	Use of Third-Party Surveillance	23
27.	Surveillance Equipment	23
PART C.	Covert Human Intelligence Sources (CHIS)	25
28.	Introduction	25
29.	Definition of CHIS	25
30.	Vulnerable and Juvenile CHIS	27
31.	Lawful Criteria	28
32.	Conduct and Use of a Source	28
33.	Handler and Controller	29
34.	Undercover Officers	30
35.	Tasking	30
36.	Risk Assessments, Security and Welfare	30
37.	Use of Equipment by a CHIS	31
38.	CHIS Management	32
39.	Operation Involving Multiple CHIS	32
40.	Social Media considerations	32
40.1	Considering a Covert Human Intelligence Source (CHIS) authorisation in social media/internet investigations	32
40.2	Tasking someone to use a profile for covert reasons	33

40.3	Registering to Access a Site	33
40.4	Use of Likes and Follows	33
40.4	The identity Being Used	34
40.5	Risk Assessment	34
41.	CHIS Record Keeping	34
41.1	Centrally Retrievable Record of Authorisations	34
41.2	Individual Source Records of Authorisation and Use of CHIS	35
41.3.	Further Documentation	36
PART D.	RIPA Roles and Responsibilities	37
42.	The Senior Responsible Officer (SIRO)	37
43.	RIPA Co-Ordinator	37
44.	Managers Responsibility and Management of the Activity	38
45.1.	Investigating Officers/Applicant	38
46.	Authorising Officers	38
47	Necessity	39
48.	Proportionality	40
49.	Collateral Intrusion	41
50	Other Factors	42
50.1	Spiritual Counselling	42
50.2	Community Sensitivities	42
PART E.	The Application and Authorisation Process	43
51.	Relevant Forms	43
52.	Duration of Authorisations	43
53.	Applications/Authorisation	44
54.	Arranging the Court Hearing	45
55.	Attending the Hearing	45
56.	Decision of the Justice of the Peace (JP)	45
57.	Post Court Procedure	46
58.	Reviews	46
59.	Renewal	47
60.	Cancellation	48
Part F	Acquisition of Communications Data	50
61.	Introduction	50
62.	Application procedure	51
Part G	Central Record and Safeguarding the Material	52
62.	Introduction	52
63.	Central Record	52
64.	Safeguarding and the Use of Surveillance Material	53
65.	Authorised Purpose	53
66.	Handling and Retention of Material	54
67.	Use of Material as Evidence	55
68.	Dissemination of Information	55
69.	Storage	56
70.	Copying	56
71.	Destruction	56
Part H.	Errors and Complaints	57
72.	Errors	57
73	Relevant Error	57
74.	Serious Errors	57
75.	Complaints	58
PART I	Relevant case law	59
76.1	R v Johnson	59

76.2	R v Sutherland 2002.....	59
76.3	Peck v United Kingdom [2003]	59
76.4	Martin v. United Kingdom [2004] European Court App	59
76.5	R v. Button and Tannahill 2005	60
76.6	C v The Police and the Secretary of State for the Home Department (2006, No: IPT/03/32/H).....	60
76.7	AB v Hampshire Constabulary (Investigatory Powers Tribunal ruling 5 February 2019) 60	
76.8	Gary Davies v British Transport Police (Investigatory Powers Tribunal 5 February 2019)	60
	APPENDIX 1 Procedure for Directed Surveillance Application.....	61
	APPENDIX 2 Procedure use of Covert Human Intelligence Source	62
	APPENDIX 3 Surveillance Assessment	63
	APPENDIX 4 - Social Media/Internet Access Log	65
	APPENDIX 5.....	66

PART A Introduction & RIPA General

1. Introduction

- 1.1 The performance of certain investigatory functions of Local Authorities may require the surveillance of individuals or the use of undercover officers and informants. Such actions may intrude on the privacy of individuals and can result in private information being obtained and as such, should not be undertaken without full and proper consideration. The Regulation of Investigatory Powers Act 2000 (RIPA) governs these activities and provides a means of ensuring that they are carried out in accordance with law and subject to safeguards against abuse.

All surveillance activity can pose a risk to the Council from challenges under the Human Rights Act (HRA) or other processes. Therefore, it must be stressed that all staff involved in the process must take their responsibilities seriously which will assist with the integrity of the Council's processes, procedures and oversight responsibilities.

In preparing this policy the Council has followed the RIPA Codes of Practice (December 2022) and Investigatory Powers Commissioner Commissioners (IPCO) guidance.

There are Home Office Codes of Practice that expand on this guidance and copies are held by each Authorising Officer. They can be accessed [here](#) and officers should ensure that they are consulting the latest version.

The Codes do not have the force of statute but are admissible in evidence in any criminal and civil proceedings. As stated in the Codes, "if any provision of the Code appears relevant to a question before any Court or tribunal considering any such proceedings, or to the tribunal established under RIPA, or to one of the commissioners responsible for overseeing the powers conferred by RIPA, it must be taken into account".

1.2 Who to contact for advice?

If having read this document you are unclear about any aspect of the process or need support then you should contact one of the following officers:

- Sam Anthony, Approved Authorising Officer - SAnthony@fenland.gov.uk;
- Peter Catchpole, Approved Authorising Officer - PeterCatchpole@fenland.gov.uk;
- Amy Brown, RIPA Coordinator – amybrown@fenland.gov.uk;
- Carol Pilson, Senior Responsible Officer (SRO) - cpilson@fenland.gov.uk;

These roles are defined in greater detail in [Section D](#), however the below provides a summary.

Senior Responsible Officer – a Senior Responsible Officer (SRO) provides senior management oversight of the use of RIPA and provides assurance and integrity for the process. This will include oversight of authorisations, errors, reporting, training and inspection.

RIPA Coordinator will maintain the central registers for covert surveillance and communications data and is responsible for coordinating of training, updates of policies, procedures and inspections in conjunction with the Head of HR/OD.

Authorising Officer (RIPA) – the Code of Practice requires that an Authorising Officer must be of service manager or above rank however the Council's approach taken is to consider Authorising Officers at head of service level as a minimum. In order to be an authorising officer, the individual must be named in this Policy. An Authorising Officer will consider the application made under RIPA. They will consider the information provided by the applicant and determine whether there is necessity and proportionality in authorising the surveillance request.

1.3 Useful Websites

General Guidance from the Investigatory Powers Commissioner's Office	https://www.ipco.org.uk/
Home Office guidance to local authorities on the judicial approval process for RIPA and the crime threshold for directed surveillance	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf
RIPA Forms	https://www.gov.uk/guidance/surveillance-and-counter-terrorism
Covert surveillance and property interference Code of Practice	https://www.gov.uk/government/collections/ripa-codes
Interception of Communications Code of Practice	https://www.gov.uk/government/collections/ripa-codes
Covert Human Intelligence Sources Code of Practice	https://www.gov.uk/government/collections/ripa-codes

2. Scope of Policy

- 2.1 The purpose of this Policy is to ensure there is a consistent approach to the undertaking and authorisation of surveillance activity that is carried out by the Council. This includes the use of undercover officers and informants, known as Covert Human Intelligence Sources (CHIS). This will ensure that the Council complies with the Regulation of Investigatory Powers Act 2000 (RIPA).
- 2.2 This document provides guidance on the authorisation processes and the roles of the respective staff involved.

- 2.3 The Policy also provides guidance on surveillance which may be necessary to be undertaken by the authority but it falls outside of the scope of the RIPA legislation. This type of surveillance will still need to be considered as necessary and proportionate to what it seeks to achieve and be compliant with the Human Rights Act. (See Section 21).
- 2.4 The policy also identifies the cross over with other policies and legislation, particularly with data protection legislation including the UK General Data Protection Regulation, the Data Protection Act 2018 (including Part 3 “Law Enforcement Processing”) and the Criminal Procedures & Investigations Act 1996.
- 2.5 All RIPA covert activity will have to be authorised and conducted in accordance with this Policy, the RIPA legislation and Codes of Practice. Therefore, all officers involved in the process will have regard to this document and the statutory RIPA Codes of Practice issued under section 71 RIPA for both Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS). The Codes of Practice are available from:

Covert surveillance and property interference Code of Practice	https://www.gov.uk/government/collections/ripa-codes
--	---

Interception of Communications Code of Practice	https://www.gov.uk/government/collections/ripa-codes
---	---

Covert Human Intelligence Sources Code of Practice	https://www.gov.uk/government/collections/ripa-codes
--	---

3. Background to RIPA and Lawful Criteria

- 3.1 On 2nd October 2000 the Human Rights Act 1998 (HRA) came into force making it potentially unlawful for a Local Authority to breach any article of the European Convention on Human Rights (ECHR).
- 3.2 Article 8 of the European Convention on Human Rights states that: -
- 1) Everyone has the right of respect for his private and family life, his home and his correspondence.
 - 2) There shall be no interference by a Public Authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protection of the rights and freedoms of others.
- 3.3 The right under Article 8 is a qualified right and Public Authorities can interfere with this right for the reasons given in 3.2 (2) above if it is necessary and proportionate to do so.

- 3.4 Those who undertake Directed Surveillance or CHIS activity on behalf of a Local Authority may not breach an individual's Human Rights, unless such surveillance is **lawful**, consistent with Article 8 of the ECHR and is both **necessary** (see Part D section 43) and **proportionate** (see Part D section 44) to the matter being investigated.
- 3.5 RIPA provides the legal framework for lawful interference to ensure that any activity undertaken, together with the information obtained, is HRA compatible.
- 3.6 However, under RIPA, Local Authorities can now only authorise Directed Surveillance for the purpose of preventing or detecting conduct which constitutes a criminal offence which is punishable (whether on summary conviction or indictment) by a maximum term of at least six month's imprisonment; (serious crime criteria) or involves the sale of alcohol or tobacco to children. (See Part B Section 15).
- 3.7 The **lawful criteria for CHIS** authorisation is **prevention and detection of crime and prevention of disorder**. The serious crime criteria of the offence carrying a 6-month sentence etc. does not apply to CHIS.
- 3.8 In either event, the Council's authorisation can only take effect once an Order approving the authorisation has been granted by a Justice of the Peace (JP).
- 3.9 RIPA ensures that any surveillance which is undertaken following a correct authorisation and approval from a Justice of the Peace is lawful. Therefore, it protects the authority from legal challenge. It also renders evidence obtained lawful for all purposes.

4. Consequences of Not Following RIPA

- 4.1 Although not obtaining authorisation does not make the authorisation unlawful per se, **it is a requirement of Fenland District Council and this Policy** and it does have significant consequences: -
- Evidence that is gathered may be inadmissible in court;
 - The subjects of surveillance can bring their own claim on Human Rights grounds i.e. we have infringed their rights under Article 8;
 - If a challenge under Article 8 is successful, the Council be subject to reputational damage and could face a claim for financial compensation;
 - The Government has also introduced a system of tribunal to deal with complaints. Any person who believes that their rights have been breached can have their complaint dealt with by the Investigatory Powers Tribunal (IPTC) (See Complaints Part G section 67)
 - It is likely that the activity could be construed as an error and therefore have to be investigated and a report submitted by the Senior Responsible Officer to the Investigatory Powers Commissioner's Office (IPCO). (See Part G Section 66 Errors),

5. Independent Oversight

- 5.1 RIPA is overseen by the Investigatory Powers Commissioner's Office (IPCO). They are the independent inspection office whose remit includes providing comprehensive oversight of the use of the powers to which the RIPA code applies, and adherence to the practices and processes described in it. They also provide guidance to be followed which is separate to the codes.
- 5.2 They have unfettered access to all locations, documentation and information systems as is necessary to carry out their full functions and duties and they will periodically inspect the records and procedures of the Council to ensure the appropriate authorisations have been given, reviewed, cancelled, and recorded properly. Their website provides good general guidance, <https://www.ipco.org.uk/>.
- 5.3 It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information they require for the purpose of enabling them to carry out their functions. Therefore, it is important that the Council can show it complies with this Policy and with the provisions of RIPA.

6. Council oversight

- 6.1 The use of RIPA powers will be a standing item on the agenda for the Audit and Risk Management Committee. An annual report will be produced detailing the usage along with any inspections, changes to policy and procedure.
- 6.2 An annual report will be produced for Senior Management detailing the usage along with any inspections, changes to policy and procedure.

7. Training

- 7.1 There will be a bi-annual programme of training for officers, which may include face to face or e-learning training. Refresher training will be provided on a biannual basis. Officers may be required to confirm they have read documentation and have understood the intervening times.
- 7.2 Only formally trained Authorised Officers will be permitted to authorise applications.

PART B Surveillance, Types and Criteria

8. Introduction

8.1 It is important to understand the definition of surveillance; what activities are classed as surveillance and the different types of surveillance covered by RIPA and the HRA. Surveillance can be both overt and covert and depending on their nature, are either allowed to be authorised under RIPA or not. There are also different degrees of authorisation depending on the circumstances.

9. Basic determination of RIPA

It is critical that prior to any activity being undertaken, the requesting officer and an Authorising Officer undertake an assessment of the activity proposed.

This assessment should follow the procedure as detailed below.

Question	Answer	Notes
1. Is the surveillance activity covert?	Yes – proceed to question 2	This means that a subject is unaware of the activity due to the way it being undertaken
2. Is the surveillance directed?	Yes – proceed to question 3	This means that the activity is for a specific investigation or purpose
3. Is the investigation into a criminal offence?	Yes – proceed to question 4	If it is not an investigation into the alleged commission of a criminal offence then RIPA does not apply however you should always be able to show that you have considered whether RIPA does apply.
4. Are you likely to obtain confidential or private information	Yes – proceed to question 5	If you are not likely to obtain such information then RIPA does not apply.
5. Does the offence meet the crime threshold?	If yes then RIPA applies	If it does not then RIPA does not apply however you should always be able to show that you have considered whether RIPA does apply.

10 . Surveillance Definition

10.1 Surveillance is:

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

10.2. Overt Surveillance

10.2.1 Overt surveillance is where the subject of surveillance is aware that it is taking place. Either by way of signage such as in the use of CCTV or because the person subject of the surveillance has been informed of the activity. Overt surveillance is outside the scope of RIPA and therefore does not require authorisation. However, it still must take account of privacy under the Human Rights Act and be necessary and proportionate. Any personal data obtained will also be subject to **data protection legislation**.

10.3. Covert Surveillance

10.3.1 **Paragraph 2.2 of the Covert Surveillance and Property Interference Revised Code of Practice defines** Covert Surveillance as “surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place” and is covered by RIPA. Covert surveillance is categorised as either **intrusive** or **directed**.

10.3.2 There are three categories of covert surveillance regulated by RIPA: -

- 1) **Intrusive surveillance** (Local Authorities are not permitted to carry out intrusive surveillance).
- 2) **Directed Surveillance;**
- 3) **Covert Human Intelligence Sources (CHIS).**

11. Intrusive Surveillance

- 11.1 **Fenland District Council has no authority in law to carry out Intrusive Surveillance and under no circumstance should any officer or other representative of the Council attempt to use it.**

It is only the Police and other law enforcement agencies that can lawfully carry out intrusive surveillance.

- 11.2 Intrusive surveillance is defined in section 26(3) of the 2000 Act as covert surveillance that:

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

- 11.3 Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises, would not be considered as intrusive surveillance.

- 11.4 A risk assessment of the capability of equipment being used for surveillance on residential premises and private vehicles, such as high-powered zoom lenses, should always be carried out to ensure that its use does not meet the criteria of Intrusive Surveillance.

12. Directed Surveillance Definition

- 12.1 The Council can lawfully carry out Directed Surveillance **provided that it is compliant with the requirements set out in this Policy**. Surveillance is Directed Surveillance if the following are all true:

- It is covert, but not intrusive surveillance;
- It is conducted for the purposes of a specific investigation or operation;
- It is likely to result in the obtaining of private information (see private information below) about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- It is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought.

13. Private Information

- 13.1 By its very nature, surveillance may involve invading an individual's right to privacy. The level of privacy which individuals can expect depends upon the nature of the environment they are in at the time. For example, within an individual's own home or private vehicle, an individual can expect the highest level of privacy. The level of expectation of privacy may reduce if the individual transfers out into public areas.
- 13.2 The Code of Practice provides guidance on what is private information. They state private information includes any information relating to a person's private or family life. As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationships.
- 13.3 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a Public Authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognizing that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.
- 13.4 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, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a Directed Surveillance authorisation may be considered appropriate.
- 13.5 Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a Directed Surveillance authorisation is appropriate.
- 13.6 Paragraph 3.3 of the Covert Surveillance and Property Interference Code of Practice confirms that information which is non-private may include publicly available information such as, books, newspapers, journals, TV and radio broadcasts, newswires, websites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public.
- 13.7 There is also an assessment to be made regarding the risk of obtaining collateral intrusion which is private information about persons who are not subjects of the surveillance (see Part D section 45).

14. Confidential or Privileged Material

- 14.1 Consideration should be given in cases where the subject of the investigation or operation might reasonably assume a high degree of confidentiality. This includes:
- where material contains confidential personal information or communications between a Member of Parliament and another person on constituency business. (9.29 to 9.35 of the Covert Surveillance and Property Interference Code of Practice);
 - confidential journalistic material or where material identifies a journalist's source, (9.36 to 9.46 of the Covert Surveillance and Property Interference Code of Practice);
 - where the material contains information that is legally privileged, (9.47 to 9.75 of the Covert Surveillance and Property Interference Code of Practice).
- 14.2 Guidance on each of these can be found in the Revised Codes of Practice as noted above. In the event that these types of information may be or are likely to be acquired, officers should consult the Revised Codes of Practice, the SIRO and RIPA Coordinator.
- 14.3 Directed surveillance likely or intended to result in the acquisition of knowledge of confidential or privileged material **may be authorised only by the Chief Executive (or their appointed deputy in their absence) and shall be sought by via the Authorising Officer in consultation with the SIRO.**
- 14.4 In cases where the likely consequence of the conduct of a Covert Human Intelligence Source would be for any person to acquire knowledge of confidential material, the deployment of the Covert Human Intelligence Source **may be authorised only by the Chief Executive (or a deputy in their absence) and shall be sought via the Authorising Officer in consultation with the SIRO.**
- 14.5 In general, any application for an authorisation which is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.
- 14.6 The following general principles apply to confidential material acquired under properly approved authorisations:
- Those handling material from such operations should be alert to anything that may fall within the definition of confidential material. If there is doubt as to whether the material is confidential, advice should be sought before further dissemination takes place.
 - Confidential material should not be retained or copied unless it is necessary for a specified purpose;
 - Confidential material should be disseminated only where the requesting officer (having sought advice) is satisfied that it is necessary for a specific purpose.

14.7 The retention of dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information.

14.8 Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose. **This should only be with the approval of the Chief Executive and Senior Responsible Officer.**

15. Lawful Grounds/**Crime Threshold**

151 The Lawful Grounds for Directed Surveillance is a higher threshold for Local Authorities and cannot be granted unless it is to be carried out for the purpose of preventing or detecting a criminal offence(s) and it meets the serious crime test i.e. that the criminal offence(s) which is sought to be prevented or detected is:

- 1) Punishable, whether on summary conviction or on indictment, by a maximum term **of at least 6 months of imprisonment**, or,
- 2) Would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933 (see 1.4 above). This is the only ground available to the Council and hence the only justification.

15.2 Preventing or detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences.

16. **General Observation Activities – When Might Authorisation Not be Required?**

16.1 The general observation duties of council officers will not require authorisation under RIPA whether covert or overt. Such duties form part of the functions we are required to provide as opposed to pre-planned surveillance of a person or group. Paragraph 3.33 of the Covert Surveillance and Property Interference Code of Practice provides some examples of when an authorisation may not be required.

Example 1: Plain clothes police officers on patrol to monitor a fly tipping hot-spot or prevent and detect it would not require a directed surveillance authorisation. Their objective is merely to observe a location and, through reactive approach, to identify offenders committing crime. The activity may be part of a specific investigation but is general observational activity, rather than surveillance of individuals, and the obtaining of private information is unlikely. **A directed surveillance authorisation need not be sought.**

Example 2: Surveillance officers intend to follow and observe Z covertly as part of a pre-planned operation to determine their suspected involvement in flytipping. It is proposed to conduct covert surveillance of Z and record their activities as part of the investigation. In this case, private life considerations are likely to arise where there is an expectation of privacy and the covert surveillance is pre-planned and not part of general observational duties or reactive policing. **A directed surveillance authorisation should therefore be considered.**

17. Test Purchases

- 17.1 Test purchase activity does not in general require authorisation as a CHIS under RIPA as vendor-purchaser activity does not normally constitute a relationship as the contact is likely to be so limited. However, if a number of visits are undertaken at the same establishment to encourage familiarity, a relationship may be established and authorisation as a CHIS should be considered. If the test purchaser is wearing recording equipment and is not authorised as a CHIS, or an adult is observing, consideration should be given to granting a Directed Surveillance authorisation.

Example of CHIS authorisation not needed	Example of CHIS authorisation needed
<p>Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A juvenile is engaged and trained by a public authority and then deployed in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the 2000 Act that a public authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to granting a directed surveillance authorisation.</p>	<p>In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to juveniles from a room at the back of the shop, providing they have first got to know and trust them. As a consequence the public authority decides to deploy its operative on a number of occasions, to befriend the shopkeeper and gain their trust, in order to purchase alcohol. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained.</p>

- 17.2 When conducting covert test purchase operations at more than one establishment, it is not necessary to construct an authorisation for each premise to be visited but the intelligence must be sufficient to prevent “fishing trips”. Premises may be combined within a single authorisation provided that each is identified at the outset. Necessity, proportionality, and collateral intrusion must be carefully addressed in relation to each of the premises. An application would need to demonstrate that covert activities are considered proportionate and demonstrate that other/overt methods have been considered or attempted and failed.

18. Urgent Cases

- 18.1 As from 1 November 2012 there is no provision for urgent oral authorisations under RIPA as all authorisations have to be approved by a J.P. If surveillance was required to be carried out in an urgent situation or as an immediate response, this would still have to be justified as necessary and proportionate under HRA. This type of surveillance is surveillance outside of RIPA.

- 18.2 It is recognised that council officers find themselves in situations where they need to carry out some form of surveillance without the time to complete a form and obtain authorisations (see also paragraph 24). In these instances, the officer should obtain authorisation from their line manager and also record their reasons, actions, what was observed and be prepared to explain their decisions. These should be reported to the appropriate Senior Responsible Officer.

19. Surveillance for Preventing Disorder

- 19.1 Authorisation for the purpose of preventing disorder can only be granted if it involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment. Surveillance for disorder not meeting these criteria would need to be carried out as surveillance outside of RIPA. (See below)

20. CCTV

- 20.1 CCTV is now known as a Surveillance Camera Systems (Section 29(6) Protection of Freedoms Act 2012). The Surveillance Camera Code of Practice 2013 defines a 'surveillance camera system' as:

- any other systems for recording or viewing visual images for surveillance purposes;
- any systems for storing, receiving, transmitting, processing or checking the images or information obtained.

- 20.2 "Surveillance Camera Systems" is taken to include:

- closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems;
- any other systems for recording or viewing visual images for surveillance purposes;

This definition will include body worn video (BWV) and overt cameras deployed to detect waste offences such as fly-tipping. This definition has far reaching implications as the use of any cameras that meet the requirement will have to be used in a manner that complies with the codes of practice mentioned above and the Data Protection Act.

This includes

- CCTV;
- Body Worn Video (BWV)
- Automatic Number Plate Recognition;
- Deployable mobile overt mobile camera systems.
- Any other system for recording or viewing visual images for surveillance purposes;
- Any systems for storing, receiving, transmitting, processing or checking images or information obtained by those systems; and
- Any other systems associated with, or otherwise connected with those systems.

- 20.2 The use of the conventional town centre CCTV systems operated by the Council do not normally fall under the RIPA regulations. However, it does fall under the UK General Data Protection Regulation, Data Protection Act 2018, the Surveillance Camera Code 2013, Information Commissioner's Office (ICO) 'In the picture: a data protection code of practice for surveillance cameras and personal information' and the Council's CCTV policy which is available via the following link: [CCTV - Fenland District Council](#). However, should there be a requirement for the CCTV cameras to be used for a specific purpose to conduct surveillance it is likely that the activity will fall under Directed Surveillance and therefore require an authorisation.
- 20.3 Operators of the Councils CCTV system need to be aware of the RIPA issues associated with using CCTV and that continued, prolonged systematic surveillance of an individual may require an authorisation.
- 20.4 On the occasions when the CCTV cameras are to be used in a Directed Surveillance situation either by enforcement officers from relevant departments within the Council or outside Law Enforcement Agencies such as the Police, the Fenland District Council CCTV Policy should be followed where relevant as well as the RIPA Codes of Practice.
- 20.5 The CCTV staff are to have a copy of the authorisation form in a redacted format, or a copy of the authorisation page. If it is an urgent oral authority from the Police, a copy of the applicant's notes are to be retained or at least some other document in writing which confirms the authorisation and exactly what has been authorised. It is important that the staff check the authority and only carry out what is authorised. A copy of the application or notes is also to be forwarded to the central register for filing. This will assist the Council to evaluate the authorisations and assist with oversight.

21. Automatic Number Plate Recognition (ANPR)

- 21.1 Automated Number Plate Recognition (ANPR) does not engage RIPA if it is used for the purpose it is registered for, such as traffic flow management or safety and enforcement within car parks. However, it is capable of being a surveillance device if used in a pre-planned way to carry out surveillance by monitoring a particular vehicle by plotting its locations, e.g. in connection with illegally depositing waste (fly-tipping).
- 21.2 Should it be necessary to use any ANPR systems to monitor vehicles, the same RIPA principles apply where a Directed Surveillance Authorisation should be sought.

22 Internet and Social Media Investigations

- 22.1 The use of the internet and social media such as Facebook, Instagram and Twitter in an investigation is permitted and may be a means of gathering intelligence. In accessing such sites, officers must consider the issues of privacy and collateral intrusion. The Covert Human Intelligence Source revised code of practice sections 4.29 to 4.35 provides good guidance on the subject. Even though a person may have placed information about themselves or others in the public arena, they have done so with an expectation of a degree of privacy. Viewing information on the internet may constitute covert surveillance, particularly if there is monitoring of subjects involved for example to establish patterns of behavior. Where information about an individual is placed on a publicly accessible database such as Companies House, then they are unlikely to have expectations of privacy.

- 22.2 The use of online open source internet and social media research techniques has become a productive method of obtaining information to assist the Council with its regulatory and enforcement functions. It can also assist with service delivery issues and debt recovery. However, the use of the internet and social media is constantly evolving and with it the risks associated with these types of enquiries, particularly regarding breaches of privacy under Article 8 Human Rights Act (HRA) and other operational risks.
- 22.3 If an investigating officer enters into a 'conversation' with a profile, and the officer informs them that he is contacting them in his role as an employee of the council, then this contact will be overt and no authorisation will be required.
- 22.4 Where the activity does not include monitoring of material in the public domain, RIPA will not apply. If repeated visits to a site are made then this will constitute monitoring and consideration needs to be given to the use of social media or the internet as part of that investigation.
- 22.5 If an investigating officer views for example a Facebook profile with whom they are not 'friends' which is not protected by any privacy settings the information can be treated as being in the public domain. Any initial viewing/visiting of this profile will be overt and authorisation under RIPA will not be required.
- 22.6 If the officer frequently or regularly views the same individual's profile this is considered targeted surveillance and a RIPA authorisation may be required should it meet the stated RIPA criteria in this policy. If it does not then the officer should be able to show that they have considered whether RIPA applied.
- 22.7 Activities of monitoring through, for example, a Facebook profile for a period of time and a record of the information is kept for later analysis or evidential purposes is likely to require a RIPA authorisation. Where covert contact is made with another person on the internet a CHIS authority may be required.
- 22.8 Where officers are building and maintaining a relationship with an individual without that individual knowing the true nature for the purposes of an investigation, this may require an application for the use of a CHIS. Guidance is provided in Part C.
- 22.9 If officers create a false or covert identity, this must only be created with the approval of an Authorising Officer and the RIPA Coordinator must be informed. All use of the identity must be logged and reported to the RIPA Coordinator.
- 22.10 Any use of the internet in an investigation must be fully documented – see Appendix 4 and authorised by the relevant Head of Service with overall responsibility for the investigation. The investigating officer then must provide regular updates to the line manager as to the need for continued use of the internet for the stated purpose and, once its use has been discontinued.
- 22.11 The following from the Code of Practice is a guide of factors to consider:
- Whether the investigation or research is directed towards an individual or organisation
 - Whether it is likely to result in obtaining private information about a person or group of people

- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile
- Whether the information obtained will be recorded and retained
- Whether the information is likely to provide an observer with a pattern of lifestyle
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s)
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties

Any similar activity carried out on the Councils' behalf by a third party then this may still require a directed surveillance authorisation.

22.12 Misuse of council devices or misuse of social media may be considered in line with the relevant disciplinary policy. Any usage should be considered in line with the Councils' ICT Acceptable Use Policy and Social Media Guidance.

22.12 The council have the capability to "audit" the use of social media sites by individual user's profile in line with the appropriate IT policies. The council will undertake such an audit in the event of a complaint or concern that social media has been misused or accessed during an investigation where RIPA may apply and has not been appropriately applied for. The concern will be raised with the RIPA Coordinator and Data Protection Officer who will advise on the appropriate procedure.

22.12 The council may also undertake spot check audits and investigators or staff will be required to detail the reason for access.

23. Surveillance Outside of RIPA

23.1 For Directed Surveillance the criminal offence must carry a **6-month prison sentence** (Directed Surveillance crime threshold) or relate to the sale of alcohol or tobacco to children. This means that there are scenarios within an investigation that do not meet this threshold, however it is necessary to undertake surveillance. This will fall outside of RIPA. Examples include:

- Surveillance for anti-social behaviour disorder which do not attract a maximum custodial sentence of at least six months imprisonment.
- Planning enforcement prior to the serving of a notice or to establish whether a notice has been breached.
- Most licensing breaches.
- Safeguarding vulnerable people.
- Civil matters.

23.2 In the above scenarios they are likely to be a targeted surveillance which are likely to breach someone's Article 8 rights to privacy. Therefore, the activity should be

conducted in way which is HRA compliant, which will include necessary and proportionate. Officers should be able to demonstrate how they have considered this.

24 Disciplinary Investigations

- 24.1 Non RIPA surveillance also includes staff surveillance in serious disciplinary investigations. Guidance dictates that this type of surveillance must be compliant with the Monitoring at Work Guidance issued by the Information Commissioner. This is to ensure that it complies with the HRA.
- 24.2 Should the investigation also involve a criminal offence which meets the RIPA criteria such as fraud, the option to carry out the surveillance under RIPA should be considered. However, it must be a genuine criminal investigation with a view to prosecuting the offender.
- 24.3 Should it be necessary to undertake disciplinary surveillance advice should be sought from the Head of HR/OD and/or the Assistant Director – Legal and Governance.
- 24.4 The RIPA codes also provide guidance that authorisation under RIPA is not required for the following types of activity:
- General observations as per section 3.33 in the codes of practice that do not involve the systematic surveillance of an individual or a group of people and should an incident be witnessed the officer will overtly respond to the situation.
 - Use of overt CCTV and Automatic Number Plate Recognition systems.
 - Surveillance where no private information is likely to be obtained.
 - Surveillance undertaken as an immediate response to a situation.
 - Covert surveillance not relating to criminal offence which carries a maximum sentence of 6 months imprisonment or relate to the sale of alcohol or tobacco to children (surveillance outside of RIPA).
 - The use of a recording device by a CHIS in respect of whom an appropriate use or conduct authorisation has been granted permitting them to record any information in their presence.
 - The covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance, the perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance this is outside of RIPA.
- 24.5 As part of the process of formally recording and monitoring non RIPA surveillance, a non RIPA surveillance application form should be completed and authorised by an Authorising Officer. (It has always been recommended that it should still be an AO. This will also improve their authorisation skills.) A copy of the non RIPA surveillance application form can be obtained from the RIPA Coordinator or Authorising Officer.
- 24.6 The SRO will therefore maintain an oversight of non RIPA surveillance to ensure that such use is compliant with Human Rights legislation. The RIPA Co Ordinator will maintain a central record of non RIPA surveillance.

25. Joint Agency Surveillance

- 25.1 In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the Police. If it is a joint operation involving both agencies, the lead agency should seek authorisation.
- 25.2 Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the authorisation form to carry out the activity. When staff are operating on another organisation's authorisation they are to ensure they see what activity they are authorised to carry out and make a written record. They should also provide a copy of the authorisation to the RIPA Co-Ordinator. This will assist with oversight of the use of Council staff carrying out these types of operations. Line Managers should be made aware if their staff are involved in this type of surveillance.

26. Use of Third-Party Surveillance

- 26.1 In some circumstances it may be appropriate or necessary for Fenland District Council to work with third parties who are not themselves a Public Authority (such as an individual, company or non-governmental organisation) to assist with an investigation. Where that third party is acting in partnership with or under the direction of the Council, then they are acting as our agent and any activities that the third party conducts which meet the RIPA definitions of Directed Surveillance should be authorised. This is because the agent will be subject to RIPA in the same way as any employee of the Council would be. The Authorising Officer should ensure that the agents are qualified or have the necessary skills to achieve the objectives. They should also ensure that they understand their obligations under RIPA. If advice is required, please contact the Senior Responsible Officer, RIPA Co-ordinator or Authorising Officer.
- 26.2 Similarly, a surveillance authorisation should also be considered where the Council is aware that a third party (that is not a Public Authority) is independently conducting surveillance and the Council intends to make use of any suitable material obtained by the third party for the purposes of a specific investigation.

27. Surveillance Equipment

- 27.1 The Council will maintain a central register of all surveillance equipment such as cameras and noise monitoring devices. This will require a description, Serial Number, an explanation of its capabilities.
- 27.2 The register will be held and maintained by the RIPA Co-Ordinator. This equipment is available for all departments to use.
- 27.3 All equipment capable of being used for Directed Surveillance such as cameras etc. should be fit for purpose for which they are intended.

27.4 When completing an Authorisation, the applicant must provide the Authorising Officer with details of any equipment to be used and its technical capabilities. The Authorising Officer will have to take this into account when considering the intrusion issues, proportionality and whether the equipment is fit for the required purpose. The Authorising Officer must make it clear on the Authorisation exactly what equipment if any they are authorising and in what circumstances.

PART C. Covert Human Intelligence Sources (CHIS)

28. Introduction

- 28.1 RIPA covers the activities of Covert Human Intelligence Sources (CHIS) which relates not only to sources commonly known as informants (members of the public providing the Council with information), but also the activities of undercover officers. It matters not whether they are employees of the Council, agents or members of the public engaged by the Council to establish or maintain a covert relationship with someone to obtain information.
- 28.2 Not all human source activity will meet the definition of a CHIS. For example, a source may be a public volunteer or someone who discloses information out of professional or statutory duty or has been tasked to obtain information other than by way of a covert relationship. However, Officers must be aware that such information may have been obtained in the course of an ongoing relationship with a family member, friend or business associate. The Council has a duty of care to all members of the public who provide information to us and appropriate measures must be taken to protect that source. How the information was obtained should be established to determine the best course of action. The source and information should also be managed correctly in line with the Criminal Procedures and Investigations Act (CPIA) and the disclosure provisions.
- 28.3 Recognising when a source becomes a CHIS is therefore important as this type of activity may need authorisation. Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of the contents of this Policy and the CHIS codes of Practice.
- 28.4 Before use of a CHIS is authorised, advice must be sought from the Senior Responsible Officer or their appointed deputy. The application can be authorised by the Chief Executive (or an appointed deputy) and the applicant must ensure that the Authorising Officer has sufficient information to make an informed decision and the prescribed forms must be fully completed.

29. Definition of CHIS

- 29.1 Paragraph 2.1 of Covert Human Intelligence Source revised code of practice state that a person is a Covert Human Intelligence Source if the Council:
- i) establish or maintain a covert relationship with another person to obtain information.
 - ii) covertly give access to information to another person, or
 - iii) disclose information covertly which they have obtained using the relationship or they have obtained because the relationship exists.

- 29.2 A relationship is established, maintained or used for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose. This does not mean the relationship with the Council Officer and the person providing the information, as this is not covert. It relates to how the information was either obtained or will be obtained. Was it or will it be obtained from a third party without them knowing it was being passed on to the Council? This would amount to a covert relationship.
- 29.3 It is possible, that a person will become engaged in the conduct of a CHIS without a public authority inducing, asking or assisting the person to engage in that conduct. An authorisation should be considered, for example, where a public authority is aware that a third party is independently maintaining a relationship (i.e. "self-tasking") in order to obtain evidence of criminal activity, and the public authority intends to make use of that material for its own investigative purposes. (Section 2.26 Codes of CHIS Codes of Practice)

29.4 The following give examples of when a CHIS would and would not be needed.

<p>Would not need a CHIS authorisation</p> <p>Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A juvenile is engaged and trained by a public authority and then deployed in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the 2000 Act that a public authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to granting a directed surveillance authorisation.</p>	<p>Would need a CHIS authorisation</p> <p>In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to juveniles from a room at the back of the shop, providing they have first got to know and trust them. As a consequence the public authority decides to deploy its operative on a number of occasions, to befriend the shopkeeper and gain their trust, in order to purchase alcohol. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained.</p>
<p>Would not need a CHIS authorisation</p> <p>A member of the public volunteers a piece of information to a member of a public authority regarding something they have witnessed in their neighbourhood. The member of the public would not be regarded as a CHIS. They are not passing information as a result of a relationship which has been established or maintained for a covert purpose.</p>	<p>Would need a CHIS authorisation</p> <p>A caller to a confidential hotline (such as Crimestoppers, the HMRC Fraud Hotline, the Anti-Terrorist Hotline, or the Security Service public telephone number) reveals that they know of criminal or terrorist activity. Even if the caller is involved in the activities on which they are reporting, the caller would not be considered a CHIS as the information is not being disclosed on the basis of a relationship which was established or maintained for that covert purpose. However, should the caller be asked to maintain their relationship with those involved and to continue to supply information (or it is otherwise envisaged that they will do so), an authorisation for the use or conduct of a CHIS may be appropriate.</p>

Would not need a CHIS authorisation	Would need a CHIS authorisation
<p>A member of the public is asked by a member of a public authority to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, directed surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual</p>	<p>Mr Y volunteers information to a member of a public authority about a work colleague out of civic duty. Mr Y is not a CHIS at this stage as he has not established or maintained (or been asked to establish or maintain) a relationship with his colleague for the covert purpose of obtaining and disclosing information. However, Mr Y is subsequently contacted by the public authority and is asked if he would ascertain certain specific information about his colleague. At this point, it is likely that Mr Y's relationship with his colleague is being maintained and used for the covert purpose of providing that information. A CHIS authorisation would therefore be appropriate to authorise interference with the Article 8 right to respect for private or family life of Mr Y's work colleague</p>

30. Vulnerable and Juvenile CHIS

- 30.1 Special consideration must be given to the use of a Vulnerable Individual as a CHIS. A 'Vulnerable Individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description, or a Juvenile as defined below, should only be authorised to act as a source in the most exceptional circumstances and only then when authorised by the Chief Executive (or, in his absence, the Corporate Director – Monitoring Officer).
- 30.2 In line with, Paragraph 4.1 of the Covert Human Intelligence Source revised code of practice, the Investigatory Powers Commissioner must be informed within seven working days of a CHIS authorisation of a vulnerable adult or a juvenile source. The Investigatory Powers Commissioner intends to keep such authorisations under close review and will report any relevant findings in his Annual Report. The Authorising Officer must therefore ensure that the SIRO/RIPA Coordinator are informed urgently should such an authorisation be made so that appropriate arrangements can be put in place.
- 30.2 Paragraph 4.3 of the CHIS Code of Practice refers to the use of juveniles in either scenario and how special safeguards also apply to the use or conduct of juveniles. The use of such a person could occur during test purchasing operations. The Code of Practice gives clear guidance:
- On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them.

- In other cases, authorisations should not be granted unless the special provisions, contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended), are satisfied.
- Authorisations for use of a juvenile as a CHIS should be granted by the Head of Paid Service i.e. the Chief Executive.
- The duration of such an authorisation is four months from the time of grant or renewal (instead of twelve months), and the authorisation should be subject to at least monthly review.
- For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

30.3 We must ensure that an appropriate adult is present at any meetings with a CHIS under 16 years of age. The appropriate adult should normally be the parent or guardian of the CHIS, unless they are unavailable or there are specific reasons for excluding them, such as their involvement in the matters being reported upon, or where the CHIS provides a clear reason for their unsuitability. In these circumstances another suitably qualified person should act as appropriate adult, e.g. someone who has personal links to the CHIS or who has professional qualifications that enable them to carry out the role (such as a social worker). Any deployment of a juvenile CHIS should be subject to the enhanced risk assessment process set out in the statutory instrument, and the rationale recorded in writing.

31. Lawful Criteria

- 31.1 The lawful criteria for CHIS authorisation is **prevention and detection of crime and prevention of disorder**. The serious crime criteria of the offence carrying a 6-month sentence etc. does not apply to CHIS.
- 31.2 Authorisations for Juvenile Sources must be authorised by the Chief Executive of the Council (or, in their absence, the Corporate Director – Monitoring Officer).

32. Conduct and Use of a Source

- 32.1 The way the Council use a CHIS for covert activities is known as ‘the use and conduct’ of a source.
- 32.2 The use of a CHIS involves any action on behalf of a Public Authority to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS.
- 32.3 The conduct of a CHIS is establishing or maintaining a personal or other relationship with another person for the covert purpose of:
- a. Using such a relationship to obtain information, or to provide access to information to another person, or
 - b. Disclosing information obtained by the use of such a relationship or as a consequence of such a relationship or
 - c. Is incidental to anything falling within a and b above.
- 32.4 In other words, an authorisation for conduct will authorise steps taken by the CHIS on behalf, or at the request, of a Public Authority.

- 32.5 The use of a source is what the Authority does in connection with the source, such as tasking (see section 33), and the conduct is what a source does to fulfil whatever tasks are given to them or which is incidental to it. The Use and Conduct require separate consideration before authorisation. However, they are normally authorised within the same authorisation.
- 32.6 The same authorisation form is utilised for both use and conduct. A Handler and Controller must also be designated, as part of the authorisation process (see Part E and section 42), and the application can only be authorised if necessary and proportionate. Detailed records of the use, conduct and tasking of the source also have to be maintained (see section 37).
- 32.7 Care should be taken to ensure that the CHIS is clear on what is or is not authorised at any given time, and that all the CHIS's activities are properly risk assessed. Care should also be taken to ensure that relevant applications, reviews, renewals and cancellations are correctly performed. (Section 210 CHIS Codes of Practice)
- 32.8 Careful consideration must be given to any particular sensitivities in the local community where the CHIS is being used and of similar activities being undertaken by other public authorities which could have an impact on the deployment of the CHIS. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a CHIS or use of information obtained from that CHIS. (Section 3.18 CHIS Codes of Practice)

33. Handler and Controller

- 33.1 Covert Human Intelligence Sources may only be authorised if the following arrangements are in place:
- That there will at all times be an officer (the **Handler**) within the Council who will have day to day responsibility for dealing with the source on behalf of the authority, and for the source's security. The Handler is likely to be the investigating officer.
 - That there will at all times be another officer within the Council who will have general oversight of the use made of the source; (**Controller**) i.e. the line manager.
 - That there will at all times be an officer within the Council who has responsibility for maintaining a record of the use made of the source. See CHIS record keeping (see Section 37)
- 33.2 The **Handler** will have day to day responsibility for:
- Dealing with the source on behalf of the Local Authority concerned;
 - Risk assessments
 - Directing the day to day activities of the source;
 - Recording the information supplied by the source;
 - Monitoring the source's security and welfare; and
 - Informing the Controller of concerns about the personal circumstances of the CHIS that might effect the validity of the risk assessment or conduct of the CHIS.

33.3 The **Controller** will be responsible for:

- The management and supervision of the “Handler” and
- General oversight of the use of the CHIS;
- maintaining an audit of case work sufficient to ensure that the use or conduct of the CHIS remains within the parameters of the extant authorisation.

34. Undercover Officers

34.1 Oversight and management arrangements for **undercover operatives**, while following the principles of the Act, will differ, in order to reflect the specific role of such individuals as members of the Council. The role of the handler will be undertaken by a person referred to as a ‘**cover officer**’. (Section 6.9 CHIS Codes of Practice).

35. Tasking

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

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

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

36. Risk Assessments, Security and Welfare

36.1 The Council has a responsibility for the safety and welfare of the source and for the consequences to others of any tasks given to the source. It is a requirement of the codes that a risk assessment is carried out. This should be submitted with the authorisation request. The risk assessment should provide details of how the CHIS is going to be handled. It should also take into account the safety and welfare of the CHIS in relation to the activity and should consider the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS after the cancellation of the authorisation should also be considered at the outset.

36.2 When considering deploying a CHIS, we should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking.

Before authorising the use or conduct of a CHIS, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. This should consider the risks relating to the specific tasking and circumstances of each authorisation separately, and should be updated to reflect developments during the course of the deployment, as well as after the deployment if contact is maintained.

36.3 The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset and reviewed throughout the period of authorised activity by that CHIS.

36.4 Consideration should also be given to the management of any requirement to disclose information which could risk revealing the existence or identity of a CHIS. For example this could be by means of disclosure to a court or tribunal, or any other circumstances where disclosure of information may be required, and strategies for minimising the risks to the CHIS or others should be put in place. Additional guidance about protecting the identity of the CHIS is provided at paragraphs 9.26 to 9.29 of the of the Covert Human Intelligence Source revised code of practice.

36.5 The CHIS handler is responsible for bringing to the attention of the CHIS controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the CHIS; and
- the safety and welfare of the CHIS.

Where appropriate, concerns about such matters must be considered by the authorising officer, and a decision taken on whether or not to allow the authorisation to continue.

36.6 Appendix 3 provides a risk assessment form for an operation.

37. Use of Equipment by a CHIS

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

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

38. CHIS Management

- 38.1 The operation will require managing by the Handler and Controller which will include ensuring that the activities of the source and the operation remain focused and there is no status drift. It is important that the intrusion is assessed to ensure the operation remains proportionate. The security and welfare of the source will also be monitored. The Authorising Officer should maintain general oversight of these functions.
- 38.2 During CHIS activity, there may be occasions when unforeseen actions or undertakings occur. Such incidences should be recorded as soon as practicable after the event and if the existing authorisation is insufficient, it should either be dealt with by way of a review and re-authorised (for minor amendments only) or it should be cancelled, and a new authorisation obtained before any further action is carried out. Similarly, where it is intended to task a CHIS in a new significantly different way than previously identified, the proposed tasking should be referred to the Authorising Officer, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and details of such referrals must be recorded.

39 Operation Involving Multiple CHIS

- 39.1 A single authorisation may be used to authorise more than one CHIS. However, this is only likely to be appropriate for operations involving the conduct of several individual operatives acting as CHISs in situations where the activities to be authorised, the subjects of the operation, the interference with private or family life, the likely collateral intrusion and the environmental or operational risk assessments are the same for each officer. If an authorisation includes more than one relevant source, each relevant source must be clearly identifiable within the documentation. In these circumstances, adequate records must be kept of the length of deployment of a relevant source to ensure the enhanced authorisation process set out in the 2013 Relevant Sources Order and Annex B of the Code of Practice can be adhered to.

40 Social Media considerations

40.1 Considering a Covert Human Intelligence Source (CHIS) authorisation in social media/internet investigations

Any council officer or person acting on their behalf, who conducts activity on the internet in such a way that they may interact with others, whether by publicly open websites such as an online news and social networking service, or more private exchanges such as e-messaging sites, in circumstances where the other parties could not reasonably be expected to know their true identity, should consider whether the activity requires a CHIS authorisation.

A directed surveillance authorisation should also be considered, unless the acquisition of that information is or will be covered by the terms of an applicable CHIS authorisation.

40.2 Tasking someone to use a profile for covert reasons

Where someone, such as an employee or member of the public, is tasked by the council to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the public authority, in order to obtain or provide access to information, a CHIS authorisation is likely to be required.

Example of when CHIS authorisation is needed

An investigator using the internet to engage with a subject of interest at the start of an operation, in order to ascertain information or facilitate a meeting in person. • Directing a member of the public (such as a CHIS) to use their own or another internet profile to establish or maintain a relationship with a subject of interest for a covert purpose. • Joining chat rooms with a view to interacting with a criminal group in order to obtain information about their criminal activities.

40.3 Registering to Access a Site

A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Some websites require a user to register providing personal identifiers (such as name and phone number) before access to the site will be permitted. Where an officer sets up a false identity for this purpose, this does not in itself amount to establishing a relationship, and a CHIS authorisation would not immediately be required, though consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met.

Example of when CHIS authorisation is not needed

A Trading Standards officer intends to make a one-off online test purchase of an item on an auction site, to investigate intelligence that counterfeit goods are being sold. The officer concludes the purchase and does not correspond privately with the seller or leave feedback on the site. No covert relationship is formed and a CHIS authorisation need not be sought.

Example of when CHIS authorisation is needed

A Trading Standards officer tasks a member of the public to purchase goods from a number of websites to obtain information about the identity of the seller, country of origin of the goods and banking arrangements. The individual is required to engage with the seller as necessary to complete the purchases. The deployment should be covered by a CHIS authorisation because of the intention to establish a relationship for covert purposes.

40.4 Use of Likes and Follows

Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as “like” or “follow” to react to information posted by others online would not in itself constitute forming a relationship. However, it should be borne in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if it is intended for a council officer or a CHIS to engage in such interaction to obtain, provide access to or disclose information.

Example of when CHIS authorisation is not needed	Example of when CHIS authorisation is needed
An officer maintains a false persona, unconnected to law enforcement activities, on social media sites in order to facilitate future operational research or investigation. As part of the legend building activity they “follow” a variety of people and entities and “likes” occasional posts without engaging further. No relationship is formed and no CHIS authorisation is needed.	The officer sends a request to join a closed group known to be administered by a subject of interest, connected to a specific investigation. A directed surveillance authorisation would be needed to cover the proposed covert monitoring of the site. Once accepted into the group it becomes apparent that further interaction is necessary. This should be authorised by means of a CHIS authorisation.

40.4 The identity Being Used

When engaging in conduct as a CHIS, a council officer should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without considering the need for authorisation. Full consideration should be given to the potential risks posed by that activity.

40.5 Risk Assessment

Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with section 7.16 of the Covert Human Intelligence Source revised code of practice should include consideration of the risks arising from that online activity including factors such as the length of time spent online and the material to which the CHIS may be exposed. This should also take account of any disparity between the technical skills of the CHIS and those of the handler or authorising officer, and the extent to which this may impact on the effectiveness of oversight.

Where it is intended that more than one officer will share the same online persona, each officer should be clearly identifiable within the overarching authorisation for that operation, providing clear information about the conduct required of each officer and including risk assessments in relation to each officer involved.

41. CHIS Record Keeping

41.1 Centrally Retrievable Record of Authorisations

41.1.1 A centrally retrievable record of all authorisations is held by Fenland District Council. This record contains the relevant information to comply with the Codes of Practice. These records are updated whenever an authorisation is granted, renewed or cancelled and are available to the Investigatory Powers Commissioner (IPCO) upon request.

41.1.2 The records are retained for 3years from the ending of the authorisation.

41.2 Individual Source Records of Authorisation and Use of CHIS

41.2.1 Detailed records must be kept of the authorisation and the use made of a CHIS. An authorising officer must not grant an authorisation for the use or conduct of a CHIS unless they believe that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. The Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No: 2725 details the particulars that must be included in these records.

41.2.2 The particulars to be contained within the records are;

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

41.2.3 The person maintaining these records is the RIPA Co-ordinator.

41.2.4 Public authorities are also encouraged to maintain auditable records for individuals providing intelligence who do not meet the definition of a CHIS. This will assist authorities to monitor the status of a human source and identify whether that person should be duly authorised as a CHIS. This should be updated regularly to explain why authorisation is not considered necessary. Such decisions should rest with those designated as Authorising Officers within Public Authorities. (Section 7.5 CHIS Codes of Practice).

41.3. Further Documentation

41.3.1 In addition to the above, when appropriate records or copies of the following, as are retained by Fenland District Council for 3 years:

- A copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- A copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- The reason why the person renewing an authorisation considered it necessary to do so;
- Any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- Any risk assessment made in relation to the operation or CHIS;
- The circumstances in which tasks were given to the CHIS;
- The value of the CHIS to the investigating authority;
- A record of the results of any reviews of the authorisation;
- The reasons, if any, for not renewing an authorisation;
- The reasons for cancelling an authorisation; and
- The date and time when any instruction was given by the authorising officer that the conduct or use of a CHIS must cease.
- A copy of the decision by a Judicial Commissioner on the renewal of an authorisation beyond 12 months (where applicable).

41.1.2 The records kept by the Council should be maintained in such a way as to preserve the confidentiality, or prevent disclosure of the identity of the CHIS, and the information provided by that CHIS. (Sec 7.7 CHIS Codes of Practice)

41.1.3 The forms are available in the Appendices: Current link to the Home office Forms is <https://www.gov.uk/government/collections/ripa-forms--2>

- [Application for the conduct or use of Covert Human Intelligence Source \(CHIS\)](#)
- [Review of a Covert Human Intelligence Source \(CHIS\) operation](#)
- [Application for renewal of a Covert Human Intelligence Source \(CHIS\) operation](#)
- [Cancellation of an authorisation for a Covert Human Intelligence Source \(CHIS\) operation](#)

References in these forms to the 'Code' are to the [Covert Human Intelligence Sources Code of Practice](#), which should be consulted for further guidance.

PART D. RIPA Roles and Responsibilities

42. The Senior Responsible Officer (SIRO)

42.1 The nominated Senior Responsible Officer is Carol Pilson Corporate Director – Monitoring Officer. The SIRO with responsibilities for:

- The integrity of the process in place within Fenland District Council to authorise Directed and Intrusive Surveillance;
- Compliance with the relevant sections of RIPA and the Codes of Practice;
- Oversight of the reporting of errors to the Investigatory Powers Commissioner (IPC) and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the Investigatory Powers Commissioner Office (IPCO) and the inspectors who support the Commissioner when they conduct their inspections;
- Where necessary, overseeing the implementation of any recommended post-inspection action plans and
- Ensuring that all Authorising Officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner.

43. RIPA Co-Ordinator

43.1 The RIPA Co-Ordinator Amy Brown – Assistant Director – Legal and Governance is responsible for storing all the original authorisations, reviews, renewals and cancellation forms and the signed approval or refusal documentation from the JP. This will include any authorisations that have not been authorised by the Authorising Officer or refused by a JP.

43.2 The RIPA Co-ordinator will: -

- Keep the copies of the forms for a period of at least 3 years
- Keep the Central Register (a requirement of the Codes of Practice) of all of the authorisations, renewals and cancellations; and Issue the unique reference number.
- Keep a database for identifying and monitoring expiry dates and renewal dates.
- Along with, Directors, Service Managers, Authorising Officers, and the Investigating Officers must ensure that any electronic and paper records relating to a RIPA investigation are used, retained or destroyed in line with the Councils Information Management policies, departmental retention schedules and the Data Protection Act 2018. (DPA)
- Provide administrative support and guidance on the processes involved.
- Monitor the authorisations, renewals and cancellations with a view to ensuring consistency throughout the Council;
- Monitor each department's compliance and act on any cases of non-compliance;
- Ensure adequate training is provided including guidance and awareness of RIPA and the provisions of this Policy; and Review the contents of this Policy.

44. Managers Responsibility and Management of the Activity

- 44.1 Line Managers within each area of the Council are responsible for ensuring that in all cases where surveillance is required, due consideration is given to the need for covert surveillance before an application is made for authorisation. That includes the consideration of using overt action, routine enquiries or inspections which are less intrusive.
- 44.2 If authorised it is important that all those involved in undertaking Directed Surveillance activities, including Line managers, are fully aware of the extent and limits of the authorisation. There should be an ongoing assessment for the need for the activity to continue including ongoing assessments of the intrusion. All material obtained, including evidence, should be stored in line with relevant legislation and procedures to safeguard its integrity and reduce a risk of challenge. (See use of material as evidence (Section 61)
- 44.3 Line Managers should also ensure that the relevant reviews (see section 53), renewals (see section 54) and cancellations (see section 55) are completed by the applicant in accordant with the codes and the dates set throughout the process.

45.1. Investigating Officers/Applicant

- 45.1 The applicant is normally an investigating officer who completes the application section of the RIPA form. Investigating Officers should think about the need to undertake Directed Surveillance or the use of a CHIS before they seek authorisation and discuss it with their Line manager. Investigating Officers need to consider whether they can obtain the information or achieve their objective by using techniques other than covert surveillance.
- 45.2 The applicant or some other person must carry out a feasibility study as this should be seen by the Authorising Officer. The person seeking the authorisation should then complete the application form having regard to the guidance given in this Policy and the statutory Codes of Practice. There should not be any real delay between the feasibility study and the completion of the application form to ensure that the details within the application are accurate and will not have changed. The form should then be submitted to the Authorising Officer for authorisation.
- 45.3 The applicant is likely to attend court to seek the approval of a JP. and if approved and involved in the covert activity they must only carry out what is authorised and approved. They, or some other person will also be responsible for the submission of any reviews (see section 53) renewals (see section 54) and cancellations (see section 55).

46. Authorising Officers

- 46.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that for Local Authorities the Authorising Officer shall be a Director, Head of Service, Service Manager or equivalent as distinct from the officer responsible for the conduct of an investigation.
- 46.2 Appendix A lists the Authorising Officers within the Council who can grant authorisations all of which are Director or Head of Service level Officers.

- 46.3 The role of the Authorising Officers is to consider whether to authorise, review, or renew an authorisation. They must also officially cancel the RIPA covert activity. Authorising Officers must have been trained to an appropriate level so as to have an understanding of the requirements in the Codes of Practice and that must be satisfied before an authorisation can be granted.
- 46.4 Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved. Where an Authorising Officer authorises such an investigation or operation, the central record of authorisations should highlight this, and it should be brought to the attention of a Commissioner or Inspector during their next inspection.
- 46.5 Authorisations must be given in writing by the Authorising Officer by completing the relevant section on the authorisation form. When completing an authorisation, the case should be presented in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the authorisation.
- 46.6 Authorising Officers must explain why they believe the activity is both necessary (see section 43) and proportionate (see section 44), having regard to the collateral intrusion. They must also consider any similar activity which may be taking place, or sensitivities in the area.
- 46.7 They also need to explain exactly what they are authorising, against who, in what circumstances, where etc. and that the level of the surveillance is appropriate to achieve the objectives. It is important that this is made clear on the authorisation as the surveillance operatives are only allowed to carry out what is authorised. This will assist with avoiding errors.
- 46.8 If any equipment such as covert cameras are to be used, the Authorising Officer should know the capability of the equipment before authorising its use. This will have an impact on collateral intrusion, necessity and proportionality. They should not rubber-stamp a request. It is important that they consider all the facts to justify their decision. They may be required to justify their actions in a court of law or some other tribunal.
- 46.9 The Authorising Officer may be required to attend court to explain what has been authorised and why.
- 46.10 Authorised Officers must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA and the current Procedures and Guidance issued by the Commissioner. This document also details the latest operational guidance to be followed. It is recommended that Authorising Officers hold their own copy of this document. This can be obtained from The RIPA Coordinator.

47 Necessity

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

- 47.2 The Act first requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds which for Local Authority Directed Surveillance is the prevention and detection of crime and that the crime attracts a custodial sentence of a maximum of 6 months or more, or for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco.
- 47.3 The lawful criteria for CHIS is prevention and detection of crime and prevention of disorder and the offence does not have to have a sentence of 6 months imprisonment.
- 47.4 The applicant and Authorising Officers must also be able to demonstrate why it is necessary to carry out the covert activity to achieve the objectives and that there were no other means of obtaining the same information in a less intrusive method. This is a part of the authorisation form.

48. Proportionality

- 48.1 If the activities are deemed necessary, the Authorising Officer must also believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.
- 48.2 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render the proposed actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.
- 48.3 When explaining proportionality, the Authorising Officer should explain why the methods and tactics to be adopted during the surveillance is not disproportionate.
- 48.4 The codes provide guidance relating to proportionality which should be considered by both applicants and Authorising Officers:
- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
 - Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
 - Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
 - Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

49. Collateral Intrusion

- 49.1 Before authorising applications for Directed Surveillance, the Authorising Officer should also take into account the risk of obtaining collateral intrusion which is private information about persons who are not subjects of the surveillance.
- 49.2 Staff should take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to anticipated collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.
- 45.3 All applications must therefore include an assessment of the risk of collateral intrusion and detail the measures taken to limit this to enable the Authorising Officer fully to consider the proportionality of the proposed actions. This is detailed in a section within the authorisation form (Contained within the following link) <https://www.gov.uk/government/collections/ripa-forms--2>
- 49.4 In order to give proper consideration to collateral intrusion, an Authorising Officer should be given full information regarding the potential scope of the anticipated surveillance, including the likelihood that any equipment deployed may cause intrusion on persons or property other than the subject(s) of the application. If an automated system such as an online search engine is used to obtain the information, the Authorising Officer should be made aware of its potential extent and limitations. Material which is not necessary or proportionate to the aims of the operation or investigation should be discarded or securely retained separately where it may be required for future evidential purposes. It may also need retaining under CPIA. The Authorising Officer should ensure appropriate safeguards for the handling, retention or destruction of such material, as well as compliance with Data Protection Act requirements.
- 49.5 Where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy of such individuals should not be considered as collateral intrusion but rather as intended intrusion.
- 49.6 In the event that authorised surveillance unexpectedly and unintentionally interferes with the privacy of any individual other than the intended subject, the authorising officer should be informed by submitting a review form. Consideration should be given in any such case to the need for any separate or additional authorisation.
- 49.7 Where a Public Authority intends to access a social media or other online account to which they have been given access with the consent of the owner, the authority will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a Directed Surveillance authorisation should be considered, particularly (though not exclusively) where it is intended to monitor the account going forward.

50 Other Factors

50.1 Spiritual Counselling

No operations should be taken in circumstances where investigators believe that surveillance will lead to them intruding on spiritual counselling between a Minister and a Member of his/her faith. In this respect, spiritual counselling is defined as conversations with Minister of Religion acting in his-her official capacity where the person being counselled is seeking or the Minister is imparting forgiveness, or absolution of conscience.

50.2 Community Sensitivities

Officers should always consider whether there are any particular sensitivities within our communities and take these into account if planning surveillance activities in those areas.

PART E. The Application and Authorisation Process

51. Relevant Forms

51.1 For both Directed Surveillance and CHIS authorisations there are 4 forms within the process. They are:

- Authorisation
- Review
- Renewal
- Cancellation

51.2 All the forms can be obtained from the Government Website at

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

52. Duration of Authorisations

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

Directed Surveillance	3 Months
Renewal	3 Months
Covert Human Intelligence Source	12 Months
Renewal	12 months
Juvenile Sources	4 Months
Renewal	4 Months

52.2 It is the responsibility of the Investigating Officer to make sure that the authorisation is still valid when they undertake surveillance.

52.3 In paragraph 4.17 of the Covert Surveillance and Property Interference Code of Practice, it is confirmed that a single authorisation may combine two or more different authorisations under RIPA however the provisions applicable for each of the authorisations must be considered separately by the appropriate authorising officer. It does not preclude the obtaining of separate authorisations.

53. Applications/Authorisation

- 53.1 The applicant or some other person must carry out a feasibility study and intrusion assessment as this may be required by the Authorising Officer. The person seeking the authorisation should then complete the application form having regard to the guidance given in this Policy and the statutory Codes of Practice. There should not be any real delay between the feasibility study and the completion of the application form to ensure that the details within the application are accurate and will not have changed. The form should then be submitted to the Authorising Officer for authorisation.
- 53.2 When completing an application for authorisation, the applicant must ensure that the case for the authorisation is presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take into account information which weakens the case for the warrant or authorisation. This is a requirement of the codes.
- 53.3 All the relevant sections must be completed with sufficient information to ensure that applications are sufficiently detailed for the Authorising Officer to consider Necessity, Proportionality having taken into account the Collateral Intrusion issues **Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.**
- 53.4 If it is intended to undertake both Directed Surveillance and the use of a CHIS on the same surveillance subject, the respective authorisation should be completed and the respective procedures followed. Both activities should be considered separately on their own merits.
- 53.5 All applications will be submitted to the Authorising Officer via the Line Manager of the appropriate enforcement team in order that they are aware of the application and activities being undertaken by the staff. The Line Manager will perform an initial quality check of the application. However, they should not be involved in the sanctioning of the authorisation. The form should then be submitted to the Authorising Officer.
- 53.6 Applications whether authorised or refused will be issued with a unique number (obtained from the RIPA Co-Ordinator) by the line manager. The number will be taken from the next available number in the central record of authorisations which is held by the RIPA Coordinator.
- 53.7 If not authorised, feedback will be provided to the applicant and the application will be forwarded to the RIPA Co-Ordinator for recording and filing. If having received the feedback, the applicant feels it is appropriate to re submit the application, they can do so and it will then be considered again.53.8 Following authorisation, the applicant will then complete the relevant section of the judicial application/order form (Contained within the following link) <https://www.gov.uk/government/collections/ripa-forms--2>

Although this form requires the applicant to provide a brief summary of the circumstances of the case, this is supplementary to and does not replace the need to supply a copy and the original RIPA authorisation as well.

54. Arranging the Court Hearing

- 54.1 It will be necessary within office hours to contact the administration at the Magistrates' Court to arrange a hearing. The hearing will be in private and heard by a single JP. The application to the JP will be on oath.
- 54.2 Officers who may present the application at these proceedings will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or information as required by the JP. If in doubt as to whether you are able to present the application seek advice from the Legal Services Team.

55. Attending the Hearing

- 55.1 The applicant in addition to the Authorising Officer will attend the hearing. Upon attending the hearing, the officer must present to the JP the partially completed judicial application/order form, the original and a copy of the RIPA application/authorisation form, together with any supporting documents setting out the case. The original RIPA authorisation should be shown to the JP but will be retained by the Council so that it is available for inspection by IPCO, and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

- 55.2 The JP will read and consider the RIPA authorisation and the judicial application/order form (contained within the following link) <https://www.gov.uk/government/collections/ripa-forms--2>

They may have questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the application form. **However, the forms and supporting papers must by themselves make the case. It is not sufficient for the Council to provide oral evidence where this is not reflected or supported in the papers provided.**

- 55.3 The JP will consider whether they are satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. In addition, they must be satisfied that the person who granted the authorisation was an appropriate Designated Person within the Council to authorise the activity and the authorisation was made in accordance with any applicable legal restrictions, for example, the crime threshold for Directed Surveillance.

56. Decision of the Justice of the Peace (JP)

- 56.1 The JP has a number of options which are:
- 56.2 **Approve or renew an authorisation.** If approved by the JP, the date of the approval becomes the commencement date for the duration of the three months and the officers are now allowed to undertake the activity.
- 56.3 **Refuse to approve or renew an authorisation.** The RIPA authorisation will not take effect and the Council may **not** use the technique in that case.

- 56.4 Where an application has been refused, the applicant may wish to consider the reasons for that refusal. If more information was required by the JP to determine whether the authorisation has met the tests, and this is the reason for refusal, the officer should consider whether they can reapply. For example, if there was information to support the application which was available to the Council, but not included in the papers provided at the hearing.
- 56.5 For, a technical error (as defined by the JP), the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.
- 56.6 **Refuse to approve or renew and quash the authorisation.** This applies where the JP refuses to approve or renew the authorisation and decides to quash the original authorisation. However, the court must not exercise its power to quash the authorisation unless the applicant has had at least 2 business days from the date of the refusal in which to make representations. If this is the case, the officer will inform the Legal who will consider whether to make any representations.
- 56.7 The JP will record their decision on the order section of the judicial application/order form. The court administration will retain a copy of the Council's RIPA application and authorisation form and the judicial application/order form. The officer will retain the original authorisation and a copy of the judicial application/order form.
- 56.8 The Council may only appeal a JP decision on a point of law by judicial review. If such a concern arises, the Legal Services Team will decide what action if any should be taken.
- 56.9 There is a Home Office chart showing the above procedure at Appendix B.

57. Post Court Procedure

- 57.1 It will be necessary to work out the cancellation date from the date of approval and ensure that the applicant and the Authorising Officer is aware. The original application and the copy of the judicial application/order form should be forwarded to the RIPA Co-Ordinator. A copy will be retained by the applicant and if necessary by the Authorising Officer. The central register will be updated with the relevant information to comply with the Codes of Practice and the original documents filed and stored securely.
- 57.2 Where dates are set within the process such as reviews, they must be adhered to. This will help with demonstrating that the process has been managed correctly in line with the Codes of Practice and reduce the risk of errors.

58. Reviews

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

- 58.2 In each case the Authorising Officer should determine how often a review should take place at the outset. This should be as frequently as is considered necessary and practicable. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides a high level of intrusion into private life or significant collateral intrusion, or confidential information. They will record when they are to take place on the application form. This decision will be based on the circumstances of each application. However, reviews will be conducted on a monthly or less basis to ensure that the activity is managed. It will be important for the Authorising Officer to be aware of when reviews are required to ensure that the applicants submit the review form on time.
- 58.3 Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application which would include a change to the level of intrusion so that the need to continue the activity can be re-assessed. However, if the circumstances or the objectives have changed considerably, or the techniques to be used are now different, a new application form should be submitted, and it will be necessary to follow the process again and be approved by a JP. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.
- 58.4 Line managers of applicants should also make themselves aware of when the reviews are required to ensure that the relevant forms are completed on time.
- 58.5 The reviews are dealt with internally by submitting the review form to the Authorising Officer. There is no requirement for a review form to be submitted to a JP.
- 58.6 The results of a review should be recorded on the central record of authorisations.

59. Renewal

- 59.1 A renewal form is to be completed by the applicant when the original authorisation period is about to expire but Directed Surveillance or the use of a CHIS is still required.
- 59.2 **Authorisation should not be allowed to lapse. They should be reviewed and cancelled or renewed.**
- 59.2 Should it be necessary to renew an authorisation for Directed Surveillance or CHIS, this must be approved by a JP.
- 59.3 Applications for renewals should not be made until shortly before the original authorisation period is due to expire. However, they must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant Authorising Officer and a JP to consider the application).
- 59.4 The applicant should complete all the sections within the renewal form and submit the form to the Authorising Officer for consideration.

- 59.5 Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.
- 59.6 If the Authorising Officer refuses to renew the application, the cancellation process should be completed. If the Authorising Officer authorises the renewal of the activity, the same process is to be followed as mentioned earlier for the initial application whereby approval must be sought from a JP.
- 59.7 A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

60. Cancellation

- 60.1 The cancellation form (contained in the following link) <https://www.gov.uk/government/collections/ripa-forms--2> is to be submitted by the applicant or another investigator in their absence. The Authorising Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the Directed Surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer.
- 60.2 As soon as the decision is taken that Directed Surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations.
- 60.3 The Investigating Officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and detail if any images were obtained, particularly any images containing innocent third parties. The Authorising Officer should then take this into account and issues instructions regarding the management and disposal of the images etc. See sections 58 to 65 Safeguarding and the Use of Surveillance Material below.
- 60.4 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what was authorised. This check will form part of the oversight function. Where issues are identified including errors (see Part G) they will be brought to the attention of the Line Manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight and comply with the Codes of Practice.
- 60.5 When cancelling a CHIS authorisation, an assessment of the welfare and safety of the source should also be assessed and any issues identified.
- 60.6 All cancellations must be submitted to the RIPA Co-Ordinator for inclusion in the central Record and storing securely with the other associated forms.

60.7 Do not wait until the 3 month period is up to cancel. Cancel it at the earliest opportunity when no longer necessary and proportionate. Line Managers should be aware of when the activity needs cancelling and ensure that staff comply with the procedure.

Part F Acquisition of Communications Data

61. Introduction

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

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

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

In order to compel a Communications Service Provider to obtain and disclose, or just disclose Communications Data in their possession, a notice under S22 (4) RIPA must be issued.

The sole ground to permit the issuing of a S22 notice by a Permitted Local Authority is for the purposes of "preventing or detecting crime or of preventing disorder". The issuing of such a notice will be the more common of the two powers utilised, in that the Communications Service Provider will most probably have means of collating and providing the communications data requested.

There is no threshold for subscriber data which can still be acquired for any crime where it is necessary and proportionate to do so. However as of 1 November 2018, there is a crime threshold for the acquisition of service or traffic data which is restricted to "serious crime". This is defined as:

- An offence capable of attracting a prison sentence of 12 months or more. This can be checked by accessing the Home Office counting rules notifiable offence list.
- An offence by a person who is not an individual i.e. a corporate body
- A Section 81 of RIPA – an offence defined as serious crime such as use of violence, substantial financial gain or large number of people in pursuit of a common purpose
- An offence which integrally involves the sending of a communication
- Breach of privacy offence

Examples of what are non-serious crimes are:

- Certain immigration offences under the Immigration Act 1971; and
- Certain gambling offences under the Gambling Act 2005 including provision of facilities for gambling, use of premises for gambling and offences relating to gambling machines.
- Some sections of the Public Order Act which do not amount to violence (including using offensive words or causing a fear of violence);

- Driving offences, such as: joy riding, driving when disqualified, failure to stop or report an accident and driving when unfit to do so through drink or drugs;
- Some sections of the Consumer Protection Act 1987 i.e. furnishing false information in response to notice, or to enforcement officer.

62. Application procedure

- 62.1 At present, the only route to obtain this type of information is through the National Anti-Fraud Network (NAFN). Fenland District Council is not currently a member of NAFN and as such cannot make an enquiry.
- 62.2 It should be noted that the council's provider of fraud investigation services, Anglia Revenue Partnership (ARP), is a member of NAFN and may make requests in relation to matters relating to Fenland District Council. In these instances, ARP should ensure that they inform the council of the request made and this be recorded by the RIPA Co-ordinator.

Part G Central Record and Safeguarding the Material

62. Introduction

- 62.1 Authorising Officers, applicants and Line Managers of relevant enforcement departments may keep whatever records they see fit to administer and manage the RIPA application process. This includes the legal obligations under the Criminal Procedures and Investigations Act. However, this will not replace the requirements under the Codes of Practice, which includes the fact that the Council must hold a centrally held and retrievable record.
- 62.2 Applicants, Authorising Officers, SIRO and the RIPA Coordinator must comply with the requirements set out in this Part of the Policy and the Guidance at Appendix 5.

63. Central Record

- 63.1 The centrally retrievable record of all authorisations will be held and maintained by Amy Brown - RIPA Co-Ordinator. It will be regularly updated whenever an authorisation is applied for, refused, granted, renewed or cancelled. The record will be made available to the relevant Commissioner or an Inspector from IPCO, upon request.
- 63.2 All original authorisations and copies of Judicial applications/order forms whether authorised or refused, together with review, renewal and cancellation documents, must be sent within 48 hours to Amy Brown – RIPA Co-Ordinator who will be responsible for maintaining the central record of authorisations. They will ensure that all records are held securely with no unauthorised access. If in paper format, they must be forwarded in a sealed envelope marked confidential.
- 63.3 The documents contained in the centrally held register should be retained for 3 years. The centrally held register contains the following information:
- If refused, (the application was not authorised by the AO) a brief explanation of the reason why. The refused application should be retained as part of the central record of authorisation;
 - If granted, the type of authorisation and the date the authorisation was given;
 - Details of attendances at the magistrates' court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision;
 - Name and rank/grade of the authorising officer;
 - The unique reference number (URN) of the investigation or operation;
 - The title of the investigation or operation, including a brief description and names of subjects, if known;
 - Frequency and the result of each review of the authorisation;
 - If the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer and the date renewed by the JP;

- Whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- The date the authorisation was cancelled;
- Authorisations by an Authorising Officer where they are directly involved in the investigation or operation. If this has taken place it must be brought to the attention of a Commissioner or Inspector during their next RIPA inspection.

63.4 As well as the central record the RIPA Co-Ordinator will also retain:

- The original of each application, review, renewal and cancellation, copy of the judicial application/order form, together with any supplementary documentation of the approval given by the Authorising Officer;
- The frequency and result of reviews prescribed by the Authorising Officer;
- The date and time when any instruction to cease surveillance was given;
- The date and time when any other instruction was given by the Authorising Officer;
- A record of the period over which the surveillance has taken place. This should have been included within the cancellation form.

63.5 These documents will also be retained for five years from the ending of the authorisation.

64. Safeguarding and the Use of Surveillance Material

64.1 This section provides guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained through Directed Surveillance or CHIS activity. This material may include private, confidential or legal privilege information. It will also show the link to other relevant legislation.

64.2 The Council should ensure that their actions when handling information obtained by means of covert surveillance or CHIS activity comply with relevant legal frameworks and the Codes of Practice, so that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. Compliance with these legal frameworks, including Data Protection requirements, will ensure that the handling of private information obtained continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards. The material will also be subject to the Criminal Procedures Investigations Act (CPIA)

65. Authorised Purpose

65.1 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. For the purposes of the RIPA codes, something is necessary for the authorised purposes if the material:

- Is, or is likely to become, necessary for any of the statutory purposes set out in the RIPA Act in relation to covert surveillance or CHIS activity;

- Is necessary for facilitating the carrying out of the functions of public authorities under RIPA;
- Is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- Is necessary for the purposes of legal proceedings; or
- Is necessary for the performance of the functions of any person by or under any enactment.

66. Handling and Retention of Material

- 66.1 Generally, all material (in whatever media) obtained or produced during the course of investigations subject to RIPA authorisations should be processed, stored and destroyed in accordance with the requirements of the UK General Data Protection Regulation, Data Protection Act 2018, the Freedom of Information Act 2000, any other legal requirements, including those of confidentiality, and the councils' policies and procedures currently in force relating to document retention. The Council's Document Retention Policy sets out the expected requirements.
- 66.2 All officers involved within this process should make themselves aware of the provisions within this legislation and how it impacts on the whole RIPA process. Material obtained, together with relevant associated paperwork should be held securely. Extra care needs to be taken if the application and material relates to a CHIS.
- 66.2 Material required to be retained under CPIA should be retained until a decision is taken whether to institute proceedings against a person for an offence or if proceedings have been instituted, at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case.
- 66.3 Where the accused is convicted, all material which may be relevant must be retained at least until the convicted person is released from custody, or six months from the date of conviction, in all other cases.
- 66.4 If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction.
- 66.5 If an appeal against conviction is in progress when released, or at the end of the period of six months, all material which may be relevant must be retained until the appeal is determined.
- 66.6 Where material is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should not be destroyed, but retained in accordance with legal disclosure requirements. All such material should be clearly labelled and stored in such a way to enable compliance with data retention and disposal.

66.6 If retention is beyond these periods it must be justified under DPA. Each relevant service within the Council may have its own provisions under their Data Retention Policy which will also need to be consulted to ensure that the data is retained lawfully and for as long as is necessary.

66.7 Any material obtained must be stored securely, either electronically or physically, and access only provided to those who have the appropriate clearance for access. Physical information must be protected by an adequate level of security such as locked rooms or a safe with a log of access kept.

66.8 Information will be destroyed securely in line with retention requirements and its retention will be reviewed accordingly.

67. Use of Material as Evidence

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

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

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

67.4 There is nothing in RIPA which prevents material obtained under Directed Surveillance authorisations from being used to further other investigations.

68. Dissemination of Information

68.1 Material obtained should only be shared with individuals within the authority and external partners where this is permitted by legislation, an information sharing agreement or a requirement to disclose. For example, a joint investigation with the Police would require information to be shared as part of that investigation and permitted by data protection legislation.

- 68.2 The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary. It must also be in connection with an authorised purpose as set out in sec 59 above. It will be necessary to consider exactly what and how much information should be disclosed. Only so much of the material may be disclosed as the recipient needs; for example, if a summary of the material will suffice, no more than that should be disclosed.
- 68.3 The obligations apply not just to Fenland District Council as the original authority acquiring the information, but also to anyone to whom the material is subsequently disclosed. In some cases, this will be achieved by requiring the latter to obtain permission from Fenland District Council before disclosing the material further. It is important that the Officer In Charge (OIC) of the enquiry considers these implications at the point of dissemination to ensure that safeguards are applied to the data.
- 68.4 A record will be maintained justifying any dissemination of material. If in doubt, seek advice.

69. Storage

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

70. Copying

- 70.1 Material obtained through covert surveillance may only be copied to the extent necessary for the authorised purposes set out above. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance, and any record which refers to the covert surveillance and the identities of the persons to whom the material relates.
- 70.2 In the course of an investigation, Fenland District Council must not act on or further disseminate legally privileged items unless it has first informed the Investigatory Powers Commissioner that the items have been obtained.

71. Destruction

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

Part H. Errors and Complaints

72. Errors

- 72.1 Errors can have very significant consequences on an affected individual's rights. Proper application of the surveillance and CHIS provisions in the RIPA codes and this Policy should reduce the scope for making errors.
- 72.2. There are two types of errors within the codes of practice which are:
- Relevant error and
 - Serious error.

73 Relevant Error

- 73.1 An error must be reported if it is a "**relevant error**". A relevant error is any error by a Public Authority in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance by public authorities with Part II of the 2000 Act (RIPA). This would include with the content of the Codes of Practice.
- 73.2 Examples of relevant errors occurring would include circumstances where:
- Surveillance activity has taken place without lawful authorisation.
 - There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Surveillance Codes of Practice relating to the safeguards of the material.
- 73.3 All relevant errors made by Public Authorities must be reported to the Investigatory Powers Commissioner by the Council as soon as reasonably practicable and a full report no later than ten working days. The report should include information on the cause of the error; the amount of surveillance conducted, and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

74. Serious Errors

- 74.1 The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless they consider that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

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

75. Complaints

75.1 Any person who reasonably believes they have been adversely affected by surveillance activity by or on behalf of the Council may complain to the Borough Solicitor who will investigate the complaint. A complaint can also be made to the official body which is the Investigatory Powers Tribunal (IPT). They have jurisdiction to investigate and determine complaints against any Public Authority's use of RIPA powers, including those covered by this Policy.

75.2 Complaints should be addressed to:

The Investigatory Powers Tribunal

PO Box 33220

London

SW1H 9ZQ

PART I Relevant case law

76. There is relevant caselaw which includes but is not limited to:

76.1 R v Johnson

In this case the Court of Appeal provided criteria that must be adopted if premises used for observation purposes by the Police are not to be disclosed in open court.

Should FDC wish not to disclose the premises used for the observation, then following the rationale in this case it would appear that the Authorising Officer must be able to testify that immediately prior to trial:

- he/she visited premises to be used for observation;
- he/she obtained and recorded the views of the owner and/or occupier in respect of the use made of the premises and the possible consequences of disclosure; which could lead to identification of the premises and occupiers.

Such views must be recorded and the record marked as sensitive. If this issue arises please contact the Senior Responsible Officer for appropriate advice.

76.2 R v Sutherland 2002

The recording and handling of confidential material (legal privilege) obtained as a result of recording equipment deployed in the exercise area of two police stations. In this matter, the activity exceeded that which had been authorised and the case against Sutherland collapsed. This emphasises the requirement to ensure that all activity is authorised prior to the operation and any errors are reported.

76.3 Peck v United Kingdom [2003]

The applicant was filmed by a CCTV camera operated by Brentwood Borough Council in a public street shortly after he had attempted to commit suicide. The council subsequently released two still photographs taken from the CCTV footage to show the benefits of CCTV. Peck's face was not specifically masked. These pictures subsequently appeared on regional television but his face was masked. Peck sought to challenge the authority's decision but was rejected by the Court of Appeal. He took the matter to the European Court of Human Rights where he was successful. The case establishes the right to privacy in a public area, even if it is a reduced level.

76.4 Martin v. United Kingdom [2004] European Court App

Alleged disorderly behaviour by M towards neighbour. Local Authority mounted covert surveillance of M on the basis that the surveillance by video was justified as the surveillance was targeted at behaviour which was visible to a neighbour or passer by. Claim of Article 8 infringement settled by agreement with damages awarded to Martin.

76.5 R v. Button and Tannahill 2005

Audio and video recording of defendants while in police custody. Audio recording had been RIPA authorised; video recording was not authorised. Video record admitted in evidence although common ground that it had been unauthorised and so obtained unlawfully (in breach of s.6 Human Rights Act 1998). *It was argued on appeal that the trial Court was itself in breach of s.6 by admitting the evidence. Held that the breach of article 8 related to the intrusion upon private life involved in the covert surveillance. So far as a trial Court is concerned: any such breach of article 8 is subsumed by the article 6 (and P.A.C.E.) duty to ensure a fair trial. The trial judge had not acted unlawfully by admitting the evidence.*

76.6 C v The Police and the Secretary of State for the Home Department (2006, No: IPT/03/32/H)

A former police sergeant (C), having retired in 2001, made a claim for a back injury he sustained after tripping on a carpet in a police station. He was awarded damages and an enhanced pension due to the injuries. In 2002, the police instructed a firm of private detectives to observe C to see if he was doing anything that was inconsistent with his claimed injuries. Video footage showed him mowing the lawn. C sued the police claiming that they had carried out Directed Surveillance under RIPA without an authorisation. The Tribunal ruled that this was not the type of surveillance that RIPA was enacted to regulate. It made the distinction between the ordinary functions and the core functions of a public authority:

“The specific core functions and the regulatory powers which go with them are identifiable as distinct from the ordinary functions of public authorities shared by all authorities, such as the employment of staff and the making of contracts. There is no real reason why the performance of the ordinary functions of a public authority should fall within the RIPA regime, which is concerned with the regulation of certain investigatory powers, not with the regulation of employees or of suppliers and service providers

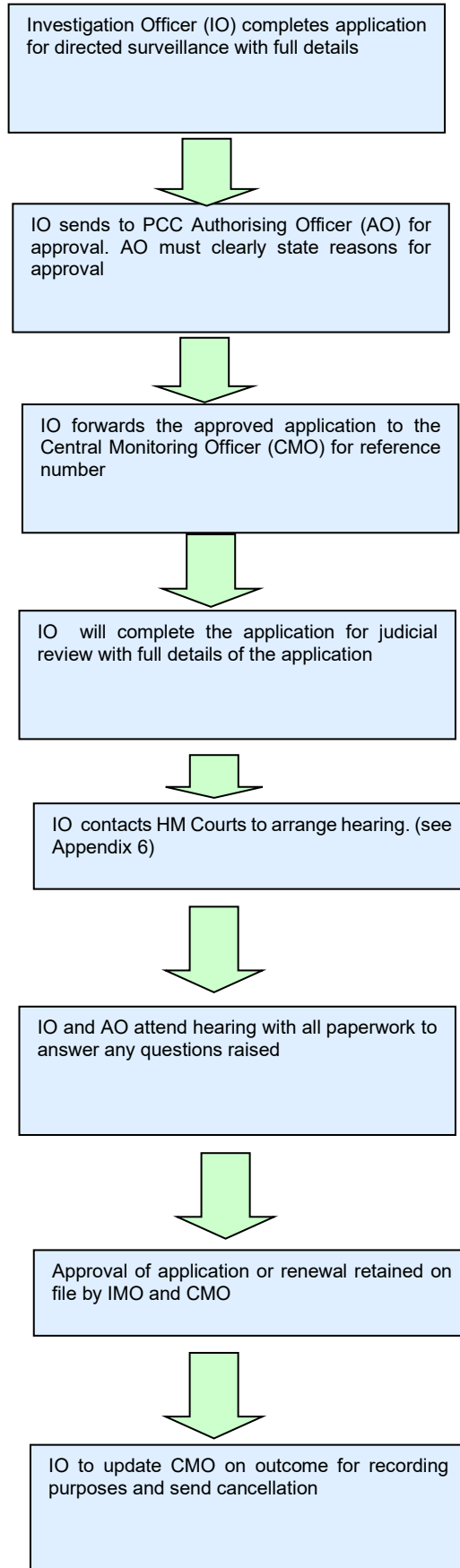
76.7 AB v Hampshire Constabulary (Investigatory Powers Tribunal ruling 5 February 2019)

This case relates to whether the use of body worn cameras can amount to surveillance as defined by legislation. In this matter, the Tribunal concluded that in this case video recording was capable of amounting to surveillance under Part II of RIPA (2000). The decision can be viewed here. <https://www.ipt-uk.com/docs/IPT%20Judgment%20-%20AB%20v%20Hants%20Constabulary.pdf>

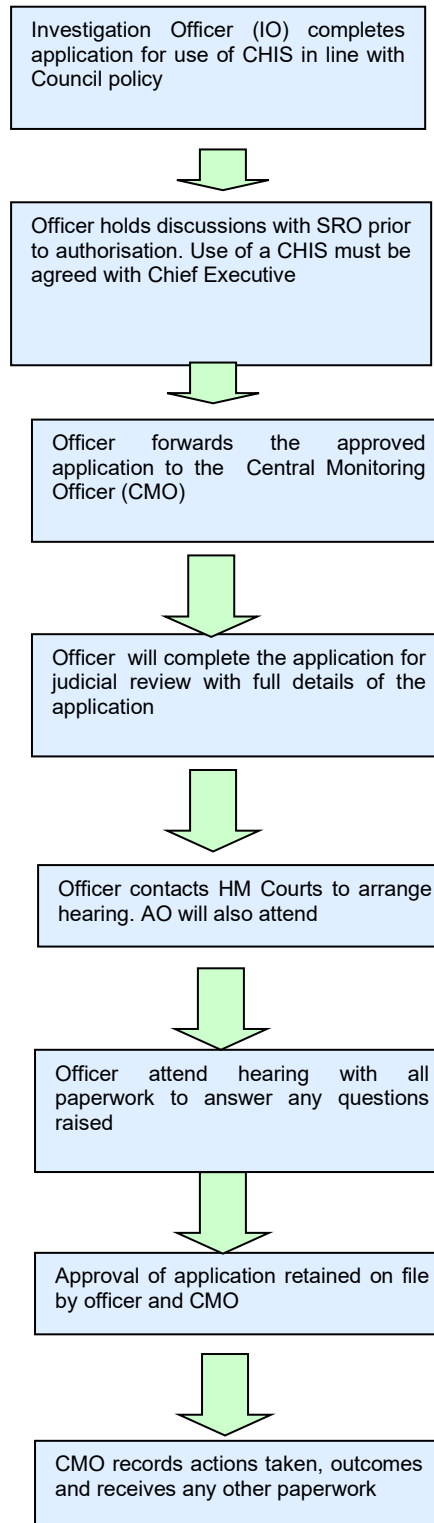
76.8 Gary Davies v British Transport Police (Investigatory Powers Tribunal 5 February 2019)

British Transport Police undertook unauthorised surveillance which led to a public arrest and a press release publicising the alleged offences. Mr Davies was subsequently acquitted by a jury. British Transport Police officers had no proper understanding of the legal requirements for such surveillance and should have obtained authorisation. The surveillance was ruled unlawful. The Tribunal rejected the British Transport Police claim that the breach was technical as authorisation could and would have been obtained. This was rejected because the case against Mr Davies required further inquiries to have been made for authorisation to be possible. The Tribunal awarded Mr Davies costs of the criminal trial and also £25,000 in compensation for damages to his reputation suffered and harm caused.

APPENDIX 1 Procedure for Directed Surveillance Application



APPENDIX 2 Procedure use of Covert Human Intelligence Source



APPENDIX 3 Surveillance Assessment

	Notes
<p>Specific location</p> <ul style="list-style-type: none"> ● Type of property ● Residents ● Number and locations of entrances/exits ● Vehicular access ● Any obstructions ● Any risks 	
<p>General Area</p> <ul style="list-style-type: none"> ● Type of area e.g. residential or commercial ● Shops in locality ● Schools ● Any potential hazards 	
<p>Subject</p> <ul style="list-style-type: none"> ● Identity ● Potentially violent ● Vehicles used ● Any known other sites 	
<p>Collateral intrusion</p> <ul style="list-style-type: none"> ● Detail any other individuals of whom private information may be captured ● Associates ● Family Children ● How will it be limited e.g. times, techniques 	
<p>Observation Point</p> <ul style="list-style-type: none"> ● Is location approved? ● Does it require use of another building? ● Routes to and from 	

<ul style="list-style-type: none"> • In event of discovery of operation, agreed movement 		
<p>Equipment</p> <ul style="list-style-type: none"> • What is being used? • Do they work? • Any issues regarding signal reception on phones 		
<p>Health and Safety Assessment</p>		
<p>Hazard (including who may be harmed)</p>	<p>Level of Risk</p>	<p>Mitigating controls</p>

APPENDIX 4 - Social Media/Internet Access Log

Name of Applicant		Team	
Service			
Directorate			
Line Manager			
Case including reference			

Visits number	Date	Site Accessed	Reason	Information obtained	Public or Private?

Please note repeated visits will be considered monitoring and you should seek advice on making an appropriate application. You should not use a false identity or build/maintain a relationship to obtain private information about someone. If you have obtained private information then you should consider an appropriate application.

INVESTIGATING OFFICER	SIGNATURE	DATE
LINE MANAGER	SIGNATURE	DATE

APPENDIX 5

RIPA/CHIS: AUTHORISATION DATA - SAFEGUARDING GUIDANCE

WHAT CAN WE KEEP?



ALL DOCUMENTS AND CORRESPONDENCE REQUIRED TO SUPPORT THE APPLICATION AND APPROVAL PROCESS TO INCLUDE:

- The original application and (1) if granted, the type and date of authorisation or (2) if not granted, the reasons for refusal;
- The name, title and contact details of the Authorising Officer;
- The URN of the investigation or operation together with its title and a brief description/overview of its purpose;
- Details of attendances at the Magistrates Court together with notes of the hearing to include the date, time and name of the Judge and, the Judicial Application and Order;
- frequency and result of reviews and renewals together with the details of those involved in the process to include name, title and contact details;
- Details as to the period of the surveillance and any instruction to stop together with the details of those involved in the process to include name, title and contact details;
- Whether confidential information is likely to be obtained and, if it is obtained, ensure that it is identified and processed accordingly;
- Any other instructions given by the Authorising Officer together with a specific record of any instances when the Authorising Officer is also involved in the investigation (these to be specifically reported to the Commissioner).
- **NO MORE INFORMATION THAN IS NEEDED SHALL BE RETAINED.**

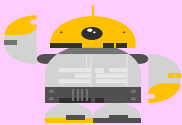
WHO CAN KEEP IT?



A CENTRALLY HELD RECORD MUST BE KEPT, UPDATED AND REVIEWED BY THE RIPA COORDINATOR

- All information must be provided to the RIPA co-ordinator as soon as possible but in any event **within 48 hours**;
- Paper records should be addressed to the RIPA co-ordinator in a sealed envelope marked **Strictly Private and Confidential**;
- Electronic records should be sent securely within the Council's network or, if external, via a Clinked File **marked Strictly Private and Confidential**;
- So far as achievable, the RIPA Co-Ordinator's central record will be kept electronically. A separate folder will be kept for each authorisation and each folder will be password protected.
- Passwords will only be provided to those officers with a need to know the content of the folder and where it is not necessary for them to know the whole content, the RIPA-Coordinator will either provide a summary or an extract using secure means.
- Only where it is necessary for paper records to be kept will they be kept. These records will be kept in a locked filing cabinet for which access will be limited to the RIPA Co-Ordinator, SIRO and Authorising Officers.
- **NO OTHER RECORDS WILL BE KEPT AND NO RECORDS SHOULD BE SHARED WITH ANYONE OUTSIDE THE PROCESS.**

HOW LONG SHOULD WE KEEP IT FOR?



THE RIPA-COORDINATOR WILL DECIDE HOW LONG THE DATA SHOULD BE KEPT. THE DECISION WILL BE TAKEN IN ACCORDANCE WITH THE COUNCIL'S RIPA AND DATA RETENTION POLICIES

- The central record for each authorisation will be retained for 3 years from the ending of the authorisation.
- Where a conviction is secured the central record for that authorisation will be retained for at least 6 months from the date of sentence;
- Where a custodial sentence is imposed, the central record for that authorisation will be kept until the person is released from custody or 6 months from the date of conviction, whichever is the greater;
- If the person appeals their conviction, all material which may be relevant must be kept until the appeal is determined even if that exceeds the ordinary period for retention.
- **NO DATA WILL BE KEPT FOR ANY LONGER THAN IS NECESSARY.**

REVIEWING AND DISPOSING OF THE DATA



THE RIPA COORDINATOR WILL REVIEW THE CENTRAL RECORD AND WILL ARRANGE FOR THE SAFE DISPOSAL OF THE DATA RELATING TO EACH AUTHORISATION ONCE THE RELEVANT RETENTION PERIOD HAS PASSED.

- The RIPA Co-Ordinator will review the central record of authorisation annually from the date of the application or following each relevant stage in the enforcement process e.g. summons, trial, sentencing, appeal. Any information which the RIPA Co-Ordinator considers is no longer required will be securely destroyed.
- The RIPA Co-Ordinator will schedule a destruction date for each authorisation in accordance with the RIPA and Retention Guideline Policies. On that date the RIPA Co-Ordinator will make enquiries with the Investigating Officer as to whether there have been any developments (such as an appeal) which mean that the central record should be retained for longer.
- Where the RIPA Co-ordinator is satisfied that the documentation is no longer required, they will arrange for its secure destruction. Paper records will be disposed of in the Council's confidential waste bins and electronic records will be deleted with assistance from ICT so as to ensure that the record is permanently removed.
- **DATA WILL BE SECURELY DESTROYED WHEN IT IS NO LONGER LEGALLY REQUIRED TO BE RETAINED.**

Agenda Item No:	9	
Committee:	Audit and Risk Management Committee	
Date:	12th February 2024	
Report Title:	Corporate Risk Register Review	

1 Purpose / Summary

- 1.1 To provide an update to the Audit and Risk Management Committee on the Council's Corporate Risk Register.

2 Key Issues

- 2.1 The Council's Risk Management Strategy ensures the effective maintenance of a risk management framework by:-
- embedding risk management across core management functions;
 - providing tools to identify and respond to internal and external risk;
 - linking risks to objectives within services and regularly reviewing these.
- 2.2 The Audit and Risk Management Committee has asked that the Council's Corporate Risk Register is reviewed and presented to it quarterly.
- 2.3 The latest Corporate Risk Register (**Appendix A**) is attached to this report.

3 Recommendations

- 3.1 The latest Corporate Risk Register is agreed as attached at Appendix A to this report.

Wards Affected	All
Forward Plan Reference	N/A
Portfolio Holder(s)	Cllr Chris Boden – Leader and Portfolio Holder for Corporate Governance
Report Originator(s)	Stephen Beacher – Head of ICT, Digital & Resilience
Contact Officer(s)	Paul Medd – Chief Executive Peter Catchpole –Corporate Director & Chief Finance Officer Stephen Beacher – Head of ICT, Digital & Resilience
Background Paper(s)	Previous reviews of the Corporate Risk Register: minutes of Audit and Risk Management Committee

1 Background / Introduction

1.1 This is the latest quarterly update in respect of the Corporate Risk register.

2 Considerations

2.1 The Council has seven considerations when considering risk:-

- Performance – can we still achieve our objectives?
- Service delivery – will this be disrupted and how do we ensure it continues?
- Injury – how do we avoid injuries and harm?
- Reputation - how is the Council's reputation protected?
- Environment – how do we avoid and minimise damage to it?
- Financial – how do we avoid losing money?
- Legal – how do we reduce the risk of litigation?

2.2 Members and Officers share responsibility for managing risk:-

- Members - have regard for risk in making decisions
- Audit and Risk Management Committee – oversee management of risk
- Corporate Management Team – maintain strategic risk management framework
- Risk Management Group – Lead Officers across the Council promote risk management and a consistent approach to it
- Managers – identify and mitigate new risks, ensure teams manage risk
- All staff – manage risk in their jobs and work safely.

2.3 Risk is scored by impact and likelihood. Each have a score of 1-5 reflecting severity. The overall score then generates a risk score if no action is taken, together with a residual risk score after mitigating action is taken to reduce risk to an acceptable level.

2.4 The level of risk the Council deems acceptable is the “risk appetite”. The Council accepts a “medium risk appetite” in that it accepts some risks are inevitable and acceptable whereas others may not be acceptable.

2.5 Managers consider risks as part of the annual service planning process. Each service has a risk register with the highest risks being reported at a strategic level, forming the Corporate Risk Register. The Corporate Management Team, supported by the Risk Management Group, ensures that the highest risks are regularly reviewed and mitigating action undertaken.

2.6 The Corporate Risk Register is very much a “living document”; the Audit and Risk Management Committee reviews it quarterly.

2.7 Where exceptional new risks present themselves, they can be referred to Audit and Risk Management Committee urgently as appropriate.

- 2.8 Risk appetite has been considered. The Council takes a medium risk appetite, accepting that the current climate in Local Government is subject to great change and that some risks are necessary in order for the Council to move forward and continue to deliver high quality, cost-effective services.

As a result of this, in some instances it is not possible to significantly reduce residual risk. Having said this, some decisions may need to be made in a timely manner and this could increase risk appetite accordingly. The Council's overall risk appetite should be reviewed regularly.

- 2.9 Risk awareness is embedded across the Council and it is important that risk awareness and management is integral to the Council's culture. To achieve this, risk awareness and training are important.
- 2.10 It is important that Members have regard for risk when considering matters and making decisions at Council, Cabinet and Committees. In addition, Audit and Risk Management Committee must take a strategic overview of risk and consider the highest risks to the Council as set out in the Corporate Risk Register.

3 Changes to the Corporate Risk Register

- 3.1 The Risk Register has been reviewed by the Corporate Risk Management Group and Corporate Management Team, with all recommended changes highlighted in green.
- 3.2 Mitigating actions and progress have been updated.
- 3.3 Commentary regarding all risks and action being taken to ensure current risks are minimised has been updated in the Risk Register.
- 3.4 All updates are highlighted in green.
- 3.5 The register also includes some narrative around the Risk Management Process (at section 2); the Monitoring and Escalation Framework (at section 4); the Risk Appetite and tolerance levels; and a heat map showing all the residual risks at page 28.

4 Next Steps

- 4.1 Officers will continue to bring a reviewed and updated Corporate Risk Register to Audit and Risk Management Committee on a regular basis.

5 Conclusions

- 5.1 The risk management process provides assurance for the Annual Governance Statement, which is substantiated by reports from the Council's External Auditors in their issuance of an unqualified audit opinion.
- 5.2 Regular review (and updating as appropriate) of the Risk Management Strategy and Corporate Risk Register will further build the assurance required above.

Corporate Risk Register

Reviewed and updated February 2024



1 Introduction

- 1.1 This is the latest Corporate Risk Register. Please refer to the Council's Corporate Risk Strategy for further information about how the Council approaches risk management. Actions and comments for each risk have been revised and other changes are highlighted in green.

2 Risk Management Process

- 2.1 Risk Management is designed to identify what could affect the achievement of objectives, and to plan a proportionate response.
- 2.2 The Council's approach to Risk Management is documented within the Risk Management Framework. It aims to ensure that risks are identified for both strategic and operational activity. This includes:
- corporate and service priorities;
 - project management;
 - decision-making and policy setting; and
 - financial and performance monitoring and planning.
- 2.3 The Risk Management Framework provides tools to manage risks for the different types of system and control environment, such as the Corporate Risk Register to capture and summarise significant and strategic risks; team risk registers which help inform service planning and actions; risk and hazard identification documents are shared with management as appropriate during audit reviews; and health and safety risk assessments which are updated annually by teams.
- 2.4 The frequency and mechanism for monitoring risks reflects the type of monitoring system, and the pace of changing circumstances, for example:
- Project risks will be recorded in project risk registers and are reviewed frequently throughout the project's life.
 - Operational risks are identified through audit and inspection work and are assigned dates and ownership.
 - Operational risks are identified through service planning and are linked to the service plan actions. These are typically monitored monthly through team meetings as part of the Councils Performance Management framework.
- 2.5 The Annual Governance Statement records governance actions, which are reviewed biannually as good practice. The Corporate Risk Register comprises strategic and significant risks. The register can both inform and reflect risks recorded in other risk management systems. It may refer to more detailed analysis of risks, presented to committees, such as the Medium-Term Financial Strategy. Appropriately, mitigation may be linked to specific actions recorded and monitored through service plans, or committee forward plans.
- 2.6 Risks are categorised and scored according to their impact and likelihood. This activity allows managers, to prioritise resources to mitigate them. Strategic and significant risks are defined by the Councils risk appetite.
- 2.7 The outcomes of this process are reported to the Audit and Risk Management Committee at least twice each year in the form of the attached Corporate Risk Register.
- 2.8 The review of the Risk Management Framework, Policy and Strategy, will be reported to the Audit and Risk Management Committee at least annually. The Risk Management process, and register, will provide assurance for the Annual Governance Statement.

3. How Risks Are Scored

- 3.1 The Council has adopted a consistent scoring mechanism for all risk identification, as it enables risks identified from other systems to be escalated to the Corporate Risk Register.
- 3.2 The probability - “likelihood”, and effect - “impact”, of each risk must be identified in order to help assess the significance of the risk and the subsequent effort put into managing it.
- 3.3 The risk score is calculated by multiplying the impact score by the likelihood score:

IMPACT	
Score	Classification
1	Insignificant
2	Minor
3	Moderate
4	Major
5	Catastrophic



LIKELIHOOD	
Score	Classification
1	Highly unlikely
2	Unlikely
3	Possible
4	Probable
5	Very likely

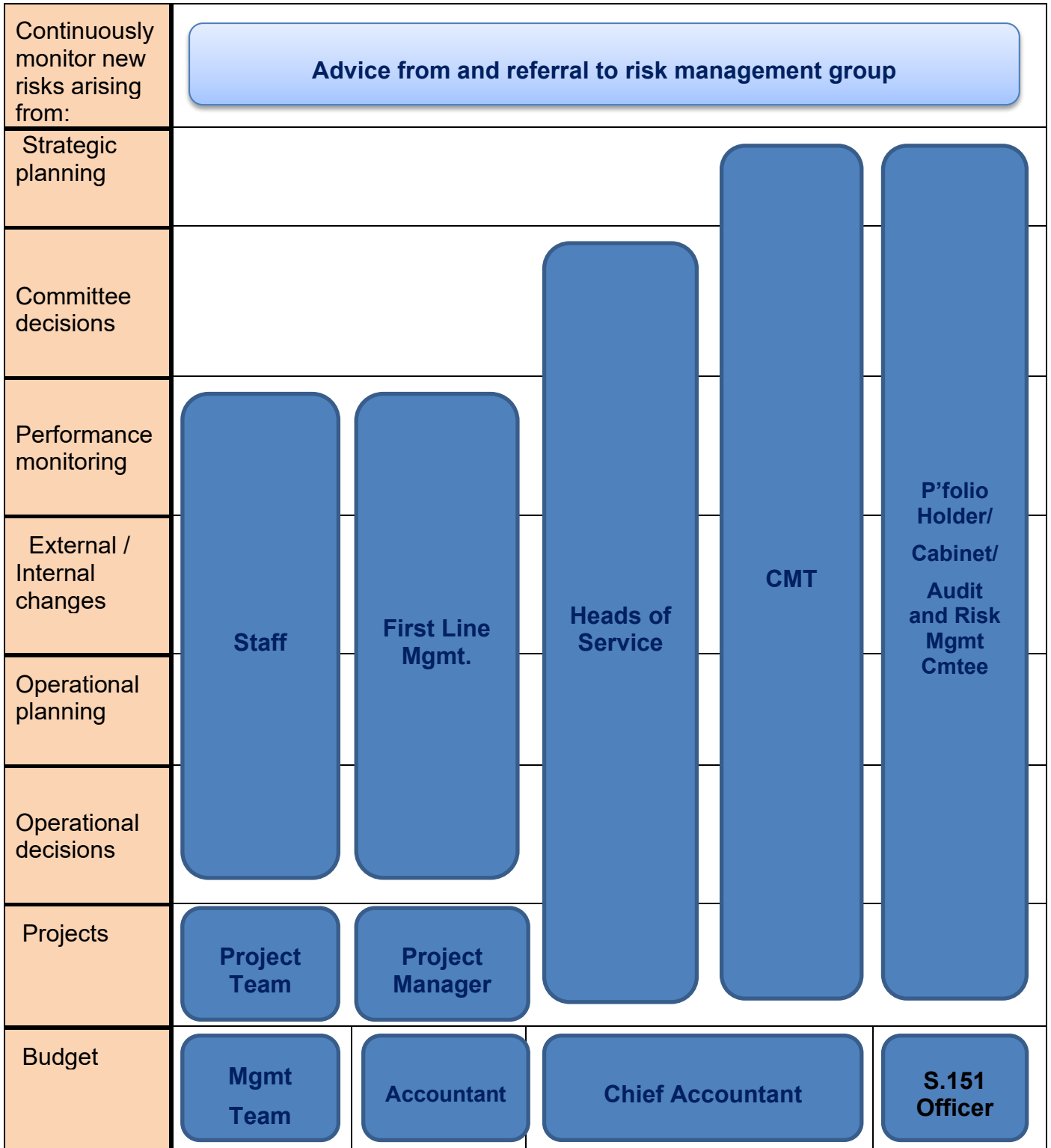
IMPACT x LIKELIHOOD = RISK SCORE

3.4 The impact and likelihood of risks is scored with regards the below levels:-

Score	1	2	3	4	5
Criteria	Insignificant impact	Minor impact	Moderate Impact	Major Impact	Catastrophic Impact
Performance	Objectives still achieved with minimum extra cost or inconvenience	Partial achievement of objectives with compensating action taken or reallocation of resources.	Additional costs required and or time delays to achieve objectives – adverse impact on PIs and targets.	Unable to achieve corporate objectives or statutory obligations resulting in significant visible impact on service provision such as closure of facilities.	Unable to achieve corporate objectives and/or corporate obligations.
Service Delivery	Insignificant disruption on internal business – no loss of customer service.	Some disruption on internal business only – no loss of customer service.	Noticeable disruption affecting customers. Loss of service up to 48 hours.	Major disruption affecting customers. Loss of service for more than 48 hours.	Loss of service delivery for more than seven days.
Physical	No injury/claims.	Minor injury/claims (first aid treatment).	Violence or threat or serious injury/claims (medical treatment required).	Extensive multiple injuries/claims.	Loss of life.
Reputation	No reputational damage.	Minimal coverage in local media.	Sustained coverage in local media.	Coverage in national media.	Extensive coverage in National Media.
Environmental	Insignificant environmental damage.	Minor damage to local environmental.	Moderate local environmental damage.	Major damage to local environment.	Significant environmental damage attracting national and or international concern.
Financial	Financial loss < £200,000	Financial loss >£200,000 <£600,000	Financial loss >£600,000 <£1,000,000	Financial loss >£1,000,000 <£4,000,000	Financial loss >£4,000,000
Legal	Minor civil litigation or regulatory criticism	Minor regulatory enforcement	Major civil litigation and/or local public enquiry	Major civil litigation setting precedent and/or national public enquiry	Section 151 or government intervention or criminal charges

4. Monitoring and Escalation Framework

4.1 The following diagram illustrates the key stakeholders for different classification of risk management:



5.0 Risk Appetite and Tolerance Levels

- 5.1 Risk appetite and tolerance is the amount of risk an organisation is prepared to accept, or be exposed to at any point in time. It can indicate where action is required to reduce risk to an acceptable level, plus opportunities for positive outcomes which can be monitored.
- 5.2 The Council has adopted the approach and definitions used by CIPFA and the Institute of Risk Management:

Risk Appetite

“The amount of risk an organisation is willing to seek or accept in the pursuit of its long-term objectives”.

An example may be consideration of the funds or resources that an organisation is prepared to invest in a venture where success is not guaranteed but that would yield benefits.

Risk Tolerance

“The boundaries of risk taking outside which the organisation is not prepared to venture in the pursuit of its long-term objectives”.

An example may be a Treasury Management Strategy that rules out certain types of investment options.

- 5.3 Typically an individual’s perception of an acceptable risk is the same irrespective of which definition is used. Differences may occur where risks cannot be controlled or completely eliminated. For example, political and legislative change is an external driver which cannot be fully mitigated. In this instance the risk tolerance, and ability to manage the risk, may be greater than risk appetite.
- 5.4 It is recognised that the tolerance or appetite is subjective, and may change according to the environment, internal and external drivers. Consequently, it is important, regardless of the terms used, that everyone has a consistent approach to risk taking to prioritise resources effectively.
- 5.5 The Councils risk appetite is set by the Corporate Management Team (CMT) and is reviewed periodically. This provides guidance to everyone on acceptable levels of risk taking, to encourage a consistent approach to risk management.
- 5.6 Different risk appetites can be illustrated on a five-by-five matrix as three levels: high, medium and low. The Council is risk aware and the current level is determined by CMT as medium. This provides guidance that any inherent risk scored at 15 or greater is to be considered for the Corporate Risk Register.
- 5.7 Once controls are in operation the risks can be scored again to illustrate the residual risk.

6. The Corporate Risk Register at a Glance

6.1 Please see below for a summary of current risks and their scores. More detail follows in section 7 of this document, in which the individual risks are ordered by severity of current risk, in descending order.

Ref	Risk	Risk if no action			Current risk			Page in this register
		Impact	Likelihood	Score	Impact	Likelihood	Score	
8	Funding changes make Council unsustainable	5	5	25	4	5	20	8
3	Failure of contractors / suppliers working on the Council's behalf	4	4	16	4	4	16	9
9	The Council's ability to cope with a natural disaster	5	4	20	4	4	16	10
4	Loss of access to data / systems required for service delivery	5	5	25	4	3	12	11
5	Insufficient staff to provide Council services	4	5	20	3	4	12	12
6	Breach of ICT security, ICT failure, causing loss of service	5	5	25	4	3	12	13
16	Service provision affected by organisational change	4	5	20	3	4	12	14
17	Legislative changes in national political priorities	5	4	20	3	4	12	15
18	Capital funding strategy failure	5	5	25	3	4	12	16
1	Legislative changes	5	5	25	2	5	10	17
10	Major health and safety incident	4	4	16	3	3	9	18
11	Fraud and error committed against the Council	5	4	20	3	3	9	19
13	Failure of Governance in major partners or in the Council as a result of partnership working	4	5	20	3	3	9	20
14	Failure to achieve required savings targets	4	5	20	3	3	9	21
19	Poor communications with stakeholders	4	5	20	3	3	9	22
20	Failure of the Council's Commercialisation and Investment Strategy	5	4	20	3	3	9	23
7	Lack of access to Council premises prevents services being delivered	4	5	20	2	4	8	24
12	Failure of external investment institutions	5	4	20	2	4	8	25
21	The Council's failure to deal with an infectious disease and/or a pandemic situation.	5	5	25	2	4	8	26
15	Over-run of major Council projects in time or cost	4	5	20	3	2	6	27

7 Corporate Risk Register

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
8	<p>Risk: - Funding changes make Council unsustainable</p> <p>The current impact of inflation and how this may present additional pressures to the Council's overall finances.</p> <p>Effects: - Economic changes, imposed savings requirements, changes to local government funding systems.</p> <p>Financial management of NNDR, CTS leads to change in income /spending making Council unsustainable.</p>	5	5	25	<ul style="list-style-type: none"> • S151/ Chief Finance Officer • Financial Regulations & Standing Orders • Appropriately trained staff • MTFS • Professional economic forecasts • Community consultation on service priorities • Our Council for the Future programme • Political decisions linked to budget strategies. • CMT efficiency planning • Modernising Council Services transformation programme • Introduction of Transformation Agenda 2 (TA2) • Executive steer of service /capital priorities. • Review fees /changes. • Reserves • Financial Mgmt System • Budget monitoring. 	4	5	20	<p>Peter Catchpole</p> <p>MS/SW</p>	<ul style="list-style-type: none"> • Using intelligence to model and plan for future changes and risks and move away from reliance on Govt funding to balance our budget. • Regular monitoring of current position and reporting to Members. • Workforce planning covers all scenarios. • Inclusion in national working groups, modelling and lobbying for funding system after RSG ceases. • Sharing Council's Efficiency Plan with the Government allows guaranteed multi-year grant settlement raising funding certainty. • Shared services and partnership working • Pursuing all opportunities for external funding • Commercial and Investment Strategy 	<p>We closely monitor information received from government and relevant interest groups and sector representatives regarding anticipated changes in the financing of local government. Our Medium-Term Financial Plan articulates the key risks to the Council arising from potential changes in the current arrangements. The MTFP forecasts the gap between the cost of delivering Council services and the resources available, including any planned use of Council reserves.</p> <p>The Fair Funding Review and Business rate Retention Scheme are still delayed. Some potential for this to impact on the Council's long-term financial position remains particularly if changes are made to the underlying formulas which determine how central government funding is allocated to local authorities.</p> <p>The Council has an agreed Commercialisation and Investment Strategy which will enable the Council to generate additional income. This provides a framework to determine which investment opportunities can be taken forward. Some income-generating investments have been made. However, the challenging economic outlook, particularly in respect of inflation and rising financing costs, is likely to reduce, at least in the short-term, the commercial viability of some planned investments.</p> <p>Each service is required to review and identify any opportunities for transformation, commercialisation and efficiency. The Council has now delivered Phase 2 of the 'Modernising Council Services' programme which is on target to deliver significant savings over the Council's current MTFP period. We have now started delivering the next phase of this transformation programme.</p> <p>Government provided financial support to local authorities which offset the impact of additional costs and reductions in income experienced as a consequence of the pandemic. It is unclear to what extent government will be able and willing to provide the same level of financial support in response to the current economic challenges. Additional funding was made available in 2022-23 to mitigate against significant rises in IDB levies and a similar amount is expected in 2023-24.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
3	<p>Risk: - Failure of contractors / suppliers working on the Council's behalf.</p> <p>Effects: - Failure of contractor or partners to deliver services or meet agreed performance objectives leads to additional costs or failed objectives.</p>	4	4	16	<ul style="list-style-type: none"> • Procurement processes, including financial aspects/ contract standing orders / equality standards. • Contract process – creation of robust contracts. • Accountability and risk ownership documented. • Service Level Agreements. • Contract monitoring. • Trained/skilled staff. • Project management. • Relationship Management. • Business Continuity Plans. 	4	4	16	<p>CMT</p> <p>All Mgrs</p>	<ul style="list-style-type: none"> • Regular monitoring of contracts and performance by Managers. • Ensure that contracts have risk registers and mitigation in event of contract failure. • Ensure all contractors have reviewed and refreshed their business continuity arrangements and plans in light of the pandemic. • Individual Council services share their own contingency to cover for contractor failure, and this is part of the Business Continuity Plan for each Service Area. • Potential contractors and suppliers are always checked for financial stability and business continuity by the Accountancy/ Procurement teams before contracts are let. 	<p>FDC has arrangements in place to manage / monitor the performance of the Tivoli Grounds Maintenance contract and the Freedom Leisure contract.</p> <p>All other shared services/contracts have a full review and governance process in place to ensure ongoing delivery and performance standards.</p> <p>The cost of living and energy crises form a significant challenge to the leisure business. Freedom Leisure and FDC are monitoring the situation closely and are working together to mitigate impact on the services provided to the local community in Fenland.</p> <p>Refresher training on procurement to be delivered to all awarding managers.</p> <p>Process of due diligence checks to be implemented for all relevant contracts and/or suppliers.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
9	<p>Risk:- The Council's ability to cope with a natural disaster or any emergency event</p> <p>Effects:- Natural disaster, malicious or accidental incident affects support required by civilians or disrupts existing Council services.</p> <p>Failure to maintain robust emergency planning.</p>	5	4	20	<ul style="list-style-type: none"> •Emergency plan •Emergency planning exercises beyond the district •Business continuity plans •Regular exercise and joint public sector workshops for Emergency Planning •Emergency Planning Communication s Strategy •Review of approach with partner organisations as a result of lessons learned from 'near-miss' flood events. •Local Resilience Forum 	4	4	16	CMT SB/DV	<ul style="list-style-type: none"> • Regularly test Emergency Plan • Test Service Business Continuity Plans • Ensure key emergency planning staff attend regular liaison meetings and training. • Ongoing management response group and regular conference call and action planning. 	<p>Management Team conduct periodical exercise to test the Council's readiness for an emergency.</p> <p>The Council's Emergency Management and Rest Centre Plans have been updated and we have increased and trained the number of volunteer rest centre staff available.</p> <p>Rest Centre training was carried out earlier this month and Internal Audit have begun a review of our Business Continuity processes.</p> <p>The Council will retain the use of each of the four Leisure Centres for rest centre sites.</p> <p>The Council has implemented a rota for senior officers to be 'on call' at Gold (Strategic), Silver (Tactical) and Bronze (Operational) levels to respond in the event of an emergency.</p> <p>The Council's response to any emergency situation will complement and support the coordinated CPLRF response to any such incident.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
4	<p>Risk: - Loss of access to data / systems required for service delivery.</p> <p>Effects: - Failure to secure and manage data leads to loss of / corruption of / inaccuracy of data, results in disruption to services.</p> <p>A further consequence could be financial penalties and reputational risk.</p>	5	5	25	<ul style="list-style-type: none"> • Data protection policy and procedure. • Freedom of Information publication scheme. • Data retention policy and procedure for archive and disposal. • Information breach response plan. • Monitoring Officer role comprises Senior Information Risk Officer function. • Business continuity plans. • ICT system security. • Public Services Network compliance. • Paperless office project. • Countywide information sharing framework. 	4	3	12	<p>Carol Pilson / Peter Catchpole</p> <p>SB/AB</p>	<ul style="list-style-type: none"> • Effective auditing of systems and data held. • Data backed-up securely off-site. • Regular penetration testing. • Regular review of business continuity plans • Disaster Recovery testing is undertaken at regular intervals • Additional ICT resource has been recruited 	<p>An additional internet feed to Fenland Hall has been installed to improve resilience.</p> <p>Resilience has been built into most of our ICT infrastructure.</p> <p>Consideration is given, when a new system is procured or replaced, as to whether it would be more appropriate to host this within the cloud in terms of resilience, capacity, performance, and cost.</p> <p>The Council has an Information Asset Register of all records it holds in both paper and electronic form, worked with IT system suppliers and conducted a staff awareness campaign to ensure that staff understand and are compliant with GDPR.</p> <p>The majority of information held by the Council is held with a legal basis for holding such as election and Council Tax records. All staff undergo GDPR training, and opportunities for further Member training in this area are currently being explored.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
5	<p>Risk:- Insufficient staff to provide Council services</p> <p>Increased competition from other regional and national employers from the same workforce pool.</p> <p>Insufficient leadership and/or management capacity to deliver Council priorities</p> <p>Effects:- Constraints to effective workforce planning lead to poor standards of service or disruption to service. Service transformation and commissioning can help build resilience but could also lead to a loss of qualified and knowledgeable staff, which exposes the council to risk of service failure and legal challenge.</p>	4	5	20	<ul style="list-style-type: none"> • Learning & Development framework / Training • Working environment /culture • Staff Committee • MTSP • Flexible working • Established suite of people policies & Procedures • Business continuity plans • Management training • 121s /Springboard staff development and appraisals • Service planning process • Access to interim staff via frameworks • Effective sickness management • Effective Governance structures 	3	4	12	<p>CMT</p> <p>SA/All Mgrs</p>	<ul style="list-style-type: none"> • Ensure all services have effective Workforce plans incorporated into Service Plans, which ensure all work is prioritised • Effective succession planning. • Effective use of project management approaches/ principles when delivering priorities/ strategies 	<p>All services are required to publish service plans, learning requirements and workforce plans to ensure teams are staffed according to current establishment and to take account of priorities and longer-term trends.</p> <p>All service Business Continuity Plans have been updated to ensure that key, priority and statutory services can be maintained in the event of a significant loss of staff through illness or absence.</p> <p>Almost all office-based staff have the necessary equipment to be able to work from home, which will maintain the delivery of a significant number of Council services. Other key/priority services have individual Business Continuity measures in place to maintain service delivery.</p> <p>A mapping exercise of all key processes is continuing to automate and e-enable where possible to increase and further improve Council resilience.</p> <p>As part of the transformation journey, we are working towards being more reactive to customer demands/needs.</p> <p>Even with mitigation in place the challenges of attracting, recruiting and retaining staff is becoming increasingly difficult.</p> <p>As part of the Transformation programme, individual service reviews have commenced and will consider this issue as part of the process.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
6	<p>Risk: - Breach of ICT security, ICT failure, causing loss of service.</p> <p>Effects: - Major IT physical hardware failure or electronic attack, such as viruses, hacking or spyware, causes disruption to services and breaches of security. A further consequence could be financial penalties and reputational risk.</p>	5	5	25	<ul style="list-style-type: none"> • Anti-virus software • Geographically distributed servers • Tested disaster recovery plan • Back-ups stored off-site. • Secondary power supply • Revised security policies • Critical services' business continuity plans include manual operation. 	3	4	12	Peter Catchpole SB/AB	<ul style="list-style-type: none"> • Effective auditing of systems and data held. • Data backed-up securely off-site. • Regular penetration testing. • Likelihood of a breach is reduced by above mitigation 	<p>The Council subscribes to the National Cyber Security Centre's (NCSC) Web Check service that helps public sector organisations fix website threats. This service regularly scans public sector websites to check if they are secure. NCSC have advised that the Fenland Council site is secure.</p> <p>Council IT systems and website are as secure as possible with current anti-attack software and processes up to date. When vulnerabilities are made known by software vendors, software is updated to reduce the risk of malicious attack.</p> <p>The likelihood score reflects the increase globally of cyber-crime.</p> <p>All Council employees are currently undertaking Cyber security training.</p> <p>Elected Members to undergo GDPR refresher training.</p> <p>FDC have contributed towards this plan and a multi-agency exercise took place in November to test this plan.</p> <p>Our ICT infrastructure and processes are accredited against the PSN Code of Connection, PCI DSS, and Cyber Essentials Plus certification.</p> <p>Internal and external independent penetration testing is regularly carried out to demonstrate our processes and security stance are adequate.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
16	<p>Risk:- Service provision affected by organisational change.</p> <p>Effects:- Service provision and performance affected by organisational change, industrial action and/or staff sickness resulting in complaints, poor performance and possible further costs.</p>	4	5	20	<ul style="list-style-type: none"> Working environment / org culture Audit & Risk Management Committee Consultation with Management, Trade Union and Staff Partnership group (MTSP) Flexible working Established suite of people policies & procedures Business continuity plans Management training “Springboard” appraisal for all staff support and development Robust human resource management procedures, which are considered at CMT level. Regular performance monitoring and management Access to interim arrangements Robust sickness absence management Project management processes 	3	4	12	<p>Peter Catchpole</p> <p>All Mgs</p> <ul style="list-style-type: none"> Robust management of all organisational change. Business continuity plans for each service. Culture of Council remains effective. Workforce planning, which includes succession planning for key roles an talent management A comprehensive programme of health surveillance for groups of employees who work in certain service areas (e.g. refuse drivers, workshop, port staff, etc.) Trained Mental Health First Aiders in place. Stress awareness training Resilience training Staff engagement and consultation processes Likelihood is reduced based on mitigating actions 	<p>All services have Business Continuity Plans in place which are regularly updated.</p> <p>All organisational changes must be supported by a full rationale and business cases and are present to and considered by the senior management; If approved, the proposed change is subject to consultation process, and then progressed and managed by a wider project group to ensure all service provision issues are properly considered and managed. This project management approach is maintained for all such changes/programmes, and is supported by communication, engagement and training support for staff groups affected.</p> <p>The Council has a health and wellbeing programme in place which supports the existing suite of Policies, Codes of Practices and processes, this includes a wide range of support to help promote and encourage their good health and wellbeing.</p> <p>Actions agreed from the most recent wellbeing survey include:</p> <ul style="list-style-type: none"> All managers will be invited to attend a two-day Mental Health First Aid course. All employees will be invited to a half-day Mental Health Awareness course. All new employees will be required to attend the training as part of their induction to the Council. Upskilling our managers to assist in the management of a remote workforce and support the wellbeing of their teams. <p>As part of the corporate Transformation programme, individual service reviews have commenced and will consider any issues as part of the process.</p>	

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
17	<p>Risk:- Legislative changes in national political priorities</p> <p>Effects:- Changes in national political priorities may result in immediate changes that require additional resource to achieve and fail to reflect priorities determined by consultation.</p>	5	4	20	<ul style="list-style-type: none"> • Financial & workforce planning. • Monitoring by CMT and resultant Cabinet reports. • Clear corporate planning and regular performance monitoring. • Effective service & financial planning. • Respond to national consultation on key policy changes. • Membership of LGA as a Council Outside Body. 	3	4	12	Paul Medd	<ul style="list-style-type: none"> • Understanding and acting on intelligence from LGA, CIPFA and other local government sources. • Resources identified, approved and implemented without delay. • Constant monitoring. • Horizon scanning via professional bodies. • Joint/collaborative working. 	<p>The likelihood of legislative change remains high. We are keeping a watching brief as any changes are announced.</p> <p>We are monitoring expected legislative changes which may arise after the introduction of the Procurement Act which will replace the current EU law-based procurement regulations and lay down new rules and procedures for selecting suppliers and awarding contracts.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
18	<p>Risk:- Capital funding strategy failure.</p> <p>Effects:- Financial risks of capital funding shortfalls leading to increased burden to the Council. Potential for marginal deficit in capital program if future funding is not realised.</p>	5	5	25	<ul style="list-style-type: none"> Asset Mgmt Plan Asset disposal linked to capital programme. Corporate Asset Team CMT monitoring of capital receipts/effect on capital programme. Regular Cabinet review of the capital programme, member with responsibility for assets Additional funding opportunities identified and pursued where possible. Project lead monitors site valuations linked to econ' dev' proposals. Marketing and identification of potential land purchasers, flexibility of planning guidance aligned to market needs. Continued consultation with econ partners 	3	4	12	<p>Peter Catchpole</p> <p>MS/SW</p>	<ul style="list-style-type: none"> Forward planning and horizon scanning. Regular high-level monitoring of direction of travel and mitigation required. Asset Management Plan. Asset Disposal Strategy. 	<p>The Council's capital funding programme is regularly reviewed by Officers and by Cabinet.</p> <p>The current projected funding deficit will be met by borrowing and the relevant annual financing cost has been included in the Council's Medium Term Financial Plan. Increasing finance costs and significant inflationary pressures mean that some projects in the capital programme may be deferred due to their lack of commercial viability. However, a significant number of projects remain which will need to be delivered in the short to medium term to address the Council's statutory responsibilities and/or deliver against agreed strategic objectives. A particular challenge exists where grant funding is received prior to going out to tender and then is insufficient to cover the full cost of planned works. The regular project meetings chaired by the Chief Executive ensure there is an ongoing discussion of project financing and consideration given to other funding options and re-scoping of projects.</p> <p>A further specific challenge relates to future costs concerning the port infrastructure and backlog maintenance of the property portfolio and the outcome of the current accommodation review. Members are aware that whilst the associated costs are not yet factored into the capital programme and medium financial plan the impact is likely to be significant. The options for cost-avoidance and reduction will depend on significant strategic decisions to be taken as part of the budget-setting process.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
1	<p>Risk:- Legislative changes/ significant legal challenge.</p> <p>Effects:- Changes arising from Central Government.</p> <p>Risk of GDPR breach and ICO sanction/fine.</p> <p>Risk of administrative or other challenge in relation to the Council's overall governance/acts/ omissions.</p>	5	5	25	<ul style="list-style-type: none"> Monitoring Officer Horizon scanning by Legal/CMT/Mgt Team Service Manager responsibilities Financial & workforce planning Membership of professional/ Local Govt bodies aids horizon scanning Mgmt of change approach to mitigate significant impact to the organisation and its staff. Detailed project plans to change implementation. Respond to consultations on new legislation. Insurance 	2	5	10	Carol Pilson AB	<ul style="list-style-type: none"> Use intelligence to identify impending changes and their effects. Ensure staff trained and procedures changed. Use professional networking to identify best practice for responding to change. We respond to government consultations on changes to legislation or policy to influence its development. Operate in accordance with best practice. Seek specialist external legal advice where required. Effective working with other local authorities 	<p>Officers continue to horizon-scan for legislative changes and their effects.</p> <p>The Council has in house senior legal advice as well as through its links with external organisations such as EM Lawshare and PCC Legal. Specialist external advice will be sought in relation to complex/technically challenging matters as appropriate.</p> <p>The Council has a dedicated GDPR Officer, and each service is required to have a dedicated GDPR lead.</p> <p>The Elections Bill 2021 includes additional requirements relating to: Voter identification; Postal and Proxy voting measures; Clarification of undue influence; Accessibility of Polls; Overseas Electors; EU Voting and Candidacy Rights; The Electoral Commission; Notional Expenditure; Political Finance; Intimidation: New Electoral sanction; and Digital Imprints.</p> <p>New procurement legislation is expected in the coming months. unknown. Officers are keeping a watching brief and will update Management team and members when the impacts become known.</p> <p>The Environment Act included changes to waste collection and treatment for implementation from 2025-2027. This will involve changes in how we are funded and what is expected of us as a local authority collecting domestic and commercial waste and recycling. The remaining lack of clarity for Cambridgeshire is part of the risk at present.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
10	<p>Risk: - Major health and safety incident</p> <p>Effects: - Major Health & Safety incident at Council leads to costs for inquiry, disruption to service and possible prosecution</p>	4	4	16	<ul style="list-style-type: none"> • Health and Safety Policy / Codes of Practice • Quarterly meetings of Council Health & Safety (H&S) Panel • H&S Management System based on HSG65 (Plan, Do, Check, Act) • H&S audits in all services • Specialist H&S advisor • Corporate wide H&S training • Insurance • Aligned Port Health and Safety arrangements • Port Management Group and annual independent audit • Robust sickness management processes 	3	3	9	CMT DV	<ul style="list-style-type: none"> • Health and safety standing item on relevant team meetings. • All services represented on H&S Panel meetings • Ensure equipment inventory and inspections are up to date. • Collation of all Service Risk Assessment Registers • All high-risk areas have increased systems of management in place, e.g. the Port Safety Management Group • Statutory building/equipment inspection programmes in place. 	<p>A thorough Health and Safety regime at the Council ensures that the residual risk remains carefully managed</p> <p>Programme of targeted health and safety refresher training is in place as per service specification.</p> <p>Health and safety e-learning courses developed and rolled out on the Council e-learning platform.</p> <p>Health and Safety performance is monitored regularly, and accident statistics remain low.</p> <p>Flu jabs are being provided for employees.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
11	<p>Risk: - Fraud and error committed against the Council.</p> <p>Effects: - Potential for fraud, corruption, malpractice, or error, by internal or external threats. In addition to immediate financial loss, this could harm reputation and lead to additional inquiry costs and penalties.</p>	4	4	16	<ul style="list-style-type: none"> • Anti-fraud & corruption policy/ strategy • Financial Regulations / Standing Ord • Codes of conduct • Appropriately trained staff • Appropriate culture and risk awareness • Segregation of duties • Supported financial mgt system • Budget monitoring regime • Internal Audit review of sys /and controls • Bribery & corruption / fraud risk assessments • Indemnity insurance • Whistle-blowing procedure • Annual Governance Statement • ARP fraud resource • National Fraud Initiative 	3	3	9	<p>Peter Catchpole / Carol Pilson</p> <p>PC</p>	<ul style="list-style-type: none"> • Increase staff vigilance • Fraud awareness training for Managers • Raise profile internally and externally for successful prosecutions 	<p>The Council works with the NFI on assurance to achieve annual compliance.</p> <p>The Council has assisted with each annual National Fraud Initiative, cross-matching information with records held nationally.</p> <p>The Fraud team within the Anglia Revenues Partnership (ARP) continue to work on this area.</p> <p>The Council's Anti-Fraud and Corruption Strategy has been approved and adopted.</p> <p>A fraud awareness training programme for all staff is being finalised and is planned to be delivered virtually.</p> <p>Financial regulations are currently being updated to ensure they are available to new and current staff.</p> <p>Our anti-money laundering policy is currently being revised. Staff training will be provided once complete.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
13	<p>Risk:- Failure of Governance in major partners or in the Council as a result of partnership working</p> <p>Effects:- Partnership governance not adopted or followed, leading to unachieved priorities and poor performance by major partner agencies:- Cambs and Peterborough Combined Authority, Anglia Revenues Partnership, CNC Building Control, Shared Planning, CCTV</p>	4	5	20	<p>Cabinet and O&S, bi-annual stakeholder events ensure accountability.</p> <ul style="list-style-type: none"> • ARP Joint Committee and Operational Improvement Board, Cabinet, O&S, joint risk registers • CNC Joint Members Board, Cabinet plus O&S • Shared Planning Board, Cabinet plus Overview and Scrutiny, joint performance indicators • Project plans / perf monitoring shared risk registers. • PCCA Membership. 	3	3	9	<p>Carol Pilson / Peter Catchpole</p> <p>All Mgrs</p>	<ul style="list-style-type: none"> • Assurance that governance models correctly followed and in the Council's interests. • Support Members in governance of partnership bodies. • Ensure that the Council's interests are protected as Members of the Combined Authority and as Officers working on joint projects. • Ensure all Partners have robust Business Continuity Plans in place. • GDPR compliance • Robust ICT governance processes 	<p>The Annual Governance Statement being reported to Audit & Risk Management Committee shows the Council is in a strong governance position.</p> <p>Scrutiny of key partners and contract monitoring takes place on an annual basis and Cabinet members sit on Boards to ensure the effective delivery of partnership arrangements.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
14	<p>Risk:- Failure to achieve required savings targets.</p> <p>Effects:- Failure to achieve efficiency saving, maximise income, or performance targets, results in greater than budgeted costs and potential risk of Council not being able to set a balanced budget.</p>	4	5	20	<ul style="list-style-type: none"> • Heightened analysis of budgets and services by CMT • Implement Service Transformation • Implement Procurement Strategy • Corporate plan • Pursue action to increase income streams • Performance Management Framework • Budget and performance monitoring • Robust Workforce planning • Project Management processes • Our Council for the Future programme • Modernising Council Services transformation programme 	3	3	9	<p>CMT</p> <p>MS/SW</p>	<ul style="list-style-type: none"> • Robust control of corporate Transformation Plan. • Regular progress reports and assurance to Members. • Organisational and Service transformation programme • Commercialisation and Investment Strategy • Transformation and Recovery Plans 	<p>Delivery of Council Efficiency targets continue including delivering savings planned for in the Council's annual budget and medium-term financial strategy.</p> <p>A significant shortfall between the net budget requirement and resources available still exists over the medium-term. The extent of this gap was re-appraised in autumn 2023 as part of the budget-setting process and will be reported to Cabinet and council in February 2024.</p> <p>The Council has now delivered Phase 2 of the Transformation programme which is on target to deliver significant savings over the Council's current MTFP period. We have now started delivering the next phase of this transformation programme. Delivering savings from the Transformation Agenda 2 (TA2) programme will be critical in enabling the Council to set a balanced budget over the medium-term.</p> <p>As part of the Council's Transformation Programme, the Council has recognised that this is an opportune time to commence a full Accommodation Review, which could contribute significantly to future savings requirements. Hybrid working is now commonplace across the Council resulting in limited occupation of our main office accommodation which presents new possibilities for the Council. By way of background, the Council has undertaken a condition survey for Fenland Hall. This indicates a requirement for significant capital and revenue investment in Fenland Hall. Whilst some costs will be unavoidable and will need to be built into updated financial forecasts, the timeframe and degree of priority will vary according to which option is taken forward once the Accommodation Strategy Outline Business Case has been considered by members.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
19	<p>Risk:- Poor communications with stakeholders.</p> <p>Effects:- Poor communication with stakeholders and staff leads to poorly informed direction of resources and lack of support for change. Reputational damage Staff turnover Increased sickness absence</p>	4	5	20	<ul style="list-style-type: none"> • Internal and external regular publications • Staff and management meetings • Regular staff communication from the Chief Executive • Key stakeholder networks for consultation • Forums for perceived hard to reach groups. • Co-ordinated press releases • Comments, Compliments and Complaints monitoring and reporting procedure. • Customer Service Excellence accreditation • Consultation strategy • MTSP 	3	3	9	<p>Carol Pilson</p> <p>DW/SA</p>	<ul style="list-style-type: none"> • CSE Action Plan. • Staff survey and Wellbeing survey • Public consultations on key issues. • 3cs refresher training • Team meetings • “What’s Breaking” communication and Vlog updates from the Chief Executive to all staff. • Use of social media communication mediums • Fully updated website 	<p>The Council’s CSE performance is assessed each year by an external expert. The Council has a dedicated project team to ensure ongoing progress against CSE requirements/actions across all service areas to ensure consistent and effective communication to our customers.</p> <p>All change projects are supported by a robust project management approach, which includes a communication programme to ensure that stakeholders are fully informed.</p> <p>Regular Chief Executive’s vlog to provide staff with updates on Council projects, share information about the organisation and its day-to-day business, and to be used as an opportunity to answer questions.</p>

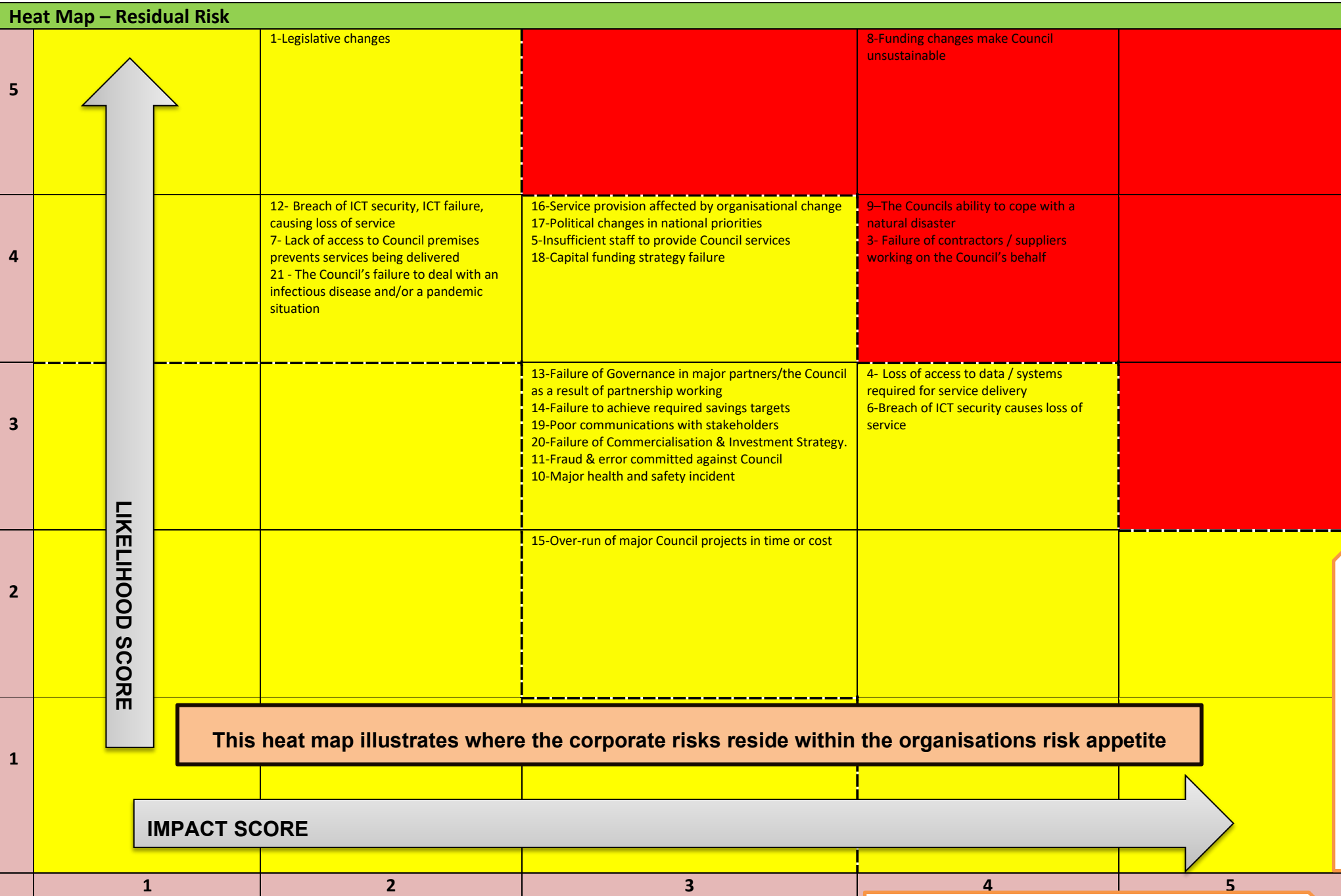
Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
20	<p>Risk:- Commercial uncertainties associated with decisions taken as part of the Council's Commercial and Investment Strategy.</p> <p>Effects:- Reputational damage Financial loss Impact on services, staff and community</p>	5	4	20	<ul style="list-style-type: none"> • Robust oversight and governance arrangements • Expert professional advice • Robust budget management • Thorough project management and business cases process 	3	3	9	CMT	<ul style="list-style-type: none"> • All governance requirements have been put in place and will be robustly reviewed going forward. • Fenland Future Ltd (FFL) has been constituted, with all appropriate governance requirements in place. • Dedicated external expert resources are identified and procured to support where required. • Annual audit on all governance arrangements. 	<p>This risk will be closely monitored to enable any new actions for mitigation to be identified and put in place.</p> <p>The Council's Commercial and Investment Strategy has a scoring matrix to inform all potential investment opportunities, which are considered fully by the Investment Board before they are ratified.</p> <p>Full business cases for all identified opportunities are taken to the Investment Board for consideration. This includes deciding on the delivery methodology. i.e. FDC or FFL and resource required to deliver each project.</p> <p>FFL's Business Plan was approved by the Council's Investment Board. Project plans setting out the preferred delivery routes for each of FFL's major projects have been prepared and the two sites now have outline planning permission. Work has progressed on the delivery models needed to develop them.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
7	<p>Risk:- Lack of access to Council premises prevents services being delivered</p> <p>Effects:- Disruption of service provision.</p> <p>The Council has undertaken a condition survey of Fenland Hall and significant repairs are needed.</p>	4	4	16	<ul style="list-style-type: none"> Alarm and security systems Fire drills Business continuity plans Emergency planning network ICT disaster recovery and offsite testing Relocation procedures - critical and support services Geographically distributed sites Remote working Statutory building inspection and checks Corporate Business Continuity Plans Carrying out necessary works to rectify urgent issues Monitoring the number of staff working from Fenland Hall to ensure the situation doesn't impact service delivery. 	2	4	8	<p>Peter Catchpole</p> <p>SB DV MG</p>	<ul style="list-style-type: none"> Regularly test Emergency Plan Test service Business Continuity Plans Ensure key emergency planning staff attend regular liaison meetings and training Provision of 'drop down' facilities for staff 	<p>Emergency plans – ongoing programme of review, testing and training of staff involved in a response</p> <p>Plans regularly checked and tested with emergency planning exercise conducted at intervals.</p> <p>Improved ICT systems provide better/increased opportunities for remote/agile working.</p> <p>Office-based staff have the necessary equipment to be able to work away from the office, with access to Council systems, which allows us to maintain the delivery of Council services.</p> <p>All key/priority services have individual Business Continuity measures in place to maintain service delivery.</p> <p>The Council has implemented Pay Point, which has enabled our resident to pay their bills (by cash or card) in a much greater number of more local rural locations across the district.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
12	<p>Risk:- Failure of external investment institutions</p> <p>Effects:- Failure of external investment institutions affecting availability of funds or return on investment reducing cash flow and resource availability</p>	5	4	20	<ul style="list-style-type: none"> • Policy for maximum investment/ borrowing levels limits liability. • Credit ratings. • Financial management. • Reserves. • Insurance. • Medium Term Financial Strategy. • Treasury Management Strategy. • Use of external advisors. 	2	4	8	<p>Peter Catchpole</p> <p>MS/SW</p>	<ul style="list-style-type: none"> • Effective Treasury Management strategy. • Robust auditing of processes and policies. 	<p>The Council's treasury management position is regularly reviewed. The Council complies with relevant sector best practice.</p> <p>The Treasury Management Strategy is subject to review by the Audit and Risk Management Committee prior to being considered and approved by Cabinet and Full Council in February each year. An annual report and a mid-year report are produced during the year for members' consideration in accordance with reporting requirements set out by CIPFA.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
21	<p>The Council's failure to deal with an infectious disease and/or a pandemic situation.</p> <p>Includes the adverse impact on all aspects of service delivery</p>	5	5	25	<ul style="list-style-type: none"> • Additional resources • Working with key partner agencies (Public Health, CPLRF, ARP etc.) • Supporting delivery of Business grants and self - solution payments • Agile working, the majority of staff are home-work enabled, and all services have split into 'bubbles' to maintain resilience and business continuity • ICT infrastructure • Ongoing communications to public and workforce 	2	4	8	CMT	<ul style="list-style-type: none"> • Regularly test Emergency Management Plan. • Test Service Business Continuity Plans • Ensure key emergency planning staff attend regular liaison meetings and training • Ongoing management response group and regular conference call and action planning • Support vaccination programmes • Enduring transmission programmes • Additional temporary resources have been identified to support key services. 	<p>The Council has implemented a rota for senior officers to be 'on call' at Gold (Strategic), Silver (Tactical) and Bronze (Operational) levels in the event of an emergency.</p> <p>The Council's response to any such situation will complement and support the coordinated CPLRF and Public Sector response to any such incident.</p>

Reference	Risk and effects	Risk if no action			Mitigation	Current risk			Risk Owner	Actions being taken to managing risk	Comments and progress of actions
		Impact	Likelihood	Score		Impact	Likelihood	Score			
15	<p>Risk:- Over-run of major Council projects in time or cost.</p> <p>Effects: - Failure to manage projects effectively leads to overruns on time or cost and failure to achieve project aims. Reputational damage.</p>	4	5	20	<ul style="list-style-type: none"> • Project Management methodology • Contract Standing Orders & Financial Regulations • Service plans • Budgetary control • Management, Cabinet and Portfolio Holder oversight • Forecasting • Horizon scanning • Amended ways of working; models have changed with remote working but remain effective. 	3	2	6	CMT	<ul style="list-style-type: none"> • Robust project management. • Effective risk registers for projects. • All projects have a CMT sponsor with experienced management membership • Project Management Board oversight • Legal due diligence around Grant Agreements 	<p>Effective project management remains a Council priority.</p> <p>Major projects are closely monitored by CMT and Cabinet members and progress is reported to Council via Portfolio Holder briefings.</p> <p>The Council has now delivered Phase 2 of the Transformation programme which is on target to deliver significant savings over the Council's current MTFP period. We have now started delivering the next phase of this transformation programme.</p> <p>Governance arrangements around project management have been reviewed and rolled out.</p>



AUDIT AND RISK MANAGEMENT COMMITTEE WORK PROGRAMME 2024

DATE OF MEETING	TITLE	TYPE OF REPORT	LEAD OFFICER	OBJECTIVES AND DESIRED OUTCOMES
12 February 2024				
	Treasury Management Strategy Statement, Capital Strategy, Minimum Revenue Provision Policy Statement and Annual Investment Strategy 2023/24	Annual	Mark Saunders	To endorse the strategy to be included in the final budget report
	Internal Audit Plan 2023/24 Progress report Q3	Quarterly	David Thacker	To consider and note the activity and performance of the Internal Audit function
	RIPA Policy	Annual	Amy Brown	To agree proposed changes/updates to the RIPA Policy
	Corporate Risk Register – update	Quarterly	Stephen Beacher	To review and approve the quarterly risk register.
	Audit and Risk Management Committee Work Programme	Quarterly	David Thacker	Information Purposes
25 March 2024				
	Draft Statement of Accounts 2022-23	Annual	Mark Saunders	Review and note the draft Statement of Accounts 2022-23
	Anti-Money Laundering Policy	4 Yearly	Peter Catchpole	To approve the Anti-Money Laundering Policy.
	Corporate Debt Policy	4 Yearly	Amy Brown / Peter Catchpole	To agree proposed changes/updates to the Corporate Debt Policy
	Risk Based Internal Audit Plan 2024/25	Quarterly	David Thacker	To approve the internal audit plan and resources for the forthcoming year
	Annual Governance Statement Update 2022/23	Annual	David Thacker	To review and note the progress on the Annual Governance Statement action plan arising from 2022/23.

Agenda Item 10

AUDIT AND RISK MANAGEMENT COMMITTEE WORK PROGRAMME 2024

	Risk Management Strategy and Corporate Risk Register	Annual	Stephen Beacher	To consider and note the annual review of risk management and corporate risk register.
	Audit and Risk Management Committee Work Programme	Quarterly	David Thacker	Information Purposes
XX July 2024				
	Treasury Management Annual Review 2023/24	Annual	Mark Saunders	To consider the overall financial and operational performance of the Council's treasury management activity for 2023/24
	Internal Audit Outturn and Quality Assurance Review	Annual	Internal Audit	To provide the Audit and Risk Management Committee with an overview of the work undertaken by Internal Audit during 2023/24. To provide the Audit Managers annual opinion on the system of internal control. To consider the effectiveness of Internal Audit.
	Audit and Risk Management Committee Annual Report 2023/24	Annual	Internal Audit	To report to Full Council the commitment and effectiveness of the Audit and Risk Management Committee's work from April 2023 to March 2024
	Audit and Risk Management Committee Work Programme	Quarterly	Internal Audit	Information Purposes

AUDIT AND RISK MANAGEMENT COMMITTEE WORK PROGRAMME 2024

Future items *(when to be brought to the committee in 2024 to be determined)*

- Corporate Debt Policy (4 Years) – March 2024

Cyclical Items *(not due this year unless policy or legislation changes require amendments prior to review date)*

- Whistleblowing Policy July 2024
- ARMC Terms of Reference December 2024
- External Auditor Appointment Process Dec – Feb 2027

Audit and Risk Management Committee Training sessions 2024

- Statement of Accounts – Mark Saunders 12th February 2024
- Risk Register – Stephen Beacher 25th March 2024

Audit and Risk Management Committee Action Plan

Title	Comments	Due by	RAG
Independent Member appointment	A report was presented to the committee in July 2022, with the committee agreeing in principle to progress with an independent member appointment to ARMC. Further report outlining skills analysis and job description to be brought back to ARMC for recommendation to Council.	March 2024	Not due yet
Committee Training	Committee Members to discuss training requirements and provide officers with suggested training topics for future meetings.	Ongoing	

AUDIT AND RISK MANAGEMENT COMMITTEE WORK PROGRAMME 2024

Abbreviations Used in Audit & Risk Management Committee

AGS	Annual Governance Statement
ARG	Additional Restrictions Grant
ARP	Anglia Revenue Partnerships
BCP	Business Continuity Planning
BEIS	The Department for Business, Energy and Industrial Strategy
CFR	Capital Financing Requirement
CIPFA	Chartered Institute of Public Finance and Accountancy
CIS	Commercial Investment Strategy
CMT	Corporate Management Team
CNC	CNC Building Control
CPCA	Cambridgeshire & Peterborough Combined Authority
CPE	Civil Parking Enforcement/
CPLRF	Cambridgeshire & Peterborough Local Resilience Forum
CTS	Council Tax Support
DFG	Disabled Facilities Grants
DPA	Data Protection Act
CSR	Comprehensive Spending Review
FFL	Fenland Future Ltd
GDPR	General Data Protection Regulations
IAS	International Accounting Standards
IFRS	International Financial Reporting Standard
LGA	Local Government Association
LGSS	Local Government Shared Services
LRSG	Local Restrictions Support Grants
MHCLG	Ministry of Housing Communities and Local Government
MoU	Memorandum of Understanding
MRP	Minimum Revenue Provision
MTFP	Medium Term Financial Plan
MTSP	Management, Trade Union & Staff Partnership
NFI	National Fraud Initiative
NNDR	National Non-Domestic Rates
OIB	Operational Improvement Board (ARP)
OLTL	Other Long-Term Liabilities
PPA	Post Payment Assurance
PSAA	Public Sector Auditor Appointments
PSIAS	Public Sector Internal Audit Standards
PWLB	Public Works Loan Board
RIPA	Regulation of Investigative Powers