

South Cambridgeshire Hall
Cambourne Business Park
Cambourne
Cambridge
CB23 6EA

t: 01954 713000

f: 01954 713149

www.scambs.gov.uk



21 March 2022

To: Chair – Councillor Tony Mason
Vice-Chair – Councillor Nick Sample
Members of the Audit and Corporate Governance Committee –
Councillors Jose Hales, Geoff Harvey, Mark Howell and Heather Williams

Quorum: 3

Substitutes: Councillors Nick Wright, Bunty Waters, Tom Bygott,
Grenville Chamberlain, Graham Cone, Steve Hunt and Henry Batchelor

Dear Councillor

You are invited to attend the next meeting of **Audit and Corporate Governance Committee**, which will be held in **Council Chamber - South Cambs Hall** at South Cambridgeshire Hall on **Tuesday, 29 March 2022 at 10.00 a.m.**

Members are respectfully reminded that when substituting on committees, subcommittees, and outside or joint bodies, Democratic Services must be advised of the substitution ***in advance of*** the meeting. It is not possible to accept a substitute once the meeting has started. Council Standing Order 4.3 refers.

Yours faithfully
Liz Watts
Chief Executive

The Council is committed to improving, for all members of the community, access to its agendas and minutes. We try to take all circumstances into account but, if you have any specific needs, please let us know, and we will do what we can to help you.

Agenda

- | | Pages |
|---|-------|
| 1. Apologies for Absence
To receive Apologies for Absence from Committee members. | |
| 2. Declarations of Interest | |
| 3. Minutes of Previous Meeting
To confirm the minutes of the meeting held on 4 February 2022 as a correct record. | 1 - 4 |

Audit Reports

4. **Completion of the 2018/19 Audit of the Accounts - Report to Follow**
2018/19 Final Accounts update from officers.
5. **2018-19 Audit Results Report from External Audit - Report to Follow**
6. **Internal Audit Update** **5 - 16**
Decision Items
7. **Regulation of Investigatory Powers Act 2000 (RIPA) Policy and Update on Use of RIPA** **17 - 48**
8. **Anti-Theft, Fraud, Bribery and Corruption Policy** **49 - 78**
Information Items
9. **Matters of Topical Interest**
10. **Date of Next Meeting**
Thursday 28 July at 10 am.

Guidance Notes for Visitors to South Cambridgeshire Hall (See end of agenda)

This page is left blank intentionally.

Agenda Item 3

South Cambridgeshire District Council

Minutes of a meeting of the Audit and Corporate Governance Committee held on
Friday, 4 February 2022 at 10.00 a.m.

PRESENT: Councillor Tony Mason – Chair

Councillors: Henry Batchelor
Geoff Harvey
Heather Williams

Jose Hales
Mark Howell

Officers: Patrick Adams
James Carter
Peter Maddock
Rory McKenna
Liz Watts

Senior Democratic Services Officer
Interim Project Accountant
Head of Finance
Monitoring Officer
Chief Executive

Auditors: Janet Dawson
Mark Russell
Jonathan Tully

Ernst & Young
Ernst & Young
Head of Shared Internal Audit

Councillor Nigel Cathcart was in attendance, by invitation.

Councillor John Williams was in attendance remotely.

1. **Apologies for Absence**

Apologies for Absence were received from Councillor Nick Sample. Councillor Henry Batchelor attended as his substitute.

2. **Declarations of Interest**

None.

3. **Minutes of Previous Meeting**

The minutes of the meeting held on 1 December 2021 were agreed as a correct record.

4. **Completion of the 2018/19 Audit of the Accounts**

The Head of Finance presented this report on the completion of the 2018/19 audit of accounts. He explained that the recommendation in the report needed to be amended to read:

“It is recommended that the attached 2018/19 Statement of Accounts is approved, and that any final updates are delegated to the Head of Finance in consultation with the Chair of this committee, in liaison with EY, in the expectation that an unqualified audit opinion will be issued by the external auditors following the committee meeting on 4 February.”

It was noted that the final responsibility for the signing of the accounts lay with the

Head of Finance and this was the reason for the amendment.

The Head of Finance highlighted amendments to the Statement of Accounts in the agenda, which were circulated at the meeting and had been published on the website as a supplement.

The Chair explained that the accounts in the agenda replaced the most recent accounts provided to the Committee and so should now be accepted as the latest version of the accounts. He further explained that if there was a material variance in the 2018/19 accounts they would be taken back to the Committee before being agreed. Councillor Heather Williams suggested that if any changes were made to the accounts the Committee members should be informed.

It was noted that it was expected that the 2018/19 accounts would be signed off by the end of February. Councillor Heather Williams suggested that if the accounts were not signed off by the end of February a meeting of the Committee should be held in early March.

It was agreed that a new timeline regarding the signing off of the 2019/20, 2020/21 and 2021/22 accounts would have to be drawn up.

By affirmation the Committee

Agreed that the 2018/19 Statement of Accounts, attached to the report, be approved and that any final updates are delegated to the Head of Finance in consultation with the Chair of this committee, in liaison with EY, in the expectation that an unqualified audit opinion will be issued by the external auditors following the committee meeting on 4 February.

5. Draft 2018-19 Audit Results Report from External Audit

Janet Dawson presented External Audit's draft results report for the 2018/19 accounts. She explained that resolving the outstanding issues should be straightforward and she was confident the work would be completed by the end of the month. However, the work could only be signed off by her and Mark Russell and so in the unlikely event of one of them being unable to carry out this work, there would be a further delay. It was noted that it was planned that work on the 2019/20 accounts was scheduled to begin on 1 March.

Timescales

In response to concerns that there could be further delays, the Head of Finance expressed his confidence that the accounts would be signed off by the end of the month, as there were only two questions that needed to be resolved and these issues did not have a cash impact on the Statement of Accounts. He further explained that the draft accounts for 2019/20 should be ready by 18 March. The Interim Project Accountant stated that on the current evidence the draft 2019/20 accounts should be presented to the Committee at its next meeting on 29 March.

The Head of Finance assured the Committee that once all the outstanding

accounts had been signed off the Council would have a team in place to ensure that future accounts would be prepared in a timely manner.

Work of the interim accountants

The Head of Finance explained that the Council had two accountants solely dedicated to the accounts and preparatory work had been done in anticipation of the External Auditors starting work on the 2019/20 audit. The Head of Finance agreed to check the notice period for the interim accountants carrying out this work. The Interim Project Accountant assured the Committee that both he and his colleagues were committed to completing the project regarding the outstanding accounts and training the rest of the team on how to deliver the accounts in the future.

External Auditors' fees

Councillor Heather Williams expressed concern that the External Auditors were attempting to charge over £120,000 more than originally estimated, and that EY had been partly responsible for some of the delay. The Head of Finance replied that he planned to discuss the fees with the External Auditors, but getting the accounts signed off was the priority. Janet Dawson explained that EY were not charging for any delays but only for the work completed.

The Committee **Noted** the report.

6. Regulation of Investigatory Powers Act 2000 (RIPA) - Update on use of RIPA

The Monitoring Officer informed the Committee that the Council had not used its RIPA powers between the period March to January 2022.

The Committee **Noted** the report.

7. Matters of Topical Interest

The Chair explained that he was meeting with the External Auditors to discuss training for audit committee members, which would be arranged soon after the elections in May.

8. Date of Next Meeting

It was noted that the next scheduled meeting would take place on Tuesday 29 March at 10 am. The Chair announced that if the 2018/19 accounts were not signed off in February an extra meeting would be held in early March.

The Meeting ended at 11.00 a.m.

This page is left blank intentionally.



Committee update March 2022

Introduction

Contents

Introduction	1
Overview	1
Accountancy and Finance.....	2
Governance, Risk and Control.....	3
Counter Fraud update.....	5
Useful Links	10
Training and development	10
Note	10

Overview

The purpose of this document is to provide an update to the Committee on key audit and governance themes.

The Chair suggested, at the July 2021 meeting, that a slot at the beginning of future meetings was allocated to check in on key areas of governance and provide any updates. If there are no updates in a particular area to report, that can be noted and taken as assurance.

This document provides summary updates for the Committee. Statistics are included to help provide an overview of work in progress and these are taken from the last financial quarter.

Your team

Head of Finance and Section 151 officer
Head of Shared Internal Audit
Corporate Fraud Manager
Monitoring Officer
Senior Democratic Services officer

Committee information

[Calendar of meetings](#)

[Committee Membership and Functions](#)

Accountancy and Finance

Local Audit Procurement

The Audit and Corporate Governance Committee discussed the next appointment period of the External Auditor at the [December meeting](#).

Public Sector Audit Appointments (PSAA) has set the length of the compulsory appointing period as the five consecutive financial years starting 1 April 2023. It will cover the audits of the accounts from 2023/24 to 2027/28.

Public Sector Audit Appointments has now [announced](#) that 470 of the 475 qualifying bodies signed up to their national auditor procurement scheme for the five-year accounting period from 2023-24 to 2027-28.

This outcome is an even higher proportion than the 98% acceptance level for the current scheme which covers the audits for financial years 2018/19 to 2022/23.

Director of Local Audit Appointment

The Financial Reporting Council (FRC) has [announced](#) the appointment of the FRC's first Director of Local Audit.

The Director of Local Audit will play an integral role in establishing a new local audit unit, ahead of the FRC assuming the "Systems Leader" role for local authority financial reporting and audit, as part of its transition to the Audit, Reporting and Governance Authority (ARGA).


In May 2021, the Government proposed ARGA take on this role in responding to Sir Tony Redmond's independent review.

Last year, the government rejected the review's main recommendation of having a standalone system leader for local audit, with Whitehall preferring a separate department within the reformed regulator.

ARGA will provide annual reports on the state of local audit and take over responsibility for the updated Code of Local Audit Practice - the guidelines councils are required to follow.

Governance, Risk and Control

Internal Audit updates

Review	Summary of report and actions
 <p>Grant assurance – Wet Led Pub scheme</p> <p>Current: Full assurance</p> <p>Previous: New review</p>	<p>We completed the Christmas Support Payment for Wet Led Pubs Post Payment Assurance Verification process (PPAS).</p> <p>The BEIS assurance and individual scheme guidance sets out that Local Authorities have a responsibility to provide assurance to both themselves and the Department that they have followed the eligibility guidance, and so minimised the risk of errors/fraud and over/irregular payments.</p> <p>In response to BEIS sampling methodology, we provided evidence of pre and post assurance checks.</p> <p>This provided assurance that the business:</p> <ul style="list-style-type: none"> • Meets the criteria of the grant scheme; • Was not in administration, insolvent or struck off the Companies House register on the date the grant was awarded; and • The business was trading at the eligibility date <p>Further testing is planned for the other grant schemes.</p>

National Fraud Initiative

The Council completed the extract of [Council Tax and Electoral Register](#) data in December. We reviewed and quality assured the data prior to uploading it to the secure Cabinet Office system. The data was very good quality which provides information governance assurance. The matches will be processed throughout 2022.

Business Grant Assurance

The Department for Business, Energy and Industrial Strategy (BEIS) announced two new funding schemes to support those

businesses affected by the pandemic. Details were published on our [grants and funding web-page](#).

We process the applications the Cabinet Office National Fraud Initiative and Spotlight system as pre-assurance checks to help mitigate the risk of fraud and error. This was unplanned activity, and we have focussed on this work to ensure payments can be allocated as promptly as possible.

We have now processed 6298 grants to date through the National Fraud Initiative bank verification system, which provides assurance that grant applications were made from legitimate businesses

Energy Rebate Scheme

The Department for Levelling Up, Housing and Communities announced that households which are in Council Tax bands A to D will receive a £150 rebate to help with the rising cost of energy. Councils will be making this payment on behalf of the Government.

We are committed to ensuring that rebates are only paid to those that are genuinely entitled. Whilst we understand that most people are honest there are, unfortunately, some people or groups that will deliberately attempt to commit fraud to misdirect funds for their own personal gain or to fund more serious crime.

Reducing fraud is important to us as it affects the services and assistance that we can provide to families and our broader communities when they need it the most.

To provide assurance that rebates are only made to those who are truly eligible we will be completing pre-assurance checks. In some cases this may mean that there is a slight delay in payment, however we believe this is necessary to pay any assistance to where it is genuinely needed.

If you suspect fraud, please report it to fraud@scams.gov.uk

More information about the rebate scheme has been [published on our website](#).

Reviews in Progress and forward planning

Our current planned assurance and follow-up reviews include:

- VAT (Value Added Tax)
- Capital – Asset Register
- Payroll

External assurance

The Driver and Vehicle Licensing Agency (DVLA) completed their first audit of the Council data processing. They confirmed that we make in the region of 150 enquiries per year through the National Anti-Fraud Network, typically for enquiries on Abandoned Vehicles.

The review concluded a “Green” rating from their RAG system, “*No issues were observed; or any non-conformance is minor*”, and this provided assurance on validity of requests and subsequent data handling.

Overall assurance

The internal audit work and assurance mapping enables us to form an opinion on the internal control environment, governance and risk management arrangements.

There is currently a Reasonable level of assurance overall, which is similar level to the previous year.

Counter Fraud update

Successful prosecution for council tax support fraud

A woman from Oakington was convicted and fined £80.00 and costs of £960.00 after pleading guilty to one count of council tax support fraud. The claimant had failed to declare capital savings and bank accounts to the Council falsely claiming £4292.91 in council tax support between the period of 12 June 2014 and 16th April 2020.

Promoting cases of fraud detection helps to prevent further fraud, and the Council issued a [press release](#) on our website.

Council finance bosses say the case is a reminder to the individuals to read the eligibility criteria carefully and to be truthful when making claims for assistance.

The claimant appeared in Huntingdon Magistrates' Court on 2 March 2020 and pled guilty to the offence laid by the district

council. She was ordered to pay a victim surcharge in addition to already paying back the full amount owed to the Council.

Cllr John Williams, South Cambridgeshire District Council's Lead Cabinet Member for Finance, said: "The case highlights why it is so important that any persons claiming assistance grants or support must tell the truth. Our teams are always happy to speak to residents about the benefits system or grant schemes and answer any queries. We want to help people claim what they're entitled to, but won't tolerate anyone claiming financial assistance that they should not be getting. If you're claiming benefits and you think your circumstances have changed, talk to us. If you don't you could end-up in court."

Fraud Team Statistics – our quarterly position

We have included some fraud statistics below from the recent quarter. The purpose of these is to provide the Committee with an overview of the work in progress, and specific individual details are not disclosed due to sensitivity and risk of compromising any investigations in progress.

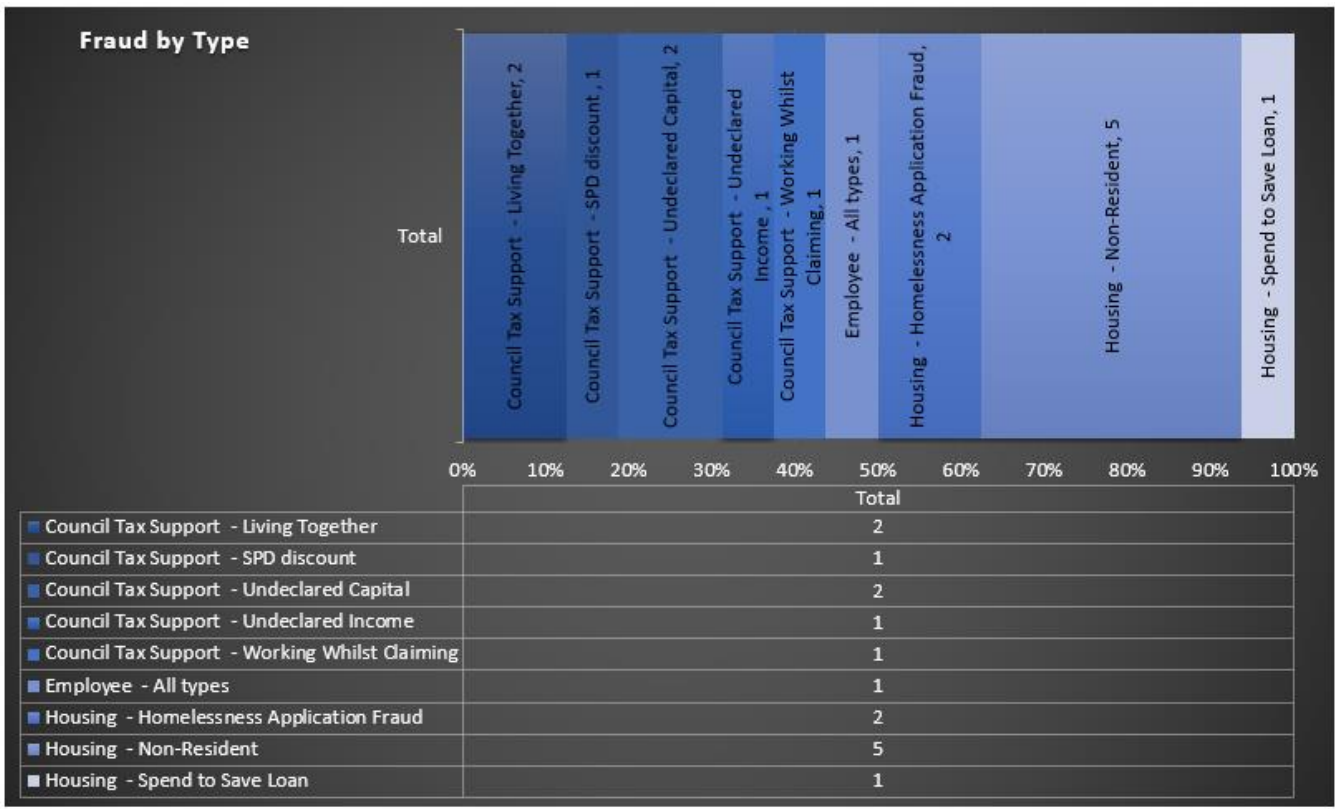
Reports of suspected fraud received

Analysis by the source of intelligence:



Fraud by type

Analysis by fraud type:



Investigations in progress (as of 30 September 2021)

Case Status	Number of Cases	Key
Live Investigation	52	Open investigations
Interview Under Caution (IUC)	NA due to FTA and Covid Closure	Number of IUC's from live investigations
Sanction decision	1	Cases submitted to sanctions panel.
Criminal Prosecution Administrative Penalty Caution Prosecution and Civil action Civil Warning Letter No Further Action Notice to quit (Secure or flexible tenancy) Notice of proceedings for possession (intro tenancy) / Notice to Seek possession (secure and flexible)	1	

Investigations Closed

Closure Reason	Number
A10 Fraud proven but no further action	1 NATIS referral
A11 Not investigated, passed for visit	
A13 Not investigated - not on benefit	
A4 Closed - claimant error only	
A5 Closed - no fraud established	1
A7 Not investigated - passed to DWP (Department for Work and Pensions)	4

Proactive work – Prevention

Prevention is an important aspect of our Counter Fraud arrangements.

Education		
Workshop Attendees	Nil	
Campaign work	Ongoing to develop “can fraud be your friend campaign”.	
Other	Omicron- Advice to Business – Prevent	Advice – Licensing Taxi Lockers
Verification checks		
Right to buy verification enquiries reported	5	7 completed
Outstanding RTB Docs/Visit	Zero	
Homelessness verification enquiries reported	2	
General housing verification enquiries	Zero	
Ermine Street	Zero	
Locta	Zero	
DWP SPOC (Single Point of Contact) enquiries		
LAIEF’s	3	
General		
Data Protection Act requests - External	Zero	
National Fraud Initiative Matching		
Biennial exercise		
Closed	472	
Annual exercise CT (Council Tax) / SPD (Single Person Discount)		
Closed – No issue	37	

RIPA (Regulation of Investigatory Powers Act) update

Cases of RIPA used in period:	0
-------------------------------	---

Useful Links

Link	Details
Public Sector Audit Appointments	PSAA is responsible for appointing an auditor and setting scales of fees for relevant principal authorities that have chosen to opt into its national scheme.
EY.com	EY (Ernst & Young) is our current externally appointed auditor
Cabinet Office NFI (National Fraud Initiative)	The National Fraud Initiative is a data matching exercise which helps public sector organisations to prevent and detect cases of fraud and error.

Training and development

The new UK Information Commissioner begins their five-year term. Further information is available on their [website](#).

Note

This document will have links to external websites where it provides more information. We are not responsible for the content of external websites.

This page is left blank intentionally.

Agenda Item 7



South
Cambridgeshire
District Council

REPORT TO: Audit & Corporate Governance
Committee

29th March 2022

LEAD OFFICER: Monitoring Officer

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) POLICY AND UPDATE ON USE OF RIPA

Executive Summary

1. The purpose of this report is to seek the approval of Members of the Audit and Corporate Governance Committee on the current policy noting that there are no updates from when it was approved last year and to provide an update on the use of RIPA powers since the committee last met.

Key Decision

2. No

Recommendations

3. It is recommended that Audit & Corporate Governance Committee:
 - (a) **APPROVE** the Council's RIPA policy at Appendix A;
 - (b) **NOTE** the Council has not used surveillance powers between January 2022 – February 2022.

Reasons for Recommendations

4. The committee are to receive quarterly updates on the Council's use of RIPA powers and to review the RIPA policy on an annual basis.

Details

5. RIPA regulates covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that law enforcement and security agencies have the powers they need to do their job effectively.
6. Following a Home Office Review into counter-terrorism and security powers the Protection of Freedoms Act 2012 was passed in May 2012 requiring all local authority surveillance authorised under RIPA to be approved by a Magistrate from November 2012. The council's policy and procedures were amended at that time to reflect these changes.
7. The Council comprehensively reviewed and updated its policy in September 2012 and last reviewed the policy in March 2021.
8. The Investigatory Powers Commissioner's Office is responsible for the inspection of public authorities with regard to compliance with RIPA. The Council was the subject of a remote inspection on the 24th February 2021 and the report concluded that the information provided demonstrated a level of compliance that removes, for the present, the requirement for a physical inspection. The Inspector also commented that the policy was a well written document and easy to read.
9. There have been no changes to the legislation since the last revision of the policy in March 2021.

The council's use of RIPA since June 2020

10. The information in the table below summarises the authorisations granted from January 2022 – February 2022.

	Directed surveillance	CHIS	Total
January 2022 – February 2022	0	0	0

Options

11. Members are required to review the policy on an annual basis and approve the policy with or without amendments.

Implications

12. In the writing of this report, taking into account financial, legal, staffing, risk, equality and diversity, climate change, and any other key issues, the following implications have been considered:-

Financial

13. None

Legal

14. Authorisation of surveillance activity gives that surveillance “lawful authority” for the purposes of the European Convention on Human Rights.

Staffing

15. None

Risks/Opportunities

16. See legal.

Equality and Diversity

17. See legal.

Climate Change

18. None

Background Papers

None

Appendices

Appendix A: RIPA Policy

Report Author:

Rory McKenna – Monitoring Officer
Telephone: 07872 116523

APPENDIX A

South Cambridgeshire District Council

Regulation of Investigatory Powers Act 2000 Corporate Policy & Procedures

Statement of Intent: South Cambridgeshire District Council attaches a high value to the privacy of citizens. It will adhere to the letter and to the spirit of the Act and will comply with this policy.

Contents

1	Introduction	3
2	Background.....	4
3	When RIPA applies	5
4	Surveillance Definitions	5
4.1	Surveillance	5
4.2	Covert Surveillance.....	6
4.3	Directed Surveillance	6
4.4	Private information.....	7
5	Risks of not having correct RIPA Authorisation	8
6	Surveillance Outside of RIPA	8
7	Immediate Response to Events.....	8
8	Recording of Telephone Conversations	8
9	Intrusive surveillance.....	9
10	Covert Human Intelligence Source (CHIS)	9
10.1	Definition	9
10.2	Conduct and Use of a Source	10
10.3	Management of Sources	11
10.4	Tasking	11
10.5	Security and Welfare	12
10.6	Records	12
11	RIPA Application and Authorisation Process	13
11.1	Application, Review, Renewal and Cancellation Forms	13
11.2	Applications.....	13
11.3	Duration of Applications	14
11.4	Reviews	14
11.5	Renewal.....	14
11.6	Cancellation	15
11.7	Authorising Officers.....	15
11.8	Urgent Oral Authorisations	16
11.9	Local Sensitivities.....	16
11.10	Authorising Officers Responsibility	16
11.11	Necessity and Proportionality	17
11.12	Collateral Intrusion	18
11.13	Unexpected Interference with Third Parties.....	18
11.14	Confidential Information	19
11.15	Documentation and Central Record	20
12	Use of CCTV.....	21
13	Joint Agency Surveillance	22
14	Activities Which May Constitute Surveillance or Require Authorisation Outside of RIPA	22
14.1	Definition.....	22
14.2	Social Networks and the Internet.....	23
14.3	Visits and Observing Properties and Vehicles	25
14.4	Aerial Cover Surveillance	26
15	Annual Report to Investigatory Powers Commissioner's Office	26
16	Storage and Retention of Material.....	26
17	Training.....	26
18	Oversight	26
18.1	Responsibilities	26

18.2	Reporting to Members.....	27
18.3	Scrutiny and Tribunal	27
Appendix 1: LIST OF AUTHORISING OFFICERS AND AUTHORISING LEVELS.....		28

1 Introduction

1.1 The Regulation of Investigatory Powers Act 2000 (“RIPA”) is designed to ensure that public bodies respect the privacy of members of the public when carrying out investigations, and that privacy is only interfered with where the law permits and where there is a clear public interest justification.

1.2 The purpose of this policy is to explain the scope of RIPA and the circumstances where it applies to the Council. It provides guidance on the authorisation procedures to be followed in the event that surveillance is needed. This policy sets out the correct management of the process by the Council.

1.3 This policy also ensures that activities that should be subject to RIPA authorisation are recognised as such and that appropriate authorisation is sought. It also seeks to ensure that any activity which should be carefully monitored, but which is not subject to RIPA authorisation, is still given correct authority and scrutiny.

1.4 The Protection of Freedoms Act 2012 imposes restrictions on the circumstances in which the Council is permitted to use Directed Surveillance and this policy has been updated to take into account these new restrictions. Separate guidance has been issued by the Home Office which specifies the procedure for the consideration and approval of applications by Magistrates and this policy must be read in conjunction with that procedure and documents issued by the Office of the Surveillance Commissioner.

1.5 The Chief Executive is the Senior Responsible Officer for the RIPA process for the Council. The SRO is also responsible for:

- the integrity of the process in place within the public authority to authorise Directed Surveillance;
- compliance with Part II of the 2000 Act, and with this code;
- engagement with the Commissioners and inspectors when they conduct their inspections, and
- where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner.

1.6 All staff involved in the process must take their responsibilities seriously in order to assist with the integrity of the Council’s processes and procedures.

1.7 In preparing this policy the Council has followed the current RIPA Codes of Practice produced by the Home Office and the Office of Surveillance Commissioners (OSC) Procedures and Guidance 2016. The OSC is now the Investigatory Powers Commissioner's Office (IPCO). However, the document is still current.

1.8 In the case of any uncertainty, advice should be sought from an Authorising Officer, the Head of Legal Practice or the Monitoring Officer, who is the Council’s RIPA Monitoring Officer.

1.9 Copies of the Codes of Practice can be found on the Council’s RIPA Intranet page and at the following links:

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

1.10 Further guidance can also be obtained from the Investigatory Powers Commissioner's Office website:

<https://www.ipco.org.uk/>

2 Background

2.1 The Human Rights Act 1998 brought into UK law many of the provisions of the 1950 European Convention on Human Rights and Fundamental Freedoms. Article 8 requires the Council to have respect for people's private and family lives, their homes, and their correspondence. These subjects can be referred to as "Article 8 rights".

2.2 The Human Rights Act makes it unlawful for any local authority to act in a way which is incompatible with the European Convention on Human Rights. However these are not absolute rights and are qualified by the ability of the Council to interfere with a person's Article 8 rights if :-

- such interference is in accordance with the law
- is **necessary**; and
- is **proportionate**

2.3 "*In accordance with the law*" means that any such interference is undertaken in accordance with the mechanism set down by RIPA and the Home Office Covert Surveillance Codes of Practice. The Codes of Practice deal with the use of Covert Surveillance and the use of persons such as informants and undercover officers who gather information in a covert capacity, known as a **Covert Human Intelligence Source or "CHIS"**. Any covert activity must also meet the test of necessity and proportionality and these are dealt with later in this policy.

2.4 A considerable amount of observations are carried out in an overt capacity by Council employees carrying out their normal functions. These activities are general and routine and do not involve the systematic surveillance of an individual. RIPA is not designed to prevent these activities or regulate them.

2.5 RIPA also applies to the **Accessing of Communications Data** under Part 1, Chapter 2 of the legislation. The Council has produced separate guidance dealing with the accessing of communications data under the Single Point of Contact ("SPOC") provisions.

2.6 The Council has numerous statutory duties and powers to investigate the activities of private individuals and organisations within its jurisdiction for the benefit and protection of the greater public. Some of these investigations may require surveillance or the use of a CHIS. These may include:

- environmental health
- housing
- planning
- audit
- fraud

2.7 RIPA provides a framework to control and supervise covert activities such as surveillance and the use of a CHIS in these criminal investigations. It aims to balance the need to protect the privacy of individuals against the need to protect others by the Council in compliance with its enforcement functions. Covert Surveillance and CHIS are covered by separate Codes of Practice which can be found on the Council's Intranet RIPA page.

3 When RIPA applies

- 3.1 For Directed Surveillance, amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (“the 2010 Order”) mean that a local authority can only grant an authorisation under RIPA where the local authority is investigating criminal offences which attract a custodial sentence of a maximum term of at least 6 months’ imprisonment, or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.
- 3.2 It should be noted that the provision relating to the prevention of disorder is no longer included for Directed Surveillance and there is no provision for a Local Authority to authorise an urgent oral authorisation as all applications and renewals must be approved by a Magistrate.
- 3.3 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.
- 3.4 The RIPA authorisation process can only be used for in connection with the Council’s core functions.
- 3.5 Using the RIPA application process helps protect the Council from legal challenges and provides the lawful authority for Officers to conduct Directed Surveillance and use CHIS South Cambridgeshire District Council and its staff have a responsibility to adhere to the legislation and the Human Rights Act. Any contract staff employed by South Cambridgeshire District Council to undertake such activity are also covered by the codes and this policy.
- 3.6 The RIPA Codes of Practice state where there is an interference by a public authority with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under the 2000 Act may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.
- 3.7 Public authorities are therefore strongly recommended to seek an authorisation under RIPA where the surveillance is likely to interfere with a person’s Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.
- 3.8 In some instances, it is not possible to obtain RIPA authorisation for surveillance activities due to the limited grounds set in the legislation where authorisation can be granted. It may be, however, that covert surveillance is still necessary and proportionate. This is dealt with later in this Policy in section 6.

4 Surveillance Definitions

4.1 Surveillance

- 4.1.1 Surveillance is defined in paragraph 2.2 of the Codes of Practice as:

“Surveillance, for the purpose of the 2000 Act, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be

conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.”

4.2 Covert Surveillance

4.2.1 Covert Surveillance is defined in paragraph 2.3 of the Codes of Practice as:

“Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place.”

4.2.2 If activities are open and not hidden from the persons subject to surveillance such as Officers conducting Council business openly, e.g. a market inspector walking through markets, the RIPA framework does not apply because that is overt surveillance. Equally, if the subject is told that surveillance will be taking place, the surveillance is overt. This would happen, for example, where a noise maker is informed that noise will be recorded if it continues. RIPA does not regulate overt surveillance.

4.2.3 RIPA regulates only two types of Covert Surveillance which are:

- Directed Surveillance
- Intrusive Surveillance

4.3 Directed Surveillance

4.3.1 Surveillance is Directed Surveillance (paragraph 3.1 of the Codes of Practice) 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 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 under Part II of the 2000 Act to be sought.

4.3.2 The planned covert surveillance of a specific person, where not intrusive, would constitute Directed Surveillance if such surveillance is likely to result in the obtaining of private information about that, or any other person.

4.3.3 Remember that the offence must be capable of having a 6 month maximum custodial sentence or relate to the sale of alcohol and tobacco to children.

4.3.4 It is important that all activity that may constitute surveillance is recognised as such and correctly authorised, either as Directed Surveillance or, in some instances, as surveillance outside of RIPA (see section 6) as governed by this policy. Anything involving the use of concealed cameras or anything involving keeping covert observation on premises or

people should be considered as potentially amounting to Directed Surveillance. In the case of uncertainty advice should be sought from the Head of Legal Practice or the Monitoring Officer.

4.4 Private information

4.5 Private information includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

4.6 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, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.

Example: Two people holding a conversation on the street or in a bus may have a reasonable expectation of privacy over the contents of that conversation, even though they are associating in public. The contents of such a conversation should therefore still be considered as private information. A directed surveillance authorisation would therefore be appropriate for a public authority to record or listen to the conversation as part of a specific investigation or operation

4.7 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 surveillance, a Directed Surveillance authorisation may be considered appropriate.

Example: South Cambs Officers wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a directed surveillance authorisation as no private information about any person is likely to be obtained or recorded. However, if the authority wished to conduct a similar exercise, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person and a directed surveillance authorisation should be considered.

4.8 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.

Example: A surveillance officer intends to record a specific person providing their name and telephone number to a shop assistant, in order to confirm their identity, as part of a criminal investigation. Although the person has disclosed these details in a public place, there is nevertheless a reasonable expectation that the details are not being recorded separately for another purpose. A directed surveillance authorisation should therefore be sought.

5 Risks of not having a RIPA Authorisation

- 5.1 If Investigators undertake covert activity to which this legislation applies without the relevant authority being obtained and the case progressed to criminal proceedings the defence may challenge the validity of the way in which the evidence was obtained under Section 78 of the Police and Criminal Evidence Act 1984. Should the evidence then be disallowed by a court, the prosecution case may be lost with a financial cost to the Council.
- 5.2 The person who was the subject of surveillance may complain to an independent tribunal who may order the Council to pay compensation. The activity may also be challenged through the civil courts under the Human Rights Act 1998 for breach of privacy.
- 5.3 A properly obtained and implemented authorisation under RIPA will provide the Council with lawful authority to interfere with the rights of the individual. It is not simply enough that an authorisation for surveillance is obtained. It must be properly obtained, implemented, managed, reviewed and cancelled.

6 Surveillance Outside of RIPA

- 6.1 There may be a necessity for the Council to undertake surveillance which does not meet the criteria to use the RIPA legislation such as, in cases of serious disciplinary investigations. The Council must still meet its obligations under the Human Rights Act and therefore any surveillance outside of RIPA must still be necessary and proportionate, having taken account of the intrusion issues. The decision making process and the management of such surveillance will mirror that of RIPA-authorized surveillance, except that the activity will not require approval from a Magistrate.
- 6.2 An application will be made using the non RIPA application forms.
- 6.3 The Authorising Officer will be required to give the application the same degree of consideration and copies of all forms will be passed to the RIPA Monitoring Officer, who will keep a record of all activity separately from the records of RIPA-authorized surveillance

7 Immediate Response to Events

- 7.1 There may be occasions when officers come across events unfolding which were not pre-planned which then require them to carry out some form of observation. This will not amount to Directed Surveillance under RIPA. However, as the Council is no longer able to grant urgent oral authority to conduct surveillance, if it is carried out the officer must be prepared to explain their decisions in court should it be necessary. Therefore, they should document their decisions, why it was necessary, what took place and what evidence or information was obtained and why it was proportionate to the incident or offence under investigation.

8 Recording of Telephone Conversations

- 8.1 The recording of telephone conversations connected to criminal investigations outside of the Councils monitoring at work policy for its own equipment, falls under RIPA. Where one party to the communication consents to the interception, it may be authorised a Directed Surveillance.

- 8.2 There may be occasions where this is required such as a witness who has text or voicemail evidence on their mobile telephone and SCDC require to examine the phone.

9 Intrusive surveillance

- 9.1 South Cambridgeshire District Council has no authority in law to carry out Intrusive Surveillance or activity under the Police Act 1997.
- 9.2 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.
- 9.3 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.
- 9.4 A risk assessment of the capability of equipment being used for surveillance on residential premises and private vehicles should be carried out to ensure that it does not fall into Intrusive Surveillance.
- 9.5 Commercial premises and vehicles are excluded from the definition of intrusive surveillance. However, they are dealt with under the heading of Property Interference contained within the Police Act 1997. SCDC has no lawful authority to carry out any activity under this Act.

10 Covert Human Intelligence Source (CHIS)

10.1 Definition

10.1.1 A CHIS could be an informant or an undercover officer carrying out covert enquiries on behalf of the council. However, the provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information such as the Fraud Hotline. Members of the public acting in this way would not generally be regarded as sources.

10.1.2 Under section 26(8) of the 2000 Act a person is a source if:

- (a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);
- (b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or

- (c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.
- 10.1.3 By virtue of section 26(9)(b) of the 2000 Act a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.
- 10.1.4 By virtue of section 26(9)(c) of the 2000 Act a relationship is used covertly, and information obtained as above is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.
- 10.1.5 Special provisions exist for the conduct in use of sources (Under 18).
- 10.1.6 A source under 16 cannot be engaged to use a relationship with any person having parental responsibility for them. A source under 16 must have an appropriate adult present during any meetings and a risk assessment must also take place before granting or renewing an authorisation for the conduct and use of a source under 16. This will take account of physical and psychological risks. See the Regulation of Investigatory Powers (Juveniles) Order 2000 for detailed guidance.
- 10.1.7 Only the Chief Executive can authorise the use of a juvenile CHIS (under 18 year of age).
- 10.1.8 Special consideration should also be given to the use of vulnerable individuals as a source. This will require the highest level of Authorising Officer, the Chief Executive (see the code of practice for further guidance).
- 10.1.9 The use by South Cambridgeshire District Council of a CHIS is expected to be extremely rare and if contemplated advice should be sought from the Head of Legal Practice or the Monitoring Officer.

10.2 Conduct and Use of a Source

- 10.2.1 South Cambridgeshire District Council will ensure that arrangements are in place for the proper oversight and management of sources including appointing a Handler and Controller for each source prior to a CHIS authorisation. The Handler and Controller of the source will usually be of a rank or position below that of the Authorising Officer.
- 10.2.2 The **use of a source** involves inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.
- 10.2.3 The **conduct** of a source is any conduct falling within section 29(4) of the 2000 Act, or which is incidental to anything falling within section 29(4) of the 2000 Act.
- 10.2.4 The **use of a source** is what the Authority does in connection with the source and the **conduct** is what a source does to fulfil whatever tasks are given to them or which is incidental to it. Both the use and conduct require separate consideration before authorisation. However, both are normally authorised on the same application.
- 10.2.5 When completing applications for the use of a CHIS this will include who the CHIS is, what they can do and for which purpose

10.2.6 When determining whether a CHIS authorisation is required consideration should be given to the covert relationship between the parties and the purposes mentioned in a, b, and c above.

10.2.7 Unlike Directed Surveillance, which relates specifically to private information, authorisations for the use or conduct of a CHIS do not relate specifically to private information, but to the covert manipulation of a relationship to gain any information. Accordingly, any manipulation of a relationship by a public authority (e.g. one party having a covert purpose on behalf of a public authority) is likely to engage Article 8, regardless of whether or not the public authority intends to acquire private information

10.3 Management of Sources

10.3.1 Within the provisions there has to be;

- (a) a person who has the day to day responsibility for dealing with the source and for the source's security and welfare (**Handler**)
- (b) at all times there will be another person who will have general oversight of the use made of the source (**Controller**)
- (c) at all times there will be a person who will have responsibility for maintaining a record of the use made of the source

10.3.2 The **Handler** will have day to day responsibility for:

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

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

10.4 Tasking

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

10.4.2 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 source may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a Council Officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the Council to determine where, and in what circumstances, such activity may require authorisation.

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

10.5 Security and Welfare

10.5.1 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. Before authorising the use or conduct of a source, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.

10.6 Records

10.6.1 Proper records must be kept of the authorisation and use of a source as required by the Regulation 3 of the Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI no 2725) namely:

- 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 (e) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
- g) the date when, and the circumstances in which, the source was recruited;
- h) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);
- i) the periods during which those persons have discharged those responsibilities;
- j) the tasks given to the source and the demands made of him in relation to his activities as a source;
- k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
- l) the information obtained by each relevant investigating authority by the conduct or use of the source;
- m) any dissemination by that authority of information obtained in that way; and
- n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on

behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

- 10.6.2 The records kept by public authorities 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.

11 RIPA Application and Authorisation Process

11.1 *Application, Review, Renewal and Cancellation Forms*

- 11.1.1 No covert activity covered by RIPA should be undertaken at any time unless it has been authorised by an Authorised Officer and approved by a Magistrate.
- 11.1.2 All the relevant forms for authorisation through to cancellation must be in writing using the standard forms which are available on the Council's Intranet site, but officers must ensure that the circumstances of each case are accurately recorded on the application form (see Application Process).
- 11.1.3 If it is intended to undertake both Directed Surveillance and the use of a CHIS on the same surveillance subject the respective applications form and procedures should be followed and both activities should be considered separately on their own merits.
- 11.1.4 An application for an authorisation must include an assessment of the risk of any Collateral Intrusion or interference. The Authorising Officer will take this into account, particularly when considering the proportionality of the Directed Surveillance or the use of a CHIS.

11.2 *Applications*

- 11.2.1 All the relevant sections on an application form must be completed with sufficient information for the Authorising Officer and then the Magistrate to consider Necessity, Proportionality and the Collateral Intrusion issues. Risk assessments should take place prior to the completion of the application form. Each application should be completed on its own merits of the case. Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.
- 11.2.2 All applications will be submitted to the Authorising Officer via the Line Manager of the appropriate enforcement team in order that they are aware of the activities being undertaken by the staff. The Line Manager will perform an initial quality check of the application. However, they should not be involved in the sanctioning of the authorisation. Completed application forms are to be initialled by Line Managers to show that the quality check has been completed.
- 11.2.3 Applications whether authorised or refused will be issued with a unique number by the Authorising Officer, taken from the next available number in the Central Record of Authorisations. To obtain this number contact the Legal Services.
- 11.2.4 The procedure for submitting applications to Magistrates for consideration is set out in the procedure issued by the Home Office for this purpose.

11.3 Duration of Applications

Directed Surveillance	3 Months
Renewal	3 Months
Covert Human Intelligence Source	12 Months
Renewal	12 Months
Juvenile Sources (Grant/Renewal)	4 Months

11.3.1 The three-month commencement date is the date approved by a Magistrate.

11.3.2 All Authorisations must be cancelled by completing a cancellation form. They must not be left to simply expire.

11.4 Reviews

11.4.1 Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves Collateral Intrusion.

11.4.2 In each case, the Authorising Officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable and they will record when they are to take place on the application form. This decision will be based on the circumstances of each application. However, reviews will be conducted on a monthly or less basis to ensure that the activity is managed. It will be important for the Authorising Officer to be aware of when reviews are required following an authorisation to ensure that the applicants submit the review form on time.

11.4.3 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 so that the need to continue the activity can be reassessed. However, if the circumstances or the objectives have changed considerably, a new application form may be more appropriate which will need authorising and approval by a Magistrate. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

11.4.4 Managers or Team Leaders of applicants should also make themselves aware of when the reviews are required to ensure that the relevant forms are completed on time.

11.5 Renewal

11.5.1 If at any time before an authorisation would cease to have effect, the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given, they may renew it in writing for a further period of three months. Like applications, all renewals must also be approved by a Magistrate.

11.5.2 An application for renewal should not be made until shortly before the authorisation period is drawing to an end but the applicant must consider the need to allow sufficient time for consideration by the Authorising Officer and any potential delay in getting the matter

before a Magistrate for consideration. A renewal for three months takes effect on which the authorisation would have ceased.

- 11.5.3 Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity.
- 11.5.4 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.
- 11.5.5 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.

11.6 Cancellation

- 11.6.1 The cancellation form is to be submitted by the applicant or another investigator in their absence as soon as it is no longer necessary or proportionate to continue with the covert activity. 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
- 11.6.2 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.
- 11.6.3 It will also be necessary to detail the amount of time spent on the surveillance as this is required to be retained by Central Register.
- 11.6.4 The officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and detail any images etc. that were obtained. The Authorising Officer should then take this into account and issue instructions regarding the management and disposal of the images etc.
- 11.6.5 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight.

11.7 Authorising Officers

- 11.7.1 Officers who are designated "Authorising Officers" may authorise written applications for the use of Directed Surveillance or the use of a CHIS.

- 11.7.2 Please refer to Appendix 1 for the list of Authorising Officers, to show name, departmental details, contact number and levels of Authority.
- 11.7.3 The Chief Executive Officer or in their absence the Chief Operating Officer will authorise cases where confidential information is likely to be gathered or in the case of a juvenile or vulnerable CHIS.
- 11.7.4 The Head of Legal Practice or the Monitoring Officer should be informed of any changes to the list of Authorising Officers and will amend the policy accordingly. The intranet will also be updated appropriately.

11.8 Urgent Oral Authorisations

- 11.8.1 The provision for urgent oral authorisations is no longer available to local authorities, All applications now have to be put before a Magistrate for consideration.

11.9 Local Sensitivities

- 11.9.1 Authorising Officers and Applicants should be aware of particular sensitivities in the local community where the Directed Surveillance is taking place, or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. This should form part of the risk assessment.
- 11.9.2 It should be noted that although this is a requirement there is no provision made within the application form for this information. Therefore, applicants should cover this where they feel it is most appropriate such as, when detailing the investigation or proportionality, or within the separate risk assessment form. However, it must be brought to the attention of the Authorising Officer when deciding whether to authorise the activity.

11.10 Authorising Officers Responsibility

- 11.10.1 Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable. 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.
- 11.10.2 Authorising Officers must treat each case individually on its merits and satisfy themselves that the authorisation is **necessary**, the surveillance is **proportionate** to what it seeks to achieve, taking into account the **Collateral Intrusion** issues, and that the level of the surveillance is appropriate to achieve the objectives. If any equipment, such as covert cameras, video 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.

- 11.10.3 Authorising Officers are responsible for determining when reviews of the activity are to take place.
- 11.10.4 Before authorising surveillance, the Authorising Officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (Collateral Intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.
- 11.10.5 In the absence of the Head of Department, the application should be submitted to another Authorising Officer for authorisation.

11.11 Necessity and Proportionality

- 11.11.1 Obtaining a RIPA authorisation 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. It must be necessary for the prevention and detection of crime with a 6 months sentence or relate to the sale of alcohol and tobacco to children. It must also be shown the reasons why the requested activity is necessary in the circumstances of that particular case. Can the same end result be achieved without the surveillance?
- 11.11.2 If the objectives could be achieved by methods other than covert surveillance, then those methods should be used unless it can be justified why they cannot be used.
- 11.11.3 Then, if the activities are **necessary**, the person granting the authorisation must believe that they are **proportionate** to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the subject and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair. The interference with the person's right should be no greater than that which is required to meet the aim and objectives.
- 11.11.4 The onus is on the Authorising Officer to ensure that the surveillance meets the tests of **necessity and proportionality**.
- 11.11.5 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.

- 11.11.6 It is important that the staff involved in the surveillance and the Line Manager manage the enquiry and operation and evaluate the need for the activity to continue.

11.12 Collateral Intrusion

- 11.12.1 Collateral Intrusion is an integral part of the decision making process and should be assessed and considered very carefully by both applicants and Authorising Officers.
- 11.12.2 The Codes state that Collateral Intrusion is intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation such as neighbours or other members of the subject's family. 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 or property of such individuals should not be considered as Collateral Intrusion but rather as intended intrusion. Any such surveillance activity should be carefully considered against the necessity and proportionality criteria.
- 11.12.3 Intended intrusion could occur if it was necessary to follow a person not committing any offences but by following this person it would lead to the person who is committing the offences.
- 11.12.4 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 the likelihood of Collateral Intrusion as to intrusion into the privacy of the intended subject of the surveillance.
- 11.12.5 Prior to and during any authorised RIPA activity, a risk assessment should take place to identify the likely intrusion into the subject and any Collateral Intrusion. Officers should take continuing precautions to minimise the intrusion where possible. The Collateral Intrusion, the reason why it is unavoidable, and the precautions taken to minimise it will have to be detailed on any relevant application forms. This will be considered by the Authorising Officer.
- 11.12.6 Before authorising surveillance, the Authorising Officer should take into account the risk of Collateral Intrusion detailed on the relevant application forms as it has a direct bearing on the decision regarding proportionality.
- 11.12.7 The possibility of Collateral Intrusion does not mean that the authorisation should not be granted, but the Authorising Officer must balance this with the importance of the activity to be carried out in operational terms.

11.13 Unexpected Interference with Third Parties

- 11.13.1 When carrying out covert Directed Surveillance or using a CHIS, the Authorising Officer should be informed if the investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. It will be appropriate in some circumstances to submit a review form and in other cases the original authorisation may not be sufficient, and consideration should be given to whether a separate authorisation is required.

11.14 Confidential Information

- 11.14.1 Confidential information consists of matters subject to Legal Privilege, confidential personal information or confidential journalistic material. Where there is a likelihood of acquiring such information, it must be authorised by the Chief Executive, or in their absence by their deputy.
- 11.14.2 No authorisation should be given if there is any likelihood of obtaining legally privileged material without consulting the Head of Legal Practice or the Monitoring Officer.
- 11.14.3 Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records. Journalistic material is also mentioned in the codes, however, it is highly unlikely that this will be obtained. The definition should it be required can be obtained from the Codes of Practice at Chapter 4.
- 11.14.4 The following general principles apply to confidential material acquired under authorisations:
- Those handling material from such operations should be alert to anything which may fall within the definition of confidential material. Where there is doubt as to whether the material is confidential, advice should be sought from the Head of Legal Practice or the Monitoring Officer 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 an appropriate officer (having sought advice from the Head of Legal Practice or the Monitoring Officer) is satisfied that it is necessary for a specific purpose;
 - The retention or 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;
 - Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

11.15 Documentation and Central Record

- 11.15.1 Authorising Officers or Managers of relevant enforcement departments may keep whatever records they see fit to administer and manage the RIPA application process.

However, this will not replace the requirements under the Codes of Practice for the Council to hold a centrally held and retrievable record. The original application and relevant approval by the Magistrate will be forwarded to the Head of Legal Practice or the Monitoring Officer for filing and to complete the central register (see below).

11.15.2 A centrally retrievable record of all authorisations will be held by the Head of Legal Practice or the Monitoring Officer who requires the original application and Magistrates approval etc to be submitted to complete the central register. This will regularly be updated whenever an authorisation is refused, granted, renewed or cancelled. The record will be made available to the relevant Commissioner or an Inspector from the Investigatory Powers Commissioner's Office, upon request. These records should be retained for at least three years from the ending of the authorisation or for the period stipulated by the Council's document retention policy, whichever is greater, and should contain the following information:

- if refused, that the application was not authorised and 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;
- date approved by a magistrate;
- 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;
- 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;
- the date and time when any instruction was given by the Authorising Officer.

11.15.3 As well as the Central Record the Head of Legal Practice or the Monitoring Officer will also retain:

- the original of each application, review, renewal and cancellation together with any supplementary documentation of the approval given by the Authorising Officer;
- a record of the period over which the surveillance has taken place.

11.15.4 **For CHIS applications the Codes state;**

In addition, records or copies of the following, as appropriate, should be kept by the relevant authority:

- the original authorisation form together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- the original 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 source;
- the circumstances in which tasks were given to the source;
- the value of the source 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;
- the date and time when any instruction was given by the Authorising Officer to cease using a source.

11.15.5 The Head of Legal Practice or the Monitoring Officer will be responsible for maintaining the Central Record of Authorisations and will ensure that all records are held securely with no unauthorised access.

11.15.6 The only persons who will have access to these documents will be the Head of Legal Practice, the Monitoring Officer, the Senior Responsible Officer and Authorising Officers.

11.15.7 The records kept by public authorities should be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source. There should, at all times, be a designated person within the relevant public authority who will have responsibility for maintaining a record of the use made of the source.

12 Use of CCTV

12.1.1 The use of the CCTV systems operated by the Council do not normally fall under the RIPA regulations. However, it does fall under the General Data Protection Regulations (GDPR) and the Councils CCTV policy. However, should there be a requirement for the CCTV cameras to be used for a specific purpose to conduct surveillance it is likely that the activity will fall under Directed Surveillance and therefore require an authorisation.

12.1.2 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, either the CCTV staff are to have a copy of the application form in a redacted format, or a copy of the authorisation page. If it is an urgent oral authority 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 Information Management Team for filing. This will assist the Council to evaluate the authorisations and assist with oversight.

- 12.1.3 Operators of the Council's 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.

13 Joint Agency Surveillance

- 13.1.1 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.
- 13.1.2 Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the authorisation page of the application 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 inform the Head of Legal Practice or the Monitoring Officer of the unique reference number, the agencies involved and the name of the officer in charge of the surveillance. This will assist with oversight of the use of Council staff carrying out these types of operations.

14 Activities Which May Constitute Surveillance or Require Authorisation Outside of RIPA

14.1 Definition

- 14.1.1 Some investigative activities may not be easily recognised as constituting surveillance which requires authorisation. Any action that is likely to reveal private information¹ may constitute surveillance if it includes:
- monitoring, observing, listening to persons, their movements, conversations, other activities or communications;
 - recording anything monitored, observed or listened to in the course of surveillance;
 - surveillance, by or with, assistance of a surveillance device

¹ Private information is defined in the RIPA Codes of Practice for Covert Surveillance as: "3.3 The 2000 Act states that private information includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships."

- 14.1.2 This policy requires RIPA authorisation to be sought in cases where an authorisation can be sought (as per Part 3 of the Policy). Where RIPA authorisation cannot be sought, for instance where an investigation is not into a criminal offence or the offence threshold in Part 3 is not met, the activity should still be authorised as per Part 6 of this policy.

14.2 Social Networks and the Internet

- 14.2.1 Online open source research is widely regarded as the collection, evaluation and analysis of material from online sources available to the public, whether by payment or otherwise to use as intelligence and evidence.
- 14.2.2 The use of online open source internet and social media research techniques has become a productive method of obtaining information to assist the council with its regulatory and enforcement functions. It can also assist with service delivery issues and debt recovery. However, the use of the internet and social media is constantly evolving and with it the risks associated with these types of enquiries, particularly regarding breaches of privacy under Article 8 Human Rights Act (HRA) and other operational risks. The activity may also require a RIPA authorisation for Directed Surveillance or CHIS. Where this is the case, the application process and the contents of this policy is to be followed.
- 14.2.3 Where the activity falls within the criteria of surveillance or CHIS outside of RIPA, again this will require authorising on a non RIPA form which will be authorised internally.
- 14.2.4 The Home Office Revised Code of Practice on Covert Surveillance and Property Interference, published in August 2018, provides the following guidance in relation to online covert activity and examples below that relevant to South Cambridgeshire District Council are given:

The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence

Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

As set out below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.

Example: A South Cambs Officer undertakes a simple internet search on a name, address or telephone number to find out whether a person has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.

Example: A South Cambs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need

an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit.

Example: South Cambridgeshire District Council undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown persons of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.

14.3 Visits and Observing Properties and Vehicles

- 14.3.1 Surveillance which is overt does not require authorisation. A visit to a property by an SCDC officer will not normally constitute surveillance if the intention is to speak to the occupier.
- 14.3.2 In some cases, repeated visits may be made to a property in connection with an investigation without the intention of speaking to the occupier, for example driving past the property to obtain details of vehicles or to look for signs of occupation. Such activity could become surveillance, as per 13.1 above and RIPA or non-RIPA authorisation should be sought if this is the case. This will be the case where the activity is intended to identify a pattern of behaviour, such as the movements of a vehicle at a particular location. A visit to obtain details of a vehicle is unlikely to constitute surveillance. Each case must be treated on its own merits.
- 14.3.3 If an officer plans to conduct a visit such as drive by visits (other than a routine visit to the occupier as per 13.3.1 above) detailed notes must be made explaining the purpose of the visit, why it is necessary and proportionate and why RIPA or non-RIPA authorisation has not been sought.

14.4 Aerial covert surveillance

- 14.4.1 Where surveillance using airborne crafts or devices, for example helicopters or unmanned aircraft (colloquially known as 'drones'), is planned, the same considerations outlined in this policy should be made to determine whether a surveillance authorisation is appropriate. In considering whether the surveillance should be regarded as covert, account should be taken of the reduced visibility of a craft or device at altitude. If these devices are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance authorisation should be considered. Such covert surveillance is likely to result in the obtaining of private information about a person (namely, a record of their movements and activities) and therefore falls properly within the definition of directed surveillance.

15 Annual Report to Investigatory Powers Commissioner's Office

- 15.1 The Council is required to provide statistics to the Investigatory Powers Commissioner's Office (IPCO) every year in March for the purposes of Annual Report. The Head of Legal Practice or the Monitoring Officer shall be responsible for completing the return and providing the statistics.

16 Storage and Retention of Material

- 16.1 All material obtained and associated with an application will be subject to the provisions of the Criminal Procedures Investigations Act 1996 (CPIA) Codes of Practice which state that relevant material in an investigation has to be recorded and retained and later disclosed to the prosecuting solicitor in certain circumstances. It is also likely that the material obtained as a result of a RIPA application will be classed as personal data for the purposes of the GDPR. 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.
- 16.2 Material is 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.
- 16.3 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.
- 16.4 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.

17 Training

- 17.1 There will be an ongoing training programme for Council Officers who will need to be aware of the impact and operating procedures with regards to this legislation. The Head of Legal Practice or the Monitoring Officer will be required to retain a list of all those officers who have received training and when the training was delivered, and it is for Departments to consider what their training needs are in this area.
- 17.2 Authorising Officers must have received formal RIPA training before being allowed to consider applications for Directed Surveillance and CHIS.

18 Oversight

18.1 Responsibilities

- 18.1.1 It is important that all staff involved in the RIPA application process take seriously their responsibilities. Overall oversight within the Council will fall within the responsibilities of the Senior Responsible Officer (SRO) for the Council. However careful management and adherence to this policy and procedures will assist with maintaining oversight and reduce unnecessary errors.

18.2 Reporting to Members

- 18.2.1 Quarterly returns of all surveillance activity undertaken by Council staff will be made to the Council's Audit and Corporate Governance Committee by the Senior Responsible Officer in line with the Constitution. The Audit and Corporate Governance Committee will review the policy annually and amend the policy where necessary.

18.3 Scrutiny and Tribunal

- 18.3.1 From 1 Sept 2017 oversight is provided by the Investigatory Powers Commissioner's Office (IPCO) which has been set up as an independent inspection regime to monitor Investigatory Powers which relate to covert activity currently under RIPA. They will periodically inspect the records and procedures of the Authority to ensure the appropriate authorisations have been given, reviewed, cancelled, and recorded properly.
- 18.3.2 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 he requires for the purpose of enabling him to carry out his functions.
- 18.3.3 A tribunal has been established to consider and determine complaints made under RIPA if it is the appropriate forum. Persons aggrieved by conduct, e.g. Directed Surveillance, can make complaints. The forum hears application on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that period.

Complaints can be addressed to the following address:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H9ZQ

Tel 0207 035 3711

Appendix 1: LIST OF AUTHORISING OFFICERS AND AUTHORISING LEVELS

Geoff Clark
Rob Lewis

Service Manager - Tenancy and Estates
Principal Commercial Officer, Waste and Environment

Senior Responsible Officer:

Anne Ainsworth, Chief Operating Officer

RIPA Monitoring Officer:

Rory McKenna, Monitoring Officer

Agenda Item 8



**South
Cambridgeshire
District Council**

Report to:	Audit and Governance Committee
Lead Cabinet Member:	John Williams
Lead Officer:	Peter Maddock
Date:	29 March 2022

Anti-Theft, Fraud, Bribery and Corruption Policy

Executive Summary

1. The Council has reviewed its Anti-Theft, Fraud, Bribery and Corruption Policy; intended to set out its approach to:
 - Protect Council assets from exposure to the risk of theft, fraud, bribery and Corruption and provide assurance that reports will be taken seriously and investigated thoroughly.
 - Provide Corporate Guidance on how to raise concerns and signpost colleagues to reporting platforms.
 - Identify responsibilities and reporting chains.
 - Warn of the potential consequences for perpetrators and highlight those policies and processes within the business which may interact with this report.

Recommendations

2. It is recommended that the Audit and Governance Committee adopt the Corporate Fraud Policy; acknowledging the governing body's responsibility for ensuring that risks associated with fraud, theft, bribery and corruption are managed effectively across all parts of the organisation.

Reasons for Recommendation

3. The Corporate Fraud Team was set up in 2020 to align internal investigatory services and to identify, disrupt, prevent and detect fraud across the business. The policy sets the framework within which the Council will operate to ensure that reports of insider fraud are reported to the appropriate person and investigated.

Details

4. This is a revised document and the Audit and Corporate Governance Committee in its terms of reference has a duty to monitor progress against the policy.
5. The Policy itself is attached at Appendix A.

Options

6. To adopt the Policy acknowledging the Council's commitment to protect assets from abuse both insider and external.
7. To adopt the Policy acknowledging the Council's commitment to protect assets from abuse both insider and external with agreed amendments.
8. To reject the Policy.

Alignment with Council Priorities

Growing Local Business and economies

9. Fraud and error limits resources available to support growth and the local economy. Where funds or resources are diverted away from those that need them the most it causes loss and disadvantage to those in genuine need.

Financial

10. Fraud and error can have a significant financial impact upon resources and misdirect resources from those in genuine need. It is recognised that maintaining resilience to fraud and corruption is a priority within the business plan to protect limited resources.

Risks/Opportunities

11. Failure to agree a fraud Policy will undermine:
 - Leadership Team's commitment to acknowledge the threat of fraud and corruption and the harm they can cause to an organisation, its aims and objectives and to its service users.
 - The Council's vision to create a culture that is resilient to the threats of fraud and corruption and align to the principals of good governance.
 - The Council's commitment to provide value for money, exploring opportunities for financial savings from enhanced fraud detection and prevention.

Equality and Diversity

12. Commitment to equity to ensure insider reports are dealt with as robustly as external reports.

Alignment with Council Priority Areas

Housing that is truly affordable for everyone to live in

13. Tenancy Fraud is categorised as a major risk facing all Local Authorities. By protecting assets from abuse those properties that are misdirected can be recovered and put back into the council stock.

Background Papers

Fighting Fraud and Corruption Locally Strategy 2020
[Fighting Fraud Corruption Locally Strategy 2020 | Cifas](#)

Insider Threat
[Fraudscape 2021 - Cifas](#)

Appendices

Appendix A: Anti-Theft, Fraud, Bribery and Corruption Policy

Report Author:

Tara Nutbeam-King - Corporate Fraud Manager tara.nutbeam-king@scams.gov.uk

This page is left blank intentionally.



Appendix A

South Cambridgeshire District Council

Anti-Theft, Fraud, Bribery and Corruption Policy

Version	2.0
Ownership	Peter Maddock
Approved by	Audit and Governance Committee
Policy Contact	Tara Nutbeam-King
Approval date	29 March 2022
Publication date	
Date of next review	Every two years



Contents

1. Introduction	4
2. Priority.....	5
3. Definitions	5
Fraud by false representation	6
Fraud by failing to disclose information	6
Fraud by abuse of position	6
Corruption.....	7
Theft	7
Bribery.....	7
Irregularity.....	8
4. Policy Statement	8
5. Responsibilities	9
6. Culture	10
7. Raising Concerns.....	11
8. Colleagues.....	12
9. Members.....	13
10. Systems	14
11. Fraud Risk Assessment	15
12. Prevention, detection and investigation	15
13. Awareness and Training	16
14. Redress and sanction	17
15. Monitoring	17
16. Annex.....	18



Annex A – Fighting Fraud Locally.....	18
Annex B – Nolan Committee	19
Annex C – Related policies	20
Annex D – Housing Benefit and Local Council Tax Support.....	21
Annex E – Bribery Risk	23



Introduction

- 1.1 The purpose of the Policy is to provide guidance on how to raise concerns about bribery, fraud, or corruption within South Cambridgeshire District Council (the Council).
- 1.2 In carrying out its functions and responsibilities, the Council wishes to provide assurance to all stakeholders that acts of theft, fraud, bribery, and corruption will not be tolerated by (the Council).
- 1.3 The Councils approved [Counter Fraud and Error Strategy Statement](#) should be read in conjunction with this policy. This document formalises the Council's approach to acts of theft, fraud, bribery and corruption, in accordance with the relevant provisions within the Local Government Act 2000; recognising the good practice guidelines in **the Fighting Fraud and Corruption Locally Plan 2020 and the Nolan Committee's 'Seven Principles of Public Life' (Annex B)**.
- 1.4 This document is intended to be considered alongside other council policies and should be read in conjunction with any relevant policies relating to theft, fraud, bribery, and corruption. **(Listed at Annex C)**. The document sets out the Council's anti-theft, fraud, bribery and corruption policy as it relates to:
 - The culture of the Council
 - Colleagues
 - Members
 - Officers
 - Audit and Governance
 - Systems; prevention, detection, and investigation
 - Redress and sanction



- Monitoring

The document will be issued as part of all induction processes for colleagues and also when new members join the Council.

Priority

2. It is recognised that maintaining resilience to fraud and corruption is a priority to:
 - ensure proper use of public funds and assets
 - protect limited resources
 - be an efficient and effective Council
 - to promote the highest standards of conduct, performance and integrity from its employees and Elected Members

Definitions

3. The definitions of fraud within the Fraud Act 2006, and an explanation of their meaning, will assist in providing an improved understanding of what constitutes Fraud, Theft, Bribery, and Corruption. The Fraud Act 2006 introduces provision for a general offence of fraud which is separated into three sections:
 - Fraud by false representation
 - Fraud by failing to disclose information
 - Fraud by abuse of position.



Fraud by false representation

- 3.1 Representation must be made dishonestly and is made with the intention of making a gain for themselves or another or causing a loss or to expose another to a risk of loss.

A representation is defined as false if it is untrue or misleading and the person making it knows that it is, or might be, untrue or misleading.

The Fraud Act doesn't expressly give it a technical meaning but examples of a representation can be by words or communicated by conduct, i.e., written, spoken or by electronic means.

Fraud by failing to disclose information

- 3.2 Fraud by failing to disclose information details that a fraud will have been committed if a person fails to declare information which he/she has a legal duty to disclose. There is a requirement that the person acts dishonestly and intends to make a gain for themselves, cause a loss to another or expose another to a risk of loss.

Fraud by abuse of position

- 3.3 Fraud by abuse of position requires a person to act dishonestly by abusing the position held; and by doing so, fails to disclose to another person, information which they are legally required to disclose. The dishonest act must be with the intention of making a gain for themselves or another. Alternatively, it may be with the intention of causing a loss or risk of loss to another. The offence may be committed by omitting to make a declaration as well as by an act.

The introduction of the Fraud Act 2006 does not prevent the prosecution of offences using the remaining Theft Act legislation and Forgery and



Counterfeiting legislation, e.g., theft, counterfeiting and falsification of documents.

Corruption

3.4 Corruption is the abuse of entrusted power or position for private gain and an example is as follows;

Receiving a bribe: A supplier gives your nephew a job but makes it clear that in return they expect you to use your influence at the Council to ensure we continue to do business with them.

It is an offence for a supplier to make such an offer. It would be an offence for you to accept the offer as you would be doing so to gain a personal advantage.

Theft

3.5 Theft is defined under [Theft Act 1968 S.1](#). A person is guilty of theft if they dishonestly appropriates property belonging to another, with the intention of permanently depriving the other of that property. It does not matter whether the appropriation is made with a view to gain or for that person's own benefit.-

Bribery

3.6 'Bribery' is defined as: an inducement or reward offered, promised or provided to gain personal, commercial, regulatory or contractual advantage.

Further information is included on Annex E.



Irregularity

3.7 Irregularities are instances of non-compliance with laws and regulations. It may be any significant matter or issue, other than fraud or corruption, which may warrant consideration or investigation.

An example may be where a member or colleague makes a genuine error or mistake during their duties/responsibilities, which is not disclosed, to the on-going detriment of the Council.

It may also involve inappropriate use of Council funds or assets, which may or may not constitute fraud, theft or corruption.

Policy Statement

4.1 The Council is committed to dealing with theft, fraud, bribery and corruption both inside and outside the Council (the latter as far as it relates to the business of the Council).

4.2 The Council acknowledges in approving this policy:

- It sets a standard to make it clear that bribery, fraud, or corruption will not be tolerated.
- that the Council is committed to preventing and detecting bribery, fraud, or corruption.
- that those perpetrating bribery, fraud, or corruption may be prosecuted.

4.3 In order to implement this policy, the Council will:

- Provide a clear framework, guidelines and procedures for the identification and investigation of bribery, fraud, and corruption



- Investigate cases of bribery, internal fraud and corruption and take appropriate action
- Ensure employees and members have the appropriate level of information and training to implement this policy
- Ensure information is provided to enable the public to report suspected cases of bribery, fraud, and corruption.

Responsibilities

- 5.1 Overall responsibility for dealing with theft, allegations of bribery, fraud, and corruption rests with the Council's Chief Finance Officer, through statutory, "section 151", responsibilities and the Chief Executive.
- 5.2 Members and officers are encouraged to express concerns to the Chief Operating Officer, Chief Finance Officer, Monitoring Officer, Head of Internal Audit, Corporate Fraud Manager or any Service Manager in the knowledge that any statements will be treated seriously and in confidence.
- 5.3 It is the Council's intention to pursue all individuals or organisations who are suspected of having defrauded or committed corrupt acts and to report them to the Police if appropriate.
- 5.4 The Council's Members and colleagues will lead by example and ensure that they comply with all Council rules, regulations, instructions, and policies.
- 5.5 The Council's commitment to dealing with theft, fraud, bribery, and corruption is demonstrated by having in place systems and procedures designed to limit, as far as possible, the opportunities to commit fraudulent acts and to enable any such acts to be detected at an early stage. The Council also has a



Whistleblowing Policy to encourage people to raise concerns and enable the Council to take appropriate action.

- 5.6 Allegations of theft, fraud and corruption will be investigated in a prompt, thorough and professional manner.
- 5.7 In accordance with recognised good practice, the Anti-Theft, Fraud, Bribery and Corruption Policy will be reviewed every two years by The Chief Finance Officer.
- 5.8 Social Housing Fraud and Council Tax support/reductions are potentially highest risk for attempted fraud by people outside the Council. **Annex D - Housing Benefit and Local Council Tax Support** sets out the Council's particular provisions relating to this.

Culture

- 6.1 The Council wishes it to be known that the culture and tone of the authority is one of honesty and openness in all its dealings with wholehearted opposition to theft, fraud, bribery, and corruption in any form. The Council's Members and colleagues play an important part in creating and maintaining this culture.
- 6.2 The Council expects all suppliers, contractors, organisations, and individuals that it deals with to always act with honesty and integrity and with no thoughts of committing theft, fraudulent or corrupt acts. Those found to have committed offences risk having their contract terminated and may be prevented from tendering for future contracts with the Authority. An investigation is likely to be undertaken and prosecution action may be considered. The Council will in turn ensure that all its dealings will be on the same basis.



- 6.3 Officers will be encouraged to participate in local and national professional groups to exchange information, initiatives, and ideas, some of which will have fraud and corruption implications.
- 6.4 The Council's external auditors examine annually the Council's arrangements for the prevention, detection and investigation of theft, fraud and corruption and will report major deficiencies and concerns.

Raising Concerns

- 7.1 Colleagues are encouraged to raise any concerns about any issue or suspicion of fraud, bribery or corruption at the earliest possible stage or matters that concern the Council's method of operation. Concerns will be treated seriously and confidentially.
- 7.2 If Council colleagues have any concerns regarding theft, fraud, or corruption, they are encouraged to report the matter to their line manager or Chief Operating Officer, Chief Finance Officer, Monitoring Officer, Head of Internal Audit or Corporate Fraud Manager, as this will help us to promptly investigate the concern and review internal controls to prevent any further risk.
- 7.3 When raising concerns, colleagues and Members can be assured that confidences will be respected. Any allegation of theft, fraud and corruption will be dealt with in a thorough, prompt, professional and impartial manner. The Corporate Fraud Manager will liaise with HR to ensure the disciplinary process is initiated if necessary.
- 7.4 Members may wish to raise concerns with:
- the Chief Operating Officer
 - the Monitoring Officer;



- the Chief Executive; or
- the S151 Officer, as appropriate.

7.5 Members of the public, organisations, Council suppliers and contractors are also encouraged to raise any issues that concern them through the channels listed above.

7.6 Issues of concern can be reported via the Council's Whistleblowing Policy. If they involve theft, fraud or corruption they will be considered according to the provisions of this policy.

7.7 A copy of the Whistleblowing Policy is available on In-Site, the Council's intranet together with other related documents and associated guidance, including anonymous reporting and the contact details of Protect, a Whistleblowing charity that offers free, confidential advice to people concerned about crime, danger or wrongdoing at work.

Colleagues

8.1 The recruitment and retention of high calibre colleagues is vital if it is to deliver quality services. The Council will take steps at the recruitment stage to establish, as far as possible, the honesty and integrity of potential colleagues.

8.2 Recruitment will be in accordance with the Council's Recruitment and Selection procedures and Disclosure and Barring (DBS) (formally CRB) policy.

8.3 Officers are bound by the Officers Code of conduct, Contract Regulations and Financial Regulations, conditions of service and departmental codes of conduct. Note should be taken of the Council's position on the giving or receipt of gifts and/or hospitality. Officers are also bound by codes issued by relevant professional bodies of which they are members where these are relevant to the



officer's role within the Council. The Council has a comprehensive gifts and hospitality policy. Officers and Members should read the policy and where they are offered gifts or hospitality refer to the policy before acceptance, noting that whether they accept, or decline it is their individual responsibility to report the offer.

- 8.4 Employees must operate within Section 117 of the Local Government Act 1972, to give notice in writing of financial interests in contracts relating to the Council or the offer of any fees or rewards other than their proper remuneration.
- 8.5 The role of colleagues in the Council's systems and procedures will be as laid down in Contract Regulations and Financial Regulations, job descriptions, departmental instructions and any applicable procedural manuals.
- 8.6 The Council recognises the importance of training in the delivery of high-quality services. Officers are required to undertake mandatory Anti -Theft, Fraud and Corruption training when they join the authority (Fighting Fraud in Local Government) in addition to internal training delivered by the Corporate Fraud (Key Policies & Procedures V2 December 2020).
- 8.7 All new colleagues will receive training on fraud identification and reporting, particularly with regard to prevention of social housing fraud and council tax support/discount fraud, as part of their induction process.

Members

- 9.1 Members are required to operate within:
- The Council Constitution;
 - Government legislation;
 - the Members' Code of Conduct



- the Protocol on Member-Officer Relations;
- the Council's Contract Regulations /Financial Regulations;
- the Procedural Guidance for Planning and Licensing.

9.2 The above matters are specifically addressed in the Member Toolkit. All Members are required by the Localism Act 2011 to register pecuniary and other interests to the Monitoring Officer and to keep that information up to date.

9.3 These matters listed above are supported by briefings received by new Members after election. - This responsibility belongs to Democratic Services.

9.4 **The Chief Finance Officer has** responsibility for:

- risk management issues and making any recommendations therein;
- the overview of the Council's Whistleblowing Policy;
- the overview of the Council's Anti-Theft, Fraud and Corruption Policy;

Systems

10.1 The Council has in place Contract Regulations and Financial Regulations that give Members and officers clear instructions, or guidance, as to carrying out the Council's functions and responsibilities. The contents of these documents should be brought to the attention of all colleagues.

10.2 The Chief Finance Officer has a statutory duty under Section 151 of the Local Government Act 1972 to ensure that there are proper arrangements in place to administer the Council's financial affairs and safeguard Council assets.



10.3 The Internal Audit planning process incorporates a risk-based approach to planning audits, which considers the risk of fraud. This will help in determining the frequency of audits and the areas to focus attention on.

10.4 All of the Council's systems will incorporate, as far as is practicable, efficient and effective internal controls. The adequacy, appropriateness and effectiveness of internal controls will be independently reviewed by Internal Audit as part of their programme of work. Any weaknesses identified in internal control will be reported to management whose duty it will be to address and respond to all the issues raised.

Fraud Risk Assessment

11.1 The Council will maintain a Corporate Fraud Risk Assessment document (FRA) to effectively identify, describe and assess individual fraud risks and to develop these into a comprehensive fraud risk assessment. The FRA will include evaluation of mitigating controls, including understanding their limitations in order to proactively identify the Council's vulnerabilities to both internal and external fraud. In order to support the FRA, Heads of Service shall ensure that fraud prevention and detection is built-in to the design of any Council procedure or system (including digital services) so that integrity is maintained through system and procedure design. Such controls need to be effective and appropriate and proportionate for the procedure or system.

11.2 For example, with regard to raising a purchase order. A requisition is raised by a requisitioner, and a separate authorised officer provides approval.

Prevention, detection and investigation

12.1 The Council's systems should, where possible, incorporate internal control features that are designed such that theft, fraud, bribery and corruption should



not be possible without collusion. It is acknowledged that this will not eradicate fraud and error in systems. Dishonest acts can still be committed and agreed procedures circumvented.

12.2 The Council's Financial Regulations place a responsibility on certain officers to notify the Chief Finance Officer immediately of any irregularity or suspected irregularity.

12.3 The Chief Finance Officer will decide the initial action to be taken and determine the most appropriate person to undertake it (e.g. Internal Audit, the Corporate Fraud Manager, or another suitably trained person). In exceptional circumstances, where an allegation involves the Chief Finance Officer, the Chief Operating Officer will assume this role. In any event Internal Audit will be notified in all instances where fraud is suspected.

12.4 Depending upon the nature of any irregularity, Internal Audit/the Corporate Fraud Manager will work closely with management and other agencies, such as the Police, to ensure that all matters are investigated thoroughly and reported upon.

12.5 The Council will participate in the Cabinet Office National Fraud Initiative to share data for the purposes of detecting fraud and error and any local data matching exercises approved by Leadership Team.

Awareness and Training

13.1 The Council supports the concept of Anti-Theft, Fraud, Bribery and Corruption training for Members, Colleagues and employees to ensure that their responsibilities and duties are current, and their understanding reinforced.



13.2 The Procurement Team will act to ensure that those organisations that work with the Council to deliver services are made aware of the Council's strong Anti-Theft, Fraud, Bribery and Corruption policy and process, including their Whistleblowing Policy and process to report suspicions.

Redress and sanction

14.1 If the investigation indicates improper behaviour by an officer. Corporate Fraud may investigate allegations and/or initiate the Council's Disciplinary Policy and Procedure. The Council may involve the Police where serious and/or organised fraudulent or corrupt acts are discovered. This will be a matter for the Chief Finance Officer to decide in consultation with other relevant parties. Where fraud is found it will constitute as Gross Misconduct, as defined within the Council's Disciplinary Policy, and may result in dismissal.

14.2 If the investigation suggests improper behaviour by a Member, the procedures of the Council's Constitution, including relevant Codes or Protocols, will be followed.

14.3 If the investigation reveals theft, fraud, bribery or corruption by another person or organisation, the Council will take whatever remedial action it considers relevant to the circumstances, including instigating criminal or civil legal proceedings where appropriate.

Monitoring

Who
Leadership Team and S151 Officer



Audit and Corporate Governance Committee
--

Head of Internal Audit

Corporate Fraud Manager

15.1 The Policy will be monitored, reviewed and revised by stakeholders of the Council.

The Policy will be reported to the Audit and Corporate Governance Committee periodically to highlight developments and changes.

Progress against the policy and updates will be noted in the annual report to the Committee.

Annex

Annex A – Fighting Fraud Locally

Fighting Fraud and Corruption Locally 2020 is the updated counter fraud and corruption strategy for local government. It provides a blueprint for a coordinated response to fraud and corruption perpetrated against local authorities with the support of those at the top.

Local authorities continue to face a significant fraud challenge and while the official figures are dated the argument about protecting funds and vulnerable people remains.

The National Fraud Authority estimated local authorities face the threat of £2.1bn fraud in a year in 2013. In fact, the Annual Fraud Indicator produced by Crowe Clark Whitehill estimates that figure may be as high as £7.8bn in 2017, out of a total of £40.4bn for the public sector as a whole). The Government's Economic Crime Plan states that the numbers of fraud offences rose by 12% during 2018 to 3.6 million – constituting a third of all crimes in the UK.



Annex B – Nolan Committee

The Seven Principles of Public Life are the basis of the ethical standards expected of public office holders. They apply to both officers and members and are included in our Local Code of Governance.

<i>Selflessness</i>	Holders of public office should take decisions solely in terms of the public interest. They should not do so in order to gain financial or other material benefits for themselves, their family, or their friends.
<i>Integrity</i>	Holders of public office should not place themselves under any financial or other obligation to outside individuals or organisations that might influence them in the performance of their official duties.
<i>Objectivity</i>	In carrying out public business, including making public appointments, awarding contracts, or recommending individuals for rewards or benefits, holders of public office should make choices on merit.
<i>Accountability</i>	Holders of public office are accountable for their decisions and actions to the public and must submit themselves to whatever scrutiny is appropriate to their office.
<i>Openness</i>	Holders of public office should be as open as possible about all the decisions and actions that they take. They should give



	reasons for their decisions and restrict information only when the wider public interest clearly demands.
<i>Honesty</i>	Holders of public office have a duty to declare any private interests relating to their public duties and to take steps to resolve any conflicts arising in a way that protects the public interest.
<i>Leadership</i>	Holders of public office should promote and support these principles by leadership and example.

Annex C – Related policies

- Enforcement and Inspection Policy
- Whistleblowing Policy
- Recruitment & Selection Procedures
- Disclosure and Barring Service (DBS) (formally CRB) Policy
- Contract Regulations
- Financial Regulations
- Officer Code of Conduct
- Member Code of Conduct
- Disciplinary Policy & Procedure
- Protocol on Member – Officer Relations
- Procedural Guidance for Planning and Licensing
- Member Toolkit
- Disclosure Policy



Annex D – Housing Benefit and Local Council Tax Support

The Council shall make provisions to prevent, detect and punish instances of fraud committed against South Cambridgeshire District Council, including Social Housing Fraud and Council Tax Support/discount Fraud.

A robust verification process will be operated in accordance with national guidelines to verify the identity of claimants and eligibility to benefits.

The facility to report suspicions of fraud will be made available through the Council's website. Fraud can also be reported confidentially over the telephone to Customer Services.

The Council will maintain a suitably resourced investigation team to detect and investigate all fraud reports against South Cambridgeshire District Council. The Council's Professional Development processes will be actioned to ensure that team members are fully trained in the law relating to fraud investigation, national guidelines, good practice and internal procedures. The team may undertake investigation of other types of fraud if requested to do so.

Any employee with concerns about a potential benefit fraud may speak in confidence to the Corporate Fraud Manager or the Benefits Manager.

Investigation officers will be given authorisation under the scheme of delegations to investigate offences of fraud against the Council.

An interview room meeting the standards required by the Police and Criminal Evidence Act shall be made available to conduct formal recorded interviews held under caution. Health and Safety risk assessment will be undertaken, by the relevant officer, prior to operational activity post CV19 pandemic. Where the law allows, and it is considered both proportionate to the alleged crime and an effective use of



resources covert surveillance will be used to detect crimes and compile evidence. Sound and image recording equipment may be used to gather evidence during such surveillance. Covert surveillance will only be conducted when Judicial Approval has been obtained and following a risk assessment of safety and collateral intrusion.

Proper records will be kept of all surveillance and authorisations and will be made available to the Investigatory Powers Commissioner's Office upon request.

The Council will enter into a Joint Working Agreement with the Department for Works and Pensions, and work jointly with other local authorities, the police and other agencies to investigate and prevent fraud.

The Council will refer to relevant Corporate Policy's to ensure that action is taken and is proportionate and consistent, according to the Public Interest Test.

The names and address of those individuals convicted of fraud will be publicised where it is considered to be in the public interest. In particular where the publication will serve as a deterrent to others either engaged in or considering a similar course of conduct, or where it will raise public awareness of fraud and the mechanisms for reporting suspicions.

The Fraud Manager will make regular reports of the Council's counter fraud performance to the lead member for Finance.

The Council will participate in data matching through the Housing Benefit Matching Service and National Fraud Initiative and will subscribe to the National Anti-Fraud Network.



Annex E – Bribery Risk

The Bribery Act 2010 came into force on 1 July 2011 and places additional requirements on ‘commercial organisations’. Whilst the Council is not a ‘commercial organisation’ in terms of its normal local authority activities, guidance issued by the Chartered Institute of Public Finance & Accountancy (CIPFA) and the National Crime Agency (NCA) states that a court would view a local authority as a relevant organisation for the purposes of the Act. It is important therefore that the Council should have regard to the principles of the Act in the conduct of its activities and its policies and procedures, to ensure that it does not fall foul of the legislation.

The [Bribery Act 2010](#) makes it an offence to offer, promise or give a bribe (Section 1). It also makes it an offence to request, agree to receive, or accept a bribe (Section 2). Section 6 of the Act creates a new separate offence of bribing a foreign public official. There is also a corporate offence under Section 7 of failure by a commercial organisation to prevent bribery.

Our [Officers’ Code of Conduct](#) explains that the Bribery Act 2010 replaces the offences at common law and the Prevention of Corruption Acts with two general offences and prohibits the offering, giving, soliciting and acceptance of money or other advantage in order to induce or reward the improper performance of public and other functions.

The Act extends to all persons associated with the Council, including employees at all levels and grades, those permanently employed and temporary agency colleagues; Members (including co-opted or external Members); suppliers; contractors; partners; volunteers and consultants.

The first offence covers the offering, promising or giving of an advantage (broadly, offences of bribing another person).



The second deals with the requesting, agreeing to receive or accepting of an advantage (broadly, offences of being bribed).

Receiving a bribe (a potential example):

A supplier gives your nephew a job but makes it clear that in return they expect you to use your influence in our organisation to ensure we continue to do business with them.

It is an offence for a supplier to make such an offer. It would be an offence for you to accept the offer as you would be doing so to gain a personal advantage.

If the matter is dealt with in the Magistrates' Court and a person is found guilty of an offence under the Act, they are liable to imprisonment for a term not exceeding six months, or to a fine not exceeding the statutory maximum, or to both.

If the matter is so serious that it can only be tried before a jury and a person is found guilty of an offence under the Act, they are liable to imprisonment for a term not exceeding ten years, or to a fine, or to both.

Bribery is a criminal offence. The Council does not, and will not pay, offer, or request bribes to anyone for any purpose, nor does it or will it accept or receive bribes or improper inducements from anyone for any purpose. To use a third party to channel bribes to others is also a criminal offence.

The Council is committed to the prevention, deterrence and detection of bribery and has a zero-tolerance attitude towards bribery. There is an expectation and requirement that all individuals and organisations associated in whatever way with the Council will act with honesty and integrity and that Council employees at all levels, and Councillors, will lead by example in these matters.



Areas of the Council's business that could be exposed to the inherent risk of bribery include:

- Procuring of supplies, goods, or services.
- Awarding concessions, grants, and licenses.
- Approving planning applications.
- Selling or letting commercial properties.
- Cancelling liabilities (e.g., business rates, debtors).
- Allocating housing.
- Recruiting colleagues.
- Determining the course of enforcement action.

This is not an exhaustive list but sets out some of the areas where there may be a risk of bribery arising.

This Policy does not change the Council's policy on gifts & hospitality, which is set out in the Officers' Code of Conduct.

This page is left blank intentionally.

Notes to help those attending meetings in person at South Cambridgeshire Hall

Notes to help those people visiting the South Cambridgeshire District Council offices – please also refer to the Covid-security measures relating to meetings in the Council Chamber which are on the website page for each relevant meeting.

Members of the public wishing to view the meeting will be able to watch the livestream via the link which will be publicised before this meeting.

Members of the public wishing to attend the meeting in person, please contact Democratic Services at democratic.services@scamb.gov.uk

While we try to make sure that you stay safe when visiting South Cambridgeshire Hall, you also have a responsibility for your own safety, and that of others.

Security

When attending meetings in non-public areas of the Council offices you must report to Reception, sign in, and at all times wear the Visitor badge issued. Before leaving the building, please sign out and return the Visitor badge to Reception.

Public seating in meeting rooms is limited. For further details contact Democratic Services on 03450 450 500 or e-mail democratic.services@scamb.gov.uk

Emergency and Evacuation

In the event of a fire, a continuous alarm will sound. Leave the building using the nearest escape route; from the Council Chamber or Mezzanine viewing gallery this is via the staircase just outside the door. Go to the assembly point at the far side of the staff car park opposite the staff entrance

- **Do not** use the lifts to leave the building. If you are unable to use stairs by yourself, the emergency staircase landings have fire refuge areas, which give

protection for a minimum of 1.5 hours. Press the alarm button and wait for help from Council fire wardens or the Fire and Rescue Service.

- **Do not** re-enter the building until the officer in charge or the Fire and Rescue Service confirms that it is safe to do so.

First Aid

If you feel unwell or need first aid, please alert a member of staff.

Access for People with Disabilities

We are committed to improving, for all members of the community, access to our agendas and minutes. We try to take all circumstances into account but, if you have any specific needs, please let us know, and we will do what we can to help you. The Council Chamber is accessible to wheelchair users. Infra-red hearing assistance systems are available in the Council Chamber and viewing gallery. To use these, you must sit in sight of the infra-red transmitter and wear a 'neck loop', which can be used with a hearing aid switched to the 'T' position. If your hearing aid does not have the 'T' position facility then earphones are also available and can be used independently. You can get both neck loops and earphones from Reception.

Toilets

Public toilets are available on each floor of the building next to the lifts. These include facilities for disabled people.

Recording of Business and Use of Mobile Phones

We are open and transparent about how we make decisions. Public meetings are webcast and are also recorded, but we allow recording, filming and photography at Council, Cabinet and other meetings, which members of the public can attend, so long as proceedings at the meeting are not disrupted. We also allow the use of social media during meetings to bring Council issues to the attention of a wider audience. To minimise disturbance to others attending the meeting, please switch your phone or other mobile device to silent / vibrate mode.

Banners, Placards and similar items

You are not allowed to bring into, or display at, any public meeting any banner, placard, poster or other similar item. If you do so, the Chair will suspend the meeting until such items are removed.

Disturbance by Public

If a member of the public interrupts proceedings at a meeting, the Chair will warn the person concerned. If they continue to interrupt, the Chair will order their removal from the meeting room. If there is a general disturbance in any part of the meeting room open to the public, the Chair may call for that part to be cleared. The meeting will be suspended until order has been restored.

Smoking

Since 1 July 2008, South Cambridgeshire District Council has operated a Smoke Free Policy. No one can smoke at any time within the Council offices, or in the car park or other grounds forming part of those offices.

Food and Drink

Until the lifting of Covid restrictions, no vending machines are available. Bottled water is available for attendees at meetings.

This page is left blank intentionally.