South Cambridgeshire Hall
Cambourne Business Park
Cambourne
Cambridge
CB23 6EA

t: 03450 450 500
f: 01954 713149
www.scambs.gov.uk

South Cambridgeshire District Council

16 March 2020

To: Chairman – Councillor Tony Mason
Vice-Chairman – Councillor Nick Sample
Members of the Audit and Corporate Governance Committee – Councillors John Batchelor, Mark Howell, Brian Milnes, Bunty Waters, Heather Williams and Eileen Wilson
Quorum: 3

Substitutes: Councillors Nick Wright, Tom Bygott, Grenville Chamberlain, Graham Cone, Clare Delderfield and Dawn Percival

Dear Councillor

You are invited to attend the next meeting of **AUDIT AND CORPORATE GOVERNANCE COMMITTEE**, which will be held in **SWANSLEY ROOM A AND B - GROUND FLOOR** at South Cambridgeshire Hall on **TUESDAY, 24 MARCH 2020** at **9.30 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 **1 - 4**
To confirm the minutes of the meeting held on 19 December 2019 as a correct record.

AUDIT REPORTS

4. Internal Audit Update **5 - 20**

5.	**Completion of the 2017/18 Audit of the Accounts and Timescales for the 2018/19 and 2019/20 Accounts and Audit**	**21 - 26**

DECISION ITEMS

6.	**Regulation of Investigatory Powers Act 2000 (RIPA) Amendments to Policy & Update on Use of RIPA**	**27 - 88**

INFORMATION ITEMS

7. Matters of Topical Interest

8. Date of Next Meeting

The next meeting will be held on Tuesday 28 July at 9:30am in the Swansley Room.

GUIDANCE NOTES FOR VISITORS TO SOUTH CAMBRIDGESHIRE HALL

Notes to help those people visiting the South Cambridgeshire District Council offices

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@scambs.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 would be 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 brigade.
- ***Do not*** re-enter the building until the officer in charge or the fire brigade 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. All meeting rooms are accessible to wheelchair users. There are disabled toilet facilities on each floor of the building. 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.

Recording of Business and Use of Mobile Phones

We are open and transparent about how we make decisions. 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. Failure to do so, will result in the Chairman suspending the meeting until such items are removed.

Disturbance by Public

If a member of the public interrupts proceedings at a meeting, the Chairman will warn the person concerned. If they continue to interrupt, the Chairman 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 Chairman 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 is allowed to smoke at any time within the Council offices, or in the car park or other grounds forming part of those offices.

Food and Drink

Vending machines and a water dispenser are available on the ground floor near the lifts at the front of the building. You are not allowed to bring food or drink into the meeting room.

This page is left blank intentionally.

SOUTH CAMBRIDGESHIRE DISTRICT COUNCIL

Minutes of a meeting of the Audit and Corporate Governance Committee held on Thursday, 19 December 2019 at 9.30 a.m.

PRESENT:	Councillor Tony Mason – Chairman Councillor Nick Sample – Vice-Chairman	
Councillors:	John Batchelor	Mark Howell
	Brian Milnes	Eileen Wilson
Officers:	Patrick Adams	Senior Democratic Services Officer
	Tracey Flack	Principal Accountant
	Daniel Hasler	Accountancy Assistant
	Peter Maddock	Head of Finance
Auditors:	Suresh Patel	Ernst & Young
	Mark Russell	Ernst & Young
	Jonathan Tully	Head of Shared Internal Audit

Councillors Bridget Smith and John Williams were in attendance, by invitation.

1. APOLOGIES FOR ABSENCE

Apologies for Absence were received from Councillor Peter Topping and Heather Williams. Councillor Mark Howell substituted for Councillor Peter Topping.

2. DECLARATIONS OF INTEREST

Councillor John Batchelor declared a non pecuniary interest as an unpaid Director of Ermine Street Housing.

3. MINUTES OF PREVIOUS MEETING

The minutes of the meeting held on 24 September 2019 were agreed as a correct record.

Housing re-evaluation
Peter Maddock agreed to ascertain when the next housing re-evaluation would be taking place.

4. TREASURY MANAGEMENT - ANNUAL REPORT 2018/19

The Head of Finance introduced this report, which outlined the Treasury Management activities in the financial year 2018/19.

Short-term borrowing
It was noted that the £3m borrowed from other local authorities was a short-term loan and had been repaid. It was understood that the Council also transferred funds internally to use for capital expenditure. This was referred to as “internal borrowing” and was temporary. The rates from other local authorities were competitive and far better than the Public Works Loan Board (PWLB).

The Head of Finance explained that all external borrowing had been agreed on a fixed rate for 2018/19, as these rates had been and remained competitive.

Benchmarking
The Head of Finance reported that the Council's return on investments was better than the client average, but the level of risk was higher. The Head of Finance assured the Committee there was a balancing act between gaining the best returns from investing in the short-term funding and long-term, but currently the difference in rates was minimal.

The Committee **APPROVED** the Treasury Management Annual report.

5. MID-YEAR 2019/2020 TREASURY MANAGEMENT REPORT

The Head of Finance presented this agenda item on the mid-year treasury management report to 30 September 2019. It was noted that the Treasury Management Policy and Treasury Management Strategy Statement had been found to be appropriate and no changes were required.

Ice rink
It was noted that the Council had made a long-term investment in the Ice Rink at Milton. In response to a query from the Committee regarding the monitoring of the Ice Rink's performance, Councillor John Williams explained that the Council would receive a review after six months of the rink opening, which equated to approximately three months from the date of the meeting.

Public Loan Work Board (PLWB)
It was noted that the PWLB's rate for loans had increased from 1.3% to 2.3%, but a discount of 0.2% could be claimed by the Council, providing it notified the Government in advance. The Council had applied to borrow at this rate until November 2020.

Income
It was noted that the Council expected to receive £842,000 in rental income for 2019/20 and receive £1.5m more in income than predicted.

Duration of investments
The Accounts Assistant explained that the advice on the length of the investment period had changed to six months or 100 days, but this was not compulsory. This explained why investments had been made that exceeded this period.

It was noted that the Council was reprofiling its investments away from 1 year deposits to shorter periods and increase its investments in instant access money market funds. This will allow the Council to cover investment strategy purchases while minimising our borrowing. The Committee supported an increase in liquidity, on the understanding that this would decrease the need for borrowing.

The Committee **NOTED** the report.

6. FINAL ACCOUNTS UPDATE 2017/18 - ERNST & YOUNG'S REPORT (REPORT TO FOLLOW)

Suresh Patel presented this report, which summarised external audit's preliminary audit conclusion in relation to the audit of the Council for 2017/18. He introduced Mark Russell, who had been a manager for EY since 2019 and was helping to complete the audit.

Executive summary
Suresh Patel reported that the external auditors had issued a qualified conclusion on finance reporting and for the third consecutive year the Council had been unable to

publish its accounts according to its timetable. There was no evidence of any deliberate errors, but one mistake in relation to NNDR income totalled approximately £3.5m. The report included recommendations for improvements and the Head of Finance explained that he would liaise with the external auditors on how to improve the whole process. Mark Russell added that a planning meeting would take place to discuss how the 2018/19 accounts would be audited.

Audit fee
Suresh Patel stated that the external auditors would be charging an extra £140,000 for the additional work carried out on this audit and this claim would be supported with detailed evidence. Members of the Committee and the Lead Cabinet Member for Finance were opposed to this level of increase, as the external auditors had been partly responsible for the delays and the extra work this incurred. Suresh Patel explained that these accounts were the most difficult he had encountered in 25 years and the charge was a fair reflection of the additional work involved. The Head of Finance explained that the Council's contract was with the Public Sector Audit Appointments (PSAA) and any dispute regarding fees would have to be resolved by them.

It was noted that the annual fee of £52,000 would be reduced by 20% for the 2018/19 accounts.

Letter of representation
The Head of Finance agreed to get legal advice on possible amendments to the letter of representation.

Future accounts
Suresh Patel agreed to amend his comments on the risk relating to the signing off of the 2019/20 accounts, which related to timings and not processes. It was noted that the 2018/19 accounts would have to be signed off in the new year before the 2019/20 accounts could be finalised.

Final testing
Suresh Patel explained that the final testing was being carried out that morning. An error had been discovered on the creditors account, but this was not material. He predicted that the external auditors would be able to sign off the accounts in early January, following a thorough check.

It was suggested that this report should come back to the Committee, after external audit had approved the Accounts. However, this was countered with the view that providing there were no significant changes, the Committee should give delegated authority to the Chairman to sign-off the accounts. The Head of Finance explained that any adjustment to the 2017/18 accounts at this stage was historic and he recommended that the Committee agree the accounts. He added that for understandable reasons these accounts were being more thoroughly audited than any other accounts he had known.

A vote was taken and with 5 votes in favour and 1 against, the Committee

AGREED to instruct the Chairman to sign-off the approved accounts, providing no material changes were necessary.

Councillor Mark Howell asked that his vote against be recorded.

7. FINAL ACCOUNT 2017/18 UPDATE - COUNCIL'S REPORT

The Head of Finance explained that the Committee were required to approve the accounts

and the Annual Governance Statement. It was noted that the Annual Governance Statement had already been approved by the Committee, but the correct procedure was for them to be formally agreed again.

The Head of Finance explained that a temporary member of staff who had suitable experience had been hired to assist in the process of closing the 2018/19 accounts. It was hoped that the 2018/19 accounts would be agreed by the end of January and then audited by the end of March. The aim was to then have the 2019/20 accounts agreed by the end of May. In response to questioning, the Head of Finance reiterated that it was preferable to delay the finalising of the accounts, than to submit accounts that he had no faith in. It was agreed that a Task and Finish Group should be held in February to review the progress being made on the 2018/19 accounts.

The Leader, the Lead Cabinet Member for Finance and the Chairman of the Committee all thanked the Head of Finance and his team for their efforts in preparing the accounts, which had required the correction of the problems of the past.

The Committee

AGREED

A) To approve the Annual Governance Statement.
B) To approve the 2017/18 Statement of Accounts, subject to the final audit procedure.
C) To note the proposed timetable for the completion and audit of the 2018/19 Statement of Accounts.

8. MATTERS OF TOPICAL INTEREST

Training
It was noted that external audit had agreed to provide the Committee with an Audit Toolkit. The Head of Finance agreed to contact the Chartered Institute of Public Finance and Accountancy (CIPFA) to arrange suitable training for the Committee.

9. DATE OF NEXT MEETING

It was noted that the next meeting was scheduled for Tuesday 24 March at 9:30am in the Swansley Room.

The Meeting ended at 11.15 a.m.

South Cambridgeshire District Council

REPORT TO:	Audit & Corporate Governance Committee	24th March 2020
LEAD CABINET MEMBER:	Not applicable	
LEAD OFFICER:	Head of Shared Internal Audit	

Internal Audit update

Executive Summary

1. The purpose of this report is to inform the committee of the work of Internal Audit, completed between October 2019 to March 2020, and operational developments.
2. The role of Internal Audit is to provide the Audit & Corporate Governance Committee, and Management, with independent assurance on the effectiveness of the internal control environment.

Recommendations

3. It is recommended that the Committee note the contents of the report.

Reasons for Recommendations

4. Regular reporting to the Audit & Corporate Governance Committee helps the Committee to understand the governance, risk and control environment, and contribute to the completion of the Annual Governance Statement.

Details

5. The Accounts and Audit Regulations 2015 require that the Council "must undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes; taking into account public sector internal auditing standards or guidance."
6. Internal Audit assists the Council, and the Audit & Corporate Governance Committee, to discharge its governance responsibilities. Our work supports the Council's corporate objectives, and the corporate governance framework.
7. Internal audit coverage is planned so that the focus is upon those areas and risks which will most impact upon the council's ability to achieve its objectives.
8. Internal Audit work should help add value to the Council by helping to improve systems, mitigate risks, and subsequently inform the Annual Governance Statement.

Options

There are no options to consider.

Implications

There are no significant implications arising.

Effect on Council Priority Areas

Growing local businesses and economies

Not applicable

Housing that is truly affordable for everyone to live in

Not applicable

Being green to our core

Not applicable

A modern and caring Council

The Internal Audit Plan is a key component in helping to provide assurance that the Council has a robust Governance, Risk and Control framework. The plan is cross-cutting, as it considers all Council activities, and also contributes to all Council Priorities.

Background Papers

Not applicable

Appendices

Appendix A: Progress Report

Appendix B: Glossary of terms

Report Author:

Jonathan Tully – Head of Shared Internal Audit

Telephone: (01223) 458180

Appendix A – Progress report

South Cambridgeshire District Council

Introduction

1. Management is responsible for the system of internal control and establishes policies and procedures to help ensure that the system is functioning correctly. On behalf of the Audit & Corporate Governance Committee, Internal Audit acts as an assurance function by providing an independent and objective opinion on the control environment.

2. The purpose of this report is to provide an update on the recent work completed by Internal Audit. The information included in the progress report will feed into and inform our overall opinion in the annual Head of Internal Audit (HoIA) report. This opinion will in turn be used to inform the Annual Governance Statement which accompanies the Statement of Accounts. We previously provided an update, to the committee, in September 2019.

3. Where appropriate reports are given an overall opinion based on four levels of assurance. This is based on the evaluation of the control environment, and the type of recommendations we make in each report. If a review has either "Limited" or "No" assurance, the system is followed up to review if the actions were implemented promptly and effectively. Further information is available in Appendix B – Glossary of terms.

Resources and team update

Audit plan

4. An audit plan is presented at least annually to the Audit & Corporate Governance Committee. It is good practice to continually review the plan, to reflect emerging risks, revisions to corporate priorities, and changes to resourcing factors. The latest internal audit plan commenced from April 2019.

5. Progress of the plan delivery is illustrated on the following pages for information.

ISO assurance framework

6. The Council's Commercial Waste Service has been certified to ISO14001 and ISO9001 since September 2015. This has in turn demonstrated the Council and the Service's commitment to deliver excellence in waste collection services, meeting and exceeding its green targets which include environmental management and pollution control.

7. BSI attend the Service on regular intervals as set out in their audit programme and assess whether the standards are being upheld.

8. One of the ISO14001 requirements is that Management undertake their own internal audits of the standard's requirements. Earlier in the year we developed an embedded assurance framework to comply with the standards. This enabled us to undertake a pre-inspection audit of the scheduled elements expected to be reviewed by the BSI Auditor. The purpose of this is to:

   (a) ensure that the elements to be scrutinised by the external auditor have been reviewed by Management and improved where required; and

   (b) demonstrate that the Shared Waste Service has an effective internal audit function as required by the ISO Standard.

9. We have now undertaken two reviews using this approach and feedback from the BSI auditor on our approach was positive.

Progress of the plan

Finalised reviews

The following audit and assurance reviews have reached completion, since the previous report to the committee:

Audit	Assurance and actions		Summary of report and actions
Payroll	**Assurance:** Current: Previous: **Actions:** Critical High Medium Low	 Reasonable Reasonable 0 1 4 3	The objectives of the Payroll system are to ensure the Council pays the right people, the right amount at the right time. Payroll is one of the Council's core financial systems and processed approximately £12m in salary payments in 2018/19. Given the importance of the system and the materiality of payments processed it is essential that there are sufficient and robust controls in place. Our testing provided reasonable assurance that controls are operating effectively.

Audit	Assurance and actions		Summary of report and actions
Accounts Receivable	**Assurance:** Current: Previous: **Actions:** Critical High Medium Low	 Limited Limited 0 5 4 3	Teams within the Council charge for services such as planning fees and obligations, licensing, trade waste, garage rent, home loans and life-lines. Debt collection and monitoring is undertaken by a Sundry Debtors team. A new Financial Management System (T1) went live on 1st October 2018, and we completed a review of the Sundry Debtor system. The Council's arrangements for managing and monitoring debts is effective, and the Sundry Debtors' team has made good progress with using the new T1 system. There are good transactional controls for setting up new accounts, invoices, credit notes and processing write offs. Our sample testing confirmed that invoices are being raised promptly for the correct amount. There are good controls in place for monitoring and managing levels of debt. As at 31 March 2019, the value of sundry debt arrears was 3.8% of the total invoices raised. We were only able to provide limited assurance overall as system reconciliations had not been completed following the implementation of T1. Postings had been made to two default suspense accounts but had not been cleared, and the Council has raised this as a technical point with T1 consultants for resolution. Regular reconciliation will provide assurance that all sundry income has been reconciled to the general ledger and has been accounted for correctly.

Audit	Assurance and actions		Summary of report and actions
Grant assurance - Disabled Facility Grant	**Assurance:** Current: Previous: **Actions:** Critical High Medium Low	 Reasonable Full 0 0 0 2	Central Government funding is allocated to the County Councils as part of the Better Care Fund. A proportion of this is allocated to District Councils to enable them to carry out improvements to housing stock, and for disabled adaptations. We reviewed a sample of grants from the financial year, plus their supporting documentation and transactions. This provided assurance that: • grant applications were legitimate, and only awarded to eligible applicants; • applications were supported by a qualified and independent medical referral; • applications were processed promptly; • suppliers and contractors were appropriately procured, and awarded based on value for money; • any project cost variations were appropriately reviewed and approved; • financial records were completed and reconciled; • projects were effectively managed by the Home Improvement Agency; and • grants were used for capital expenditure as set out in the MHCLG conditions. Management have agreed to include additional data in the T1 accounting system to assist reporting, and also to review the template grant spreadsheets used to calculate Agency fees and VAT, which will minimise the risk of calculation errors.

Audit	Assurance and actions		Summary of report and actions
Program assurance - ISO14001 - Visit 2	**Assurance:** Current: Previous: **Actions:** Critical High Medium Low	 Reasonable Reasonable 0 0 0 0	We completed a Program Assurance review to support the periodic BSI inspection, which covered: • documentation, policies and procedures; • planning for risk and opportunity; • compliance obligations and evaluation of compliance; • objectives and targets, monitoring and measuring; • training, competence and awareness; • internal and external communication; • operational control and change management – depot tour; • emergency preparedness and response; and • nonconformity, correction and corrective action The team had made progress through implementation of previous actions. There were no significant non-conformities arising.
Program assurance - ISO9001 - Visit 2	**Assurance:** Current: Previous: **Actions:** Critical High Medium Low	 Reasonable Reasonable 0 0 0 0	We completed a Program Assurance review to support the periodic BSI inspection, which considered: • Quality Management System; • product realisation, service delivery and inspection (monitoring); • customer feedback including customer complaints; and • plant, equipment and control of monitoring & measuring equipment. The team had implemented previous actions; and there were no significant non-conformities arising.

Works in Progress

The following reviews are currently in progress and plan updates:

Audit	Assurance and actions		Summary of current position and any emerging points
HRA – Voids and lettings	Previous:	Limited	We have completed our testing and are currently finalising our report.
Carbon Management – Data Quality	Previous:	New review	We have completed our testing and are currently finalising our report.
Capital - Strategy & Asset Management	Previous:	New review	We have completed our testing and are currently finalising our report.
Project Management Framework	Previous:	Limited	We have completed our testing and are currently finalising our report.
Key Performance Indicators	Previous:	Reasonable	We have completed our testing and are currently finalising our report.
Emergency planning - Business Continuity	Previous:	New review	We are currently undertaking our testing in this area.
Legal services	Previous:	New review	We are currently undertaking our testing in this area.
Accounts Payable	Previous:	New review	We are currently undertaking our testing in this area.
Main Accounting System	Previous:	New review	We are currently undertaking our testing in this area.
HRA – Former tenant Arrears	Previous:	New review	Now scheduled to commence in 20/21 following annual billing

Audit	Assurance and actions		Summary of current position and any emerging points
Scheme of Delegation	Previous:	New review	Now scheduled to commence in 20/21 following organizational change

Other assurance and consultancy work

Below is a summary of other work completed to date, from the current year. These have already been reported to the Audit & Corporate Governance Committee, will be used to inform the annual opinion, and further information can be read in the previous committee reports.

Assurance			Actions			
System reviewed	**Date last reported:**	**Assurance / Status:**	**Critical:**	**High:**	**Medium:**	**Low:**
Annual Internal Audit Opinion	July 2019	Completed	0	0	0	0
Public Sector Internal Audit Standards	July 2019	Completed	0	0	0	0
National Fraud Initiative	July 2019	Ongoing	0	0	0	0

Counter fraud and corruption update

10. The Council participates in a national data matching service known as the National Fraud Initiative (NFI), which is run by the Cabinet Office. Data is extracted from Council systems for processing and matching. It flags up inconsistencies in data that may indicate fraud and error, helping councils to complete proactive investigation. Nationally it is estimated that this work has identified £1.69 billion of local authority fraud, errors and overpayments since 1996. Historically this process has not identified significant fraud and error at the Council, and this provides assurance that internal controls continue to operate effectively. Work has commenced on reviewing the current matches from the biennial exercise and will continue throughout the year. In January we completed data quality assurance of Council Tax and Electoral Roll data, prior to submission to the Cabinet Office for the annual exercise. The Council procures the premium matching service, which provides an enhanced profiling of high-risk cases, and consequently provides assurance that other individuals entitled to the discount are receiving it correctly. Any significant matters arising in terms of fraud and error will be reported, and there are no matters arising at this time.

Other audit and assurance activity

11. We have provided advice and consultancy, and also completed some special investigations in the period. A contingency resource is included within our plan to manage a reasonable amount of unplanned work.

12. We are currently undertaking compliance reviews for Ermine Street Housing and will be reported through the Board. This will also provide assurance for South Cambs Ltd which we can report to this committee.

13. We continue to review the governance framework which includes preparing the Annual Governance Statement, and the Local Code of Governance, which accompanies the Statement of Accounts. We have drafted the 18/19 Annual Governance Statement, which is ready for review with the accompanying Statement of Accounts.

Appendix B – Glossary of terms

Assurance ratings

Internal Audit provides management and Members with a statement of assurance on each area audited. This is also used by the Head of Shared Internal Audit to form an overall opinion on the control environment operating across the Council, including risk management, control and governance, and this informs the Annual Governance Statement (AGS).

Term	Description
Full Assurance	Controls are in place to ensure the achievement of service objectives and good corporate governance, and to protect the Authority against significant foreseeable risks.
Reasonable Assurance	Controls exist to enable the achievement of service objectives and good corporate governance, and mitigate against significant foreseeable risks. However, occasional instances of failure to comply with control process were identified and/or opportunities still exist to mitigate further against potential risks.
Limited Assurance	Controls are in place and to varying degrees are complied with, however, there are gaps in the process which leave the service exposed to risks. Therefore, there is a need to introduce additional controls and/or improve compliance with existing ones, to reduce the risk exposure for the Authority.
No Assurance	Controls are considered to be insufficient, with the absence of at least one critical control mechanism. There is also a need to improve compliance with existing controls, and errors and omissions have been detected. Failure to improve controls leaves the Authority exposed to significant risk, which could lead to major financial loss, embarrassment, or failure to achieve key service objectives.

Organisational impact

The overall impact may be reported to help provide some context to the level of residual risk. For example if no controls have been implemented in a system it would have no assurance, but this may be immaterial to the organisation. Equally a system may be operating effectively and have full assurance, but if a risk materialised it may have a major impact to the organisation.

Term	Description
Major	The risks associated with the system are significant. If the risk materialises it would have a major impact upon the organisation.
Moderate	The risks associated with the system are medium. If the risk materialises it would have a moderate impact upon the organisation.
Minor	The risks associated with the system are low. If the risks materialises it would have a minor impact on the organisation.

Actions

As part of our reviews we identify opportunities for improvement, which have been shared with Management. These are developed into actions to improve the effectiveness of the governance, risk management arrangements, and the internal control environment.

Management are responsible for implementing their actions and providing assurance when they are completed. Timescales for implementing actions should be proportionate and achievable to the available resources. To help prioritise the actions we have produced guidance below:

Priority	Description	Timescale for action	Monitoring
Critical	Extreme control weakness that jeopardises the complete operation of the service.	To be implemented immediately.	Within 1 month
High	Fundamental control weakness which significantly increases the risk / scope for error, fraud, or loss of efficiency.	To be implemented as a matter of priority.	Within 6 months
Medium	Significant control weakness which reduces the effectiveness of procedures designed to protect assets and revenue of the Authority.	To be implemented at the first opportunity.	Within 12 months
Low	Control weakness, which, if corrected, will enhance control procedures that are already relatively robust.	To be implemented as soon as reasonably practical.	Within 24 months

The Council has a Risk Management system, which is used for tracking their progress.

This page is left blank intentionally.

South Cambridgeshire District Council

Report To:	Audit and Governance	24th March 2020
Lead Cabinet Member(s):	Councillor John Williams, Lead Cabinet Member for Finance	
Lead Officer:	Peter Maddock, Head of Finance	

COMPLETION OF THE 2017/18 AUDIT OF THE ACCOUNTS AND TIMESCALES FOR THE 2018/19 and 2019/20 ACCOUNTS AND AUDIT

PURPOSE

1. To update the Committee on the latest position regarding the accounts for 2017/18, 2018/19 and 2019/20.

RECOMMENDATIONS

2. **To note the position with the 2017/18 Statement of Accounts and proposed timetable for the completion and audit of the 2018/19 and 2019/20 accounts.**

REASON FOR RECOMMENDATION

3. The 2017/18 accounts audit is nearing completion and once these are completed and signed off focus will shift to the 2018/19 and 2019/20 accounts.

BACKGROUND INFORMATION

Introduction

4. There is a requirement under the Accountancy and Audit Regulations for Council's to present their accounts for the preceding financial year for audit by 31st of May each year and an expectation for those accounts to be audited and published by 31st July each year.

2017/2018 Accounts

5. As regards 2017/18 I do not propose to go through the issues with the accounts prior to December 2019 again but concentrate on what has happened since then.

6. At the last meeting a set of accounts was presented and approved subject to their not being any further 'significant' issues identified. It was noted that there was still an outstanding issue to resolve and following investigation it soon became clear that there was a further material error within the accounts.

7. The completion of the audit has been impacted to a degree by staff sickness both within the Council and Ernst and Young (EY), but also accountancy staff have been

finalising the 2020/21 budget during January and the first couple of weeks of February.

8. EY also carry out the Housing Benefit audit and the Department for Work and Pensions (DWP) deadline for this is 30th November. Due to difficulties concluding accounts audits across the County an extension was sought and agreed by the DWP to 29th February. This audit has to be completed by the agreed deadline otherwise the DWP has the power to impose financial penalties on the Council. This audit was completed and signed off ahead of the revised deadline but of course the work was carried out during January and February.

9. Having said this the substantive audit work has now been completed and making sure the adjustments identified have been carried out and correctly reflected in the accounts is no small task given the sheer number of adjustments necessary. This process is currently being undertaken and whilst it was hoped that it would be completed in time for this meeting this now looks unlikely.

10. The Council has recently taken on an additional resource to complete the accounts for 2017/18 and future years. This colleague has considerable experience in this area and has previously worked in audit so has a good understanding of the processes they undertake and the information they need to complete the audit. It should therefore be possible to complete this work and get the accounts signed off by the end of March. It will then be necessary for the Committee to re-approve the accounts as soon as practically possible after everything has been concluded.

11. The other related issue is that of the Asset Register. Since 1st April 2007 accounting for Non-Current Assets has become more complicated and it is generally recognised that in order to keep track of individual assets a proper asset register system is required. Whilst this should have been done some years ago we now have a proper asset register system that has in excess of 5,500 individual assets on it the majority being HRA dwellings. A lengthy process of reconciling this to the 2017/18 accounts has been ongoing for sometime and we have finally achieved this in the last week or so.

2018/2019 Accounts

12. Turning to the 2018/19 accounts. These have been substantially prepared but cannot be completed until the final position for 2017/18 has been ascertained and the asset register reconciled for 2018/19 too.

13. One of the issues with 2017/18 was the lack of working papers and evidence to support the figures in the accounts. A significant amount of effort has been put in to ensuring that there is enough information and evidence for the audit when it does take place which should mean a smoother audit and take less time. There will also need to be plenty of reasonableness checking in an effort to reduce the number of errors and given the recent history surrounding accounts preparation this may take a while.

14. Having said that as soon as the 2017/18 accounts are complete we can move straight to the 2018/19 accounts and providing the final outstanding capital transaction are processed, checked and put into the statements fairly quickly a set of accounts can probably be ready within a month or so.

15. Once completed they can be published and presented for audit. EY have said they will not be able to audit the 2018/19 accounts until September but it makes sense to complete the 2018/19 accounts albeit subject to audit so we can then move on to the 2019/20 accounts. The audit of the 2018/19 accounts should be completed by the end of October or early November.

2019/2020 Accounts

16. Work on the 2019/20 accounts is already taking place. For example the housing stock valuation work was completed and valued at 29th February and a reasonableness check is being carried out. This work can be carried out in isolation and there are a number of other tasks that can be done before we reach the year end. Most of the year end transactions are carried out by colleagues who are not involved in either the 2017/18 or 2018/19 accounts so the two processes should not conflict with each other to a significant extent.

17. When the accounts are prepared to the proper timetable it is usual to do most of the year end transactions in April and the first week of May and put the statement together after that. The intention is to try to meet this timetable for 2019/20 if at all possible but given the amount of work needed between now and then this seems a very tall order. There is also the issue of publishing a draft set of 2019/20 accounts before the previous year is audited and unsurprisingly the Accounts and Audit Regulations do not envisage this situation occurring, so the legality and practicality of this approach needs to be fully explored.

18. As regards the audit EY have said they can go straight onto the 2019/20 audit after they have completed 2018/19 so it is possible we might be up to date by Christmas 2020 but there is a possibility that this will continue until January 2021. The colleague working on the accounts is with us until 30th November 2020 but providing he is willing and able it would make sense to keep him on until the 2019/20 audit is complete.

Other Issues

19. As well as getting the final accounts process back on track there is the issue of making sure, going forward, we are in a position to complete the accounts to timetable and to a satisfactory standard. This involves a degree of staff training as significant knowledge was lost back in 2017 and this has never been fully restored. Some progress has been made on this but because of the protracted nature of the 2017/18 accounts and other work commitments much of this is still to be done. The period between mid-June and mid-September of this year is probably the first opportunity we will get to address this fully but it should be enough time to do so.

20. It is proposed that a set of final accounts guidance papers are produced detailing the accounting treatment for particular aspects of the accounts as these can be quite complex and difficult to follow. Local Authority accounts are very different to the private sector and indeed more complex not least because of the need to exclude certain items from the deficit or surplus for the year to calculate the amount chargeable against the Council Tax and/or Housing Rents.

21. The final issue is with the accounting system which whilst it records transactions accurately and is capable of producing all the information needed for the final accounts it has not been set up in the most efficient manner and the coding structure

is not the best. Work therefore needs to be done to get the system working in a way that makes our life easier and all transactions are grouped in the appropriate manner.

Summary Position

22. The 2017/18 accounts audit should be complete by the end of March and both the 2018/19 and 2019/20 should follow within a few months afterwards. The Audit though is unlikely to be completed until the autumn so 2020/21 will probably be the first year for sometime that we are on track to meet the required timetable.

OPTIONS

23. There are few other options available to the Council. The accounts need to be completed and audited the only other options are around amending the timeline. If we try and complete the accounts sooner there is more chance of error but since they are not going to be audited for sometime this does not make much sense. Alternatively we could delay accounts completion but we then run the risk of affecting the audit timeline which from past experience could mean it takes even longer to get the process back on track.

IMPLICATIONS

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

Policy

25. Timely and robust consideration of the Council's accounts is vital to ensure that corporate procedures and priorities are met and the financial position of the Council is effectively managed and monitored.

Legal

26. There is a requirement under the Accountancy and Audit Regulations for Council's to present their accounts for the preceding financial year for audit by 31st of May each year and for those accounts to be audited and published by 31st July each year.

Financial

27. Timely and robust consideration of the Council's budgets is vital to ensure that financial statements are correctly stated, financial procedures are followed and that the financial position of the Council is effectively managed and monitored. The failure to deliver the 2017/18 accounts on time and without error has lead to additional cost to the Council.

Risk

28. There is a risk that the financial statements are incorrectly stated with consequential impacts.

Environmental

29. There are no environmental implications arising directly from the report.

Equality Analysis

30. In preparing this report, due consideration has been given to the District Council's statutory Equality Duty to eliminate unlawful discrimination, advance equality of opportunity and foster good relations, as set out in Section 149(1) of the Equality Act 2010. It is considered that the report has no relevance to South Cambridgeshire District Council's statutory equality duty to eliminate unlawful discrimination, advance equality of opportunity and foster good relation. An equality analysis is not needed.

BACKGROUND PAPERS

Where the Local Authorities (Executive Arrangements) (Meetings and Access to Information)
England) Regulations 2012 require documents to be open to inspection by members of the
Public, they must be available for inspection:

(a) at all reasonable hours at the offices of South Cambridgeshire District Council;
(b) on the Council's website; and
(c) In the case of documents to be available for inspection pursuant to regulation 15, on payment of a reasonable fee required by the Council by the person seeking to inspect the documents at the offices of South Cambridgeshire District Council.

REPORT AUTHOR: Peter Maddock – Head of Finance
E-mail: peter.maddock@scambs.gov.uk

This page is left blank intentionally.

South Cambridgeshire District Council

REPORT TO:	Audit & Corporate Governance Committee	24 March 2020
LEAD OFFICER:	Monitoring Officer	

Regulation of Investigatory Powers Act 2000 (RIPA) Amendments to Policy & 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 for the revised policy and procedure on the use of covert surveillance under RIPA 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) **AGREE** the recommendations for amendments to the Council's RIPA policy at Appendix A;
   (b) **NOTE** the information contained in the report about the Council's use of surveillance powers between September 2019 – February 2020.

Reasons for Recommendations

4. The Committee's terms of reference provide for it to receive quarterly updates on the Council's use of Regulation of Investigatory Powers Act 2000 (RIPA) powers and to review the RIPA policy on an annual basis and make amendments as necessary.

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 made further minor amendments as part of annual reviews in September 2013, September 2014, March 2017 and March 2019.

8. The Investigatory Powers Commissioner's Office is responsible for the inspection of public authorities with regard to compliance with RIPA. The Council was inspected on the 24th May 2018 and the report concluded that the policy, training and oversight regime was very good and made no recommendations.

9. The Director for Environmental Health (also acting Interim Chief Executive) was the Senior Responsible Officer for the RIPA process and his replacement needs to be appointed.

10. The Senior Responsible Officer (SRO) has overall oversight of RIPA within the Council and is responsible for reporting to Audit and Corporate Governance Committee on the use of RIPA powers. 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

11. There have been no changes to the legislation since the last revision of the policy in March 2019.

12. It is proposed that the Chief Executive takes on the responsibility of Senior Responsible Officer and that the Council's Monitoring Officer takes on the role of

RIPA Monitoring Officer. Throughout the policy, references to obligations on the Head of Legal Practice are now shared with the Monitoring Officer.

13. There are no other proposed changes at this time and a copy of the revised policy is at Appendix A. A track changes version has also been provided to Members of the Committee and is at Appendix B.

The Council's use of RIPA since September 2019

14. The information in the table below summarises the authorisations granted from June 2018 to March 2020.

	Directed surveillance	CHIS	Total	Purpose
September 2019 – March 2020	0	0	0	

Options

15. Members are required to approve the policy with or without amendments.

Implications

16. None.

Background Papers

None

Appendices

Appendix A: RIPA Policy
Appendix B: RIPA Policy showing tracked changes.

Report Author:

Rory McKenna – Monitoring Officer
Telephone: (01223) 457194

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

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-authorised 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-authorised 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 or 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
Juvenile Sources	1 Month
Renewal	12 Months
Juvenile Sources	1 Month

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 Executive Director (Corporate Services) 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 Office of Surveillance Commissioners, 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 information[1] 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.

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

[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."*

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 Office of Surveillance Commissioners

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 RIPA was overseen by the Office of Surveillance Commissioners (OSC). However, from 1 Sept 2017 oversight is now 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	Interim Assistant Director of Housing (HRA)
Rob Lewis	Operational Manager, Environmental Health & Licensing – Business Team
Senior Responsible Officer:	Liz Watts, Chief Executive
RIPA Monitoring Officer:	Rory McKenna, Monitoring Officer

This page is left blank intentionally.

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

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 ~~Executive Director (Corporate Services)~~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, ~~or~~ 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-authorised 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-authorised 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 or 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
Juvenile Sources	1 Month
Renewal	12 Months
Juvenile Sources	1 Month

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 Executive Director (Corporate Services) 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 Office of Surveillance Commissioners, 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 information[1] 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 Office of Surveillance Commissioners

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 RIPA was overseen by the Office of Surveillance Commissioners (OSC). However, from 1 Sept 2017 oversight is now 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	Interim Assistant Director of Housing (HRA)~~Neighbourhood Services Manager~~
Rob Lewis	~~_____~~Operational Manager, Environmental Health & Licensing – Business Team
Senior Responsible Officer:	Liz Watts~~Mike Hill~~, ~~Interim~~ Chief Executive
RIPA Monitoring Officer: ~~Legal Practice~~	Rory McKenna~~Tom Lewis~~, Monitoring Officer~~Head of~~

Formatted: Indent: Left: 0 cm, Hanging: 7.62 cm