

Audit & Standards Committee

Date: **18 April 2023**

Time: **4.00pm**

Venue: **Council Chamber, Brighton Town Hall**

Councillors: Wilkinson (Chair), Hugh-Jones (Group Spokesperson), Atkinson, Meadows, Shanks, Simson, West and Yates

Independent Persons: David Bradly and David Gill

Contact: **John Peel**
Democratic Services Officer
01273 291058
john.peel@brighton-hove.gov.uk

Agendas and minutes are published on the council's website www.brighton-hove.gov.uk. Agendas are available to view five working days prior to the meeting date.

Electronic agendas can also be accessed through our meetings app available through ModernGov: [iOS/Windows/Android](#)

This agenda and all accompanying reports are printed on recycled paper

Date of Publication – Thursday, 6 April 2023

AGENDA

Part One

Page

43 PROCEDURAL BUSINESS

- (a) **Declarations of Substitutes:** Where councillors are unable to attend a meeting, a substitute Member from the same political group may attend, speak and vote in their place for that meeting.
- (b) **Declarations of Interest:**
 - (a) Disclosable pecuniary interests;
 - (b) Any other interests required to be registered under the local code;
 - (c) Any other general interest as a result of which a decision on the matter might reasonably be regarded as affecting you or a partner more than a majority of other people or businesses in the ward/s affected by the decision.

In each case, you need to declare

- (i) the item on the agenda the interest relates to;
- (ii) the nature of the interest; and
- (iii) whether it is a disclosable pecuniary interest or some other interest.

If unsure, Members should seek advice from the committee lawyer or administrator preferably before the meeting.

- (c) **Exclusion of Press and Public:** To consider whether, in view of the nature of the business to be transacted or the nature of the proceedings, the press and public should be excluded from the meeting when any of the following items are under consideration.

Note: Any item appearing in Part Two of the agenda states in its heading the category under which the information disclosed in the report is exempt from disclosure and therefore not available to the press and public. A list and description of the exempt categories is available for public inspection at Brighton and Hove Town Halls and on-line in the Constitution at part 7.1.

44 MINUTES

To Follow

To consider the minutes of the previous meeting

Contact Officer: John Peel

Tel: 01273 291058

45 CHAIR'S COMMUNICATIONS

46 CALL OVER

- (a) Items 49 - 52 will be read out at the meeting and Members invited to reserve the items for consideration.
- (b) Those items not reserved will be taken as having been received and the reports' recommendations agreed.

47 PUBLIC INVOLVEMENT

To consider the following matters raised by members of the public:

- (a) **Petitions:** to receive any petitions presented to the full council or at the meeting itself;
- (b) **Written Questions:** to receive any questions submitted by the due date of 12 noon on the 12 April 2023;
- (c) **Deputations:** to receive any deputations submitted by the due date of 12 noon on the 12 April 2023.

48 MEMBER INVOLVEMENT

To consider the following matters raised by councillors:

- (a) **Petitions:** to receive any petitions submitted to the full Council or at the meeting itself;
- (b) **Written Questions:** to consider any written questions;
- (c) **Letters:** to consider any letters;
- (d) **Notices of Motion:** to consider any Notices of Motion referred from Council or submitted directly to the Committee.

49 INTERNAL AUDIT AND COUNTER FRAUD QUARTER 3 PROGRESS REPORT 2022/23 7 - 22

Contact Officer: Carolyn Sheehan
Ward Affected: All Wards

50 INTERNAL AUDIT STRATEGY AND ANNUAL AUDIT PLAN 2023-24 23 - 48

Contact Officer: Carolyn Sheehan
Ward Affected: All Wards

51 ANNUAL SURVEILLANCE REPORT 2022 49 - 90

Contact Officer: Jo Player *Tel: 01273 292488*
Ward Affected: All Wards

52 STANDARDS UPDATE

91 - 102

Contact Officer: Victoria Simpson
Ward Affected: All Wards

Tel: 01273 294687

53 ITEMS REFERRED FOR COUNCIL

To consider items to be submitted to the 20 July 2023 Council meeting for information.

In accordance with Procedure Rule 24.3a, the Committee may determine that any item is to be included in its report to Council. In addition, any Group may specify one further item to be included by notifying the Chief Executive no later than 10am on the eighth working day before the Council meeting at which the report is to be made, or if the Committee meeting take place after this deadline, immediately at the conclusion of the Committee meeting

54 ITEMS FOR THE NEXT MEETING

The City Council actively welcomes members of the public and the press to attend its meetings and holds as many of its meetings as possible in public. Provision is also made on the agendas for public questions to committees and details of how questions can be raised can be found on the website and/or on agendas for the meetings.

The closing date for receipt of public questions and deputations for the next meeting is 12 noon on the fourth working day before the meeting.

Meeting papers can be provided, on request, in large print, in Braille, on audio tape or on disc, or translated into any other language as requested.

Infra-red hearing aids are available for use during the meeting. If you require any further information or assistance, please contact the receptionist on arrival.

Further information

For further details and general enquiries about this meeting contact John Peel, (01273 291058, email john.peel@brighton-hove.gov.uk) or email democratic.services@brighton-hove.gov.uk

Webcasting notice

This meeting may be filmed for live or subsequent broadcast via the Council's website. At the start of the meeting the Chair will confirm if all or part of the meeting is being filmed. You should be aware that the Council is a Data Controller under the Data Protection Act 1998. Data collected during this web cast will be retained in accordance with the Council's published policy.

Therefore, by entering the meeting room and using the seats in the chamber you are deemed to be consenting to being filmed and to the possible use of those images and sound recordings for the purpose of web casting and/or Member training. If members of the public do not wish to have their image captured, they should sit in the public gallery area.

Access notice

The Public Gallery is situated on the first floor of the Town Hall and is limited in size but does have 2 spaces designated for wheelchair users. The lift cannot be used in an emergency. Evac Chairs are available for self-transfer and you are requested to inform Reception prior to going up to the Public Gallery. For your own safety please do not go beyond the Ground Floor if you are unable to use the stairs.

Please inform staff on Reception of this affects you so that you can be directed to the Council Chamber where you can watch the meeting or if you need to take part in the proceedings e.g. because you have submitted a public question.**Fire & emergency**

evacuation procedure

If the fire alarm sounds continuously, or if you are instructed to do so, you must leave the building by the nearest available exit. You will be directed to the nearest exit by council staff. It is vital that you follow their instructions:

- You should proceed calmly; do not run and do not use the lifts;
- Do not stop to collect personal belongings;
- Once you are outside, please do not wait immediately next to the building, but move some distance away and await further instructions; and
- Do not re-enter the building until told that it is safe to do so

Brighton & Hove City Council

Audit & Standards Committee

Agenda Item 49

Subject: Internal Audit and Counter Fraud Quarter 3 Progress Report 2022/23

Date of meeting: 18th April 2023

Report of: Executive Director Governance, People and Resources

Contact Officer: Carolyn Sheehan (Audit Manager)
Tel: 07795 335692
Email: carolyn.sheehan@brighton-hove.gov.uk

Russell Banks (Chief Internal Auditor)
Tel: 07824 362739
Email: russell.banks@eastsussex.gov.uk

Ward(s) affected: All

For general release

1. Purpose of the report and policy context

1.1 The purpose of this report is to provide Members with an update on all internal audit and counter fraud activity completed during quarter 3 (2022/23), including a summary of all key audit findings. The report also includes an update on the performance of the Internal Audit Service during the period.

2. Recommendations

2.1 That the Committee note the report.

3. Context and background information

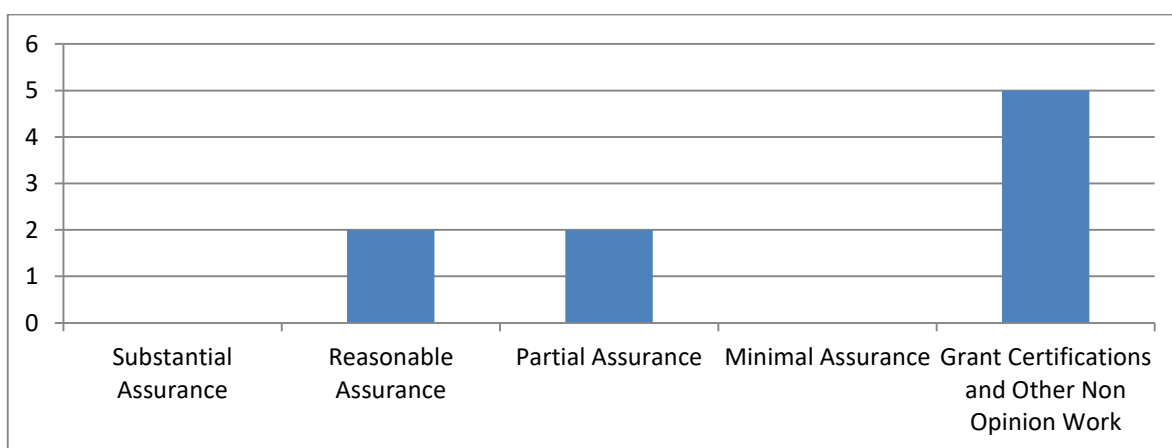
3.1 The current annual plan for internal audit is contained within the Internal Audit Strategy and Annual Plan 2022/23 which was approved by the Audit and Standards Committee on 19 April 2022.

3.2 This report provides an update on progress against that plan and includes a narrative summary of all audits that have been finalised during the quarter as well as details of counter fraud and other activity delivered during the period.

4. Analysis and consideration of alternative options

4.1 Full details of both the audit and non-audit work delivered during quarter 3 are detailed in Appendix 1, together with our progress against our performance targets.

- 4.2 The opinions given are summarised in the chart below. There were two partial assurance and two reasonable assurance reports finalised during the quarter. In addition, there were three grant certifications, which have been included under the category “Grant Certifications and Non-Opinion work”.
- 4.3 Due to the timing of the end of this quarter and the availability of officers to deal with requests for information, some delays have been experienced in finalising audit reports. It should, however, be noted that at the end of quarter 3, five audit reports had been issued as draft that will be reported within the quarter 4 progress report.
- 4.4 Internal Audit resources have also been utilised in providing ongoing advice and support to the replacement of the back-office systems (ERP) and the housing repairs works management system programmes.



5. Community engagement and consultation

- 5.1 The annual report has been informed by internal audit and counter fraud work carried out during the year which has included extensive engagement with officers and members.

6. Conclusion

- 6.1 The Committee is asked to note the report.

7. Financial implications

- 7.1 It is expected that the Internal Audit Annual Plan 2022/23 will be delivered within existing budgetary resources. Progress against the plan and action taken in line with actions support the robustness and resilience of the council’s practices and procedures in support of the council’s overall financial position.

Name of finance officer consulted: James Hengeveld Date consulted 28/03/2023

8. Legal implications

- 8.1 The Accounts and Audit Regulations 2015 require the Council to undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account Public Sector Internal Audit Standards. It is an important part of the Audit and Standards Committee's role to review the level of work completed and planned by the Council's internal audit function.

Name of lawyer consulted: Victoria Simpson Date consulted 21.3.23

9. Equalities implications

- 9.1 There are no direct equalities implications.

10. Sustainability implications

- 10.1 There are no sustainability implications.

11. Other Implications

- 11.1 There are no other implications.

Supporting Documentation

1. Appendices

1. Internal Audit and Counter Fraud Quarter 3 Progress Report

Internal Audit and Counter Fraud

Quarter 3 Progress Report 2022/23

CONTENTS

1. Summary of Completed Audits
2. Counter Fraud and Investigation Activities
3. Action Tracking
4. Amendments to the Audit Plan
5. Internal Audit Performance

1. Summary of Completed Audits

Adult Social Care Financial Assessments - Partial Assurance

1.1 As part of the Care Act a financial assessment must be undertaken to ascertain whether service users are able to make a contribution towards the cost of their care and this determines the extent of financial support that will be provided by the Council. These financial assessments are completed by the Council with the service user.

1.2 The purpose of this audit was to provide independent assurance on the adequacy of the controls in place to manage financial assessments and ensure that they are accurate, completed in a timely manner and client contributions are raised for payment and correctly recorded in financial systems.

1.3 In providing an audit opinion of Partial Assurance, we found that further improvements are required to ensure financial assessments processes and controls are robust. These include the following:

- Agreeing a process to ensure that the Council can manage reviews of care assessments for non-residential clients, that complies with the Care Act and matches available resources;
- Improving regularity of updating financial assessments so that they reflect any significant change in circumstances for service users;
- Improving the oversight of assessments to identify any errors, omissions or miscalculations;
- Retaining evidence of monthly reconciliations;
- Improving management information to monitor performance and workloads;
- Establishing and publishing service standards; and
- Providing assessment teams with guidance manuals detailing the process.

1.4 Following the audit, we formally agreed 8 actions with management to address the issues highlighted in the report, including:

- An options paper will be written to consider the cost benefit risk analysis of undertaking non-residential care assessments;
- Quality assurance processes will be reviewed;
- Service plan and performance indicators will be reviewed and developed to include implementation, reporting and responsibility arrangements;
- Process and deadline guidance for issuing notification letters will be included in guidance;
- Guidance notes will be developed and made available to the assessment teams;
- Monthly reconciliations will be retained and will be reviewed and approved by a second officer;
- Signature and initial of the visiting officer will be added to the financial assessment form, and;
- Communication to service users will include a reminder to inform the Council of any changes in their financial circumstances.

1.5 For all partial assurance audits, we undertake a formal follow-up review to that the agreed actions are implemented and have addressed the issues raised.

School Attendance – Reasonable Assurance

1.6 Legal duties for school attendance are set out in the Education Act 1996 and the Education (Pupil Registration) Regulations 2006. New non-statutory guidance was issued in May 2022 and is expected to become statutory. The changes include new statutory expectations for local authority attendance services. During and following on from the pandemic, there has been widespread concern over school attendance and welfare of pupils.

1.7 During the autumn 2021 and spring 2022 terms, Brighton and Hove schools had an absence rate of 8.2% compared to 7.4% for both the South East and the rest of England. Attendance levels both nationally and locally have been lower than pre-pandemic, though there is a gradual upward trend.

1.8 The purpose of this audit was to provide assurance that controls are in place and are operating as expected. These include that a school attendance strategy (including those with elective home education) is in place and is effective, policies and procedures are set in accordance with national guidance, reviewed regularly and disseminated, attendance data is collected, analysed and used to identify and support vulnerable pupils.

1.9 Our review found that the service has increased their scrutiny on school attendance since the start of the Covid-19 pandemic. A Hidden Children Officer post has been created and there is evidence of cross service working to identify young people who are not receiving a full-time education.

1.10 The expected regulatory changes have been evaluated by the service to ensure that they can be met and there is a commitment to discuss these further with Ofsted to ensure that the Council has fully understood new guidance and operates in compliance.

1.11 Whilst we were able to provide Reasonable Assurance, some opportunities for further improvement were found during the audit, these included:

- Ensuring that policy and procedure documents are updated, recorded as approved and published as final documents;
- That all relevant policy, procedure and guidance documents are communicated to schools and can be accessed through BEEM;
- Improving the quality and timeliness of data provided by schools and;
- Improving data analysis, particularly around movements in the data.

1.12 Appropriate actions to address all of the above areas have been agreed with management, as part of a formal action plan.

Public Sector Bodies (Website and Mobile Applications) Accessibility Regulations – Reasonable Assurance

1.13 The Public Sector Bodies (website and mobile applications) Accessibility Regulations came into force in September 2018. Failure to comply with these regulations would constitute a breach of the 2010 Equality Act. Public Sector Bodies must make their websites and mobile applications more accessible by making them ‘perceivable, operable, understandable and robust’.

1.14 This audit is a follow-up review of a previous audit report issued December 2021 concluding Partial Assurance. The objective of this audit was to follow-up on the actions agreed from the previous audit and to provide assurance that actions have been implemented and key controls are in place and operating effectively.

1.15 We found that work to ensure compliance continues to progress. A Senior Responsible Officer has been appointed to a project overseeing these regulations. Further accessibility guidance has been developed and provided by IT&D for staff considering using new applications.

1.16 Following the audit, we were able to revise the opinion to Reasonable Assurance. Of the previous four actions, we found that three had been implemented.

1.17 There is still a concern that there may not be sufficient resources to maintain compliance without a dedicated project manager and an action to address this has been agreed.

Schools

1.18 We have a standard audit programme in place for all school audits, with the scope of our work designed to provide assurance over key controls operating within schools. The objectives of our work are to ensure that:

- Governance structures are in place and operate to ensure there was independent oversight and challenge by the Governing Body;
- Decision making is transparent, well documented, and free from bias;
- The school is able to operate within its budget through effective financial planning;
- Unauthorised or inappropriate people do not have access to pupils, systems, or the site;
- Staff are paid in accordance with the schools pay policy;
- Expenditure is controlled and funds used for an educational purpose;
- All unofficial funds are held securely and used in accordance with their agreed purpose; and,
- Security arrangements keep data and assets secure and are in accordance with data protection legislation.

1.19 At the time of writing, school audits continue to be undertaken under remote working arrangements.

1.20 One school audit was finalised in quarter 3 and another two are in progress in Q4. The table below summarises our findings together with the final level of assurance given.

Name of School	Audit Opinion	Areas Requiring Improvement
Queens Park Primary School	Partial Assurance	<ul style="list-style-type: none"> • Scrutiny and challenge by the Governing Body regarding financial management should be recorded in minutes of meetings. • Ensure that staff involved in managing the school finances are involved in strategic financial planning and budget monitoring reporting. • The school should ensure that the Governing Body receives financial reports to aid their role of providing financial oversight. • School Improvement and Development Plan should be fully costed and included in the school budget. • The staffing structure needs to be periodically reviewed to ensure it meets the needs of the school. • The contracts register needs to be updated with key details. • Purchase orders should be raised and approved prior to staff placing orders for goods, works or services with suppliers.

1.21 We aim to undertake follow-up audits at all schools with Minimal and most schools with Partial Assurance opinions.

1.22 The core financial role of the LA is to set and monitor a local framework, including provision of budgetary information, provision of a financial oversight and ultimately intervening where schools are causing financial concerns. Schools (the governing body and the Headteacher) are required to manage their delegated budget effectively ensuring the school meets all its statutory obligations, and through the Headteacher comply with the LA’s Financial Regulations and Standing Orders.

Grant Certifications and Non-Opinion Work

EU Grant – Solarise (Claim 9)

1.23 This is a European Union (EU) Interreg project that requires grant certification. The full title of the project is ‘Solar Adoption Rise in the 2 Seas’. The total value of the project is approximately EUR

320,686, with 60% funded by the EU. The funding has been used to support solar innovation projects at three council housing sites. This was the final claim on this project

1.24 No significant issues were identified in the grant certification.

EU Grant – Blueprint for a Circular Economy (Claim 5 and on the spot check)

1.25 This is a European Union (EU) Interreg project that requires grant certification. The total value of the project is EUR 402,322, with 69% funded by the EU. The funding has been used to grow and embed circular principles into the wider community by supporting the growth of circular business models and practices across existing and new emerging social enterprises based in the City.

1.26 During the life of the project there is a requirement for an ‘on the spot’ check of the progress of the programme and expenditure against the grant.

1.27 No significant issues were identified in the grant certification.

DfT Grant – Local Transport Capital Funding

1.28 This is a ringfenced grant available to local authorities from the Department of Transport (DfT) to provide capital funding towards local transport. The amount of £4.902m was provided to the Council for 2021-22. The grant expenditure requires certification by Internal Audit.

1.29 We note that there is an underspend of £2.438m that has been carried forward to 2022-23 capital programme to meet planned and re-profiled local transport capital expenditure.

1.30 No significant issues were identified in the grant certification.

Enterprise Resource Planning (ERP) Programme

1.31 In July 2022, Policy and Resources Committee agreed to commence procurement of a corporate Enterprise Resource Planning (ERP) system to replace the current Finance and HR/Payroll systems which have been used by the Council for 16 and 12 years respectively.

1.32 Internal Audit have been attending Programme Board meetings to provide independent and objective ad-hoc advice, guidance and challenge.

1.33 A package of deliverable work is being agreed with the Board, designed to provide the Board with assurance when making critical decisions, including the provision of assurance over the design of the control environment within the new system.

1.34 We will continue to update the Committee on our work as the programme progresses.

Housing Repairs Works Management System Replacement Programme

1.35 It was agreed by the Housing & New Homes Committee and the Policy, Resources & Growth Committee in 2018 to bring the responsive repairs and empty property refurbishments service in house on 1st April 2020. This service includes emergency repairs, and the procurement of suppliers to provide specialist works, where the in-house team do not have the skills to complete them.

1.36 We have agreed, to attend programme board meetings and provide ad-hoc support, challenge and guidance as appropriate to support the procurement of a Works Management System that works alongside and interfaces with the NEC Housing Management System.

1.37 Whilst no specific internal audit work has yet been required of the new system, internal audit work will be provided to support the programme as and when appropriate, in agreement with the Board.

1.38 A follow-up review of the 2020-21 Housing Repairs audit is also scheduled for quarter 4.

2. Proactive Counter Fraud Work

Counter Fraud Activity

2.1 Internal Audit have been liaising with the relevant services to ensure that the data extracts for the 2022 NFI Single Person Discount exercise are uploaded. The team continue to monitor intel alerts and share information with relevant services when appropriate. A fraud awareness bulletin, focusing on emerging fraud risks, was produced and published on the intranet as part of International Fraud Awareness week in November 2022.

Summary of Completed Investigations

2.2 There was one completed investigation to report on for this quarter. Advice was also provided to service management/Human Resources in cases referred to Internal Audit.

Misconduct

2.3 Internal Audit investigated an allegation that a member of staff was letting their Council property via AirBnB and they had not realised that this was a breach of their Council tenancy. The advert was subsequently removed, and the member of staff was issued a letter of expectation.

Advice and Support

2.4 Advice was provided to the Revenue and Benefits Teams following an allegation that a member of staff received an exemption on her council tax account where there was a question over eligibility. In addition the team continue to provide advice to the Adult Social Care team in relation to potential false statements and misappropriation of funds.

Housing Tenancy & Local Taxation

2.5 A key focus area remains housing tenancy fraud and Local Taxation. The CIPFA Fraud & Corruption Tracker continues to place Housing Fraud as the largest threat to local authorities, and the volume of succession and application fraud in particular, has seen significant increases in recent years. Unlike other sectors, tackling this type of fraud is, however, not just about financial savings but the social benefits to the community.

2.6 In recognition of the continued threat facing the city, increased resource has been committed by the Executive Director Housing, Neighbourhoods and Communities. This has resulted in an additional post funded from the Housing Revenue Account which is currently being recruited to. This additional role will provide resource to enhance the reactive investigations whilst also providing capacity to deliver proactive and preventative aspects to enhance the tenancy fraud work.

3. Action Tracking

3.1 All high priority actions agreed with management as part of individual audit reviews are subject to action tracking. When high priority actions become due, we seek confirmation from Service management that actions have been implemented. As at the end of quarter 3, 95% of high priority actions due have been confirmed as implemented by management.

3.2 There was one high priority action which was overdue. Details are provided below.

Details of Audit Issue	Dir.	Due date	Revised date	Agreed Action
Direct Payments - Annual Client Reviews. We found that 46% of annual reviews for direct payments were overdue at October 2021.	HASC	31.08.22	31.12.22	Staff will target overdue reviews.

3.3 A follow-up review of the Direct Payments audit is scheduled for quarter 4 where we will seek to assess the level of progress made against the above action.

3.4 A number of high priority actions have had their implementation deadlines extended, in agreement with management. Where the revised deadlines are not met, these will be reported to the next meeting of the Audit & Standards Committee.

4. Amendments to the Audit Plan

4.1 In accordance with proper professional practice, the Internal Audit plan for the year has been kept under regular review to ensure that the service continues to focus its resources in the highest priority areas based on an assessment of risk. Through discussions with management the following audits have been added to the audit plan this quarter:

Planned Audit	Rationale for Addition
Adult Social Care - Service Agreements in Brokerage	This audit was included at the request of service leads and will replace the planned audit on residential care procurement.
Budget Management - Savings Targets	This audit has been added to the plan in response to the challenging financial situation and proposed savings. This audit will review the impact of savings on the control framework.
CIPFA Financial Management Code	This review has been added to the plan at the request of the S151 officer. It will review the completed self - assessment to provide further assurance, especially in relation to the supporting evidence.

4.2 In order to allow these additional audits to take place, the following audits have been removed or deferred from the audit plan and, where appropriate, will be considered for inclusion in future audit plans as part of the overall risk assessment completed during the annual audit planning process. These changes have been made on the basis of risk prioritisation and/or as a result of developments within the service areas concerned requiring a rescheduling of audits:

- Surveillance Cameras
- Kofax IT Application
- Residential Care Procurement

5. Internal Audit Performance

5.1 In addition to the annual assessment of internal audit effectiveness against Public Sector Internal Audit Standards (PSIAS), the performance of the service is monitored on an ongoing basis against a set of agreed key performance indicators as set out in the following table:

Aspect of Service	Orbis IA Performance Indicator	Target	RAG Score	Actual Performance
Quality	Annual Audit Plan agreed by Audit Committee	By end April	G	2022/23 Audit Plan approved by Audit & Standards Committee on 19 April 2022
	Annual Audit Report and Opinion	By end July	G	2021/22 Annual Report and Opinion approved by Audit Committee on 28 June 2022
	Customer Satisfaction Levels	90% satisfied	G	100%
Productivity and Process Efficiency	Audit Plan – completion to draft report stage	68%	G	70%
Compliance with Professional Standards	Public Sector Internal Audit Standards	Conforms	G	<p>Dec 2022 - External Quality Assurance completed by the Institute of Internal Auditors (IIA). Orbis Internal Audit assessed as achieving the highest level of conformance available against professional standards with no areas of non-compliance identified, and therefore no formal recommendations for improvement arising. In summary the service was assessed as:</p> <ul style="list-style-type: none"> •Excellent in: Reflection of the Standards, Focus on performance, risk and adding value •Good in: Operating with efficiency, Quality Assurance and Improvement Programme •Satisfactory in: Coordinating and maximising assurance
	Relevant legislation such as the Police and Criminal Evidence Act, Criminal Procedures and Investigations Act	Conforms	G	No evidence of non-compliance identified

Aspect of Service	Orbis IA Performance Indicator	Target	RAG Score	Actual Performance
Outcome and degree of influence	Implementation of management actions agreed in response to audit findings	95% for high priority agreed actions	G	95% for high priority agreed actions (see above)
Our staff	Professionally Qualified/Accredited (Includes part-qualified staff and those undertaking professional training)	80%	G	90%

Audit Opinions and Definitions

Opinion	Definition
Substantial Assurance	Controls are in place and are operating as expected to manage key risks to the achievement of system or service objectives.
Reasonable Assurance	Most controls are in place and are operating as expected to manage key risks to the achievement of system or service objectives.
Partial Assurance	There are weaknesses in the system of control and/or the level of non-compliance is such as to put the achievement of the system or service objectives at risk.
Minimal Assurance	Controls are generally weak or non-existent, leaving the system open to the risk of significant error or fraud. There is a high risk to the ability of the system/service to meet its objectives.

Brighton & Hove City Council

Audit and Standards Committee

Agenda Item 51

Subject: Internal Audit Strategy and Annual Audit Plan 2023/24

Date of meeting: 18th April 2023

Report of: Executive Director, Governance People and Resources

Contact Officer: Carolyn Sheehan (Audit Manager)
Tel: 07795 335692
Email: carolyn.sheehan@brighton-hove.gov.uk

Russell Banks (Chief Internal Auditor)
Tel: 07824 362739
Email: russell.banks@eastsussex.gov.uk

Ward(s) affected: All

1. Purpose of the report and policy context

- 1.1 The purpose of this report is to provide Members with the Internal Audit Strategy and Annual Audit Plan for 2023/24.
- 1.2 This includes the proposed programme of internal audit and counter-fraud work for the coming year (Appendix 1 and 2).
- 1.3 It also includes the Internal Audit Charter which sets out the purpose, authority, and responsibilities of the Internal Audit function (Appendix 3).

2. Recommendations

- 2.1 That the Committee approves the Internal Audit Strategy and Annual Audit Plan for 2023/24 and notes the Internal Audit Charter.

3. Context and background information

- 3.1 Regulation 5 of The Accounts and Audit Regulations 2015 requires the Council to 'undertake an effective internal audit to evaluate the effectiveness of its risk management, control, and governance processes'. In addition, the Public Sector Internal Audit Standards (PSIAS) require "senior management" and "the board" to approve internal audit activity's plans and resource requirements and the Internal Audit Charter.
- 3.2 For Brighton & Hove, "senior management" is the Executive Leadership Team (ELT), and the "board" is the Audit & Standards Committee.
- 3.3 A copy of the Internal Audit Strategy and Annual Audit Plan for 2023/24 is included as Appendix 1 and 2.

- 3.4 The development of the annual plan involves extensive consultation with key stakeholders and horizon scanning is undertaken to ensure audit activity is proactive and future focussed. For 2023/24, the plan composes 1815 days, including 440 days funded directly from the Housing Revenue Account to support Housing related activities.
- 3.5 The strategy, which accompanies the schedule of audits, details the priorities for delivering an effective internal audit and counter fraud service together with details of the quality assurance and performance management arrangements for the coming year.
- 3.6 The Internal Audit Charter (Appendix 3) describes the purpose, authority and responsibilities on internal audit, its statutory basis and the standards which underpin best practice.

4. Analysis and consideration of alternative options

- 4.1 The 2023/24 audit plan will again be delivered in partnership with our colleagues from East Sussex County Council and Surrey County Council as part of Orbis Internal Audit. The service will be delivered predominantly by a sovereign team of staff based at Brighton & Hove City Council supplemented by two specialist teams (ICT and Corporate Fraud) who will undertake audit work across the Orbis partnership. There are also resources in place to allow for the delivery external IT and other specialist audits if required.

5. Community engagement and consultation

- 5.1 The process of compiling the Internal Audit plan has involved substantial consultations, including with members of ELT, heads of service and other senior management staff.

6. Conclusion

- 6.1 The Internal Audit Strategy and Annual Audit Plan, attached at Appendix 1, sets out proposals for maintaining an adequate and effective system of internal audit for 2023/24.

7. Financial implications

- 7.1 It is expected that the 2023/24 Internal Audit plan will be delivered within the proposed budgetary resources.
- 7.2 The strategy, audit plan and action taken in response to internal audit findings support the robustness and resilience of the Council's practices and procedures and support delivering of the Council's overall objectives.

Name of finance officer consulted: James Hengeveld Date consulted
28/03/2023

8. Legal implications

- 8.1 This report sets out the Council's plan for complying with Regulation 5 of the Accounts and Audit Regulations 2015 which requires the Council to 'undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes.' It is within the delegated powers of the Council's Audit and Standards Committee to approve the Plan.

Name of lawyer consulted: Victoria Simpson Date consulted 27/03/23

9. Equalities implications

- 9.1 There are no direct equalities implications.

10. Sustainability implications

- 10.1 There are no sustainability implications.

11. Other Implications [delete any or all that are not applicable]

- 11.1 There are no other implications.

Supporting Documentation

Appendices

1. Internal Audit Strategy and Annual Audit Plan 2023/24
2. Detailed Annual Audit Plan 2023/24
3. Internal Audit Charter

Internal Audit Strategy and Annual Audit Plan 2023-2024

1. Role of Internal Audit

1.1 The full role and scope of the Council’s Internal Audit Service is set out within the Internal Audit Charter and Terms of Reference (attached as Appendix 3).

1.2 The mission of Internal Audit, as defined by the Chartered Institute of Internal Auditors (CIIA), is to enhance and protect organisational value by providing risk-based and objective assurance, advice and insight. Internal Audit is defined as *“an independent, objective assurance and consulting activity designed to add value and improve an organisation’s operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.”*

1.3 The organisation’s response to internal audit activity should lead to a strengthening of the control environment, thus contributing to the overall achievement of organisational objectives.

2. Risk Assessment and Audit Planning

2.1 Brighton and Hove City Council’s Internal Audit Strategy and Annual Audit Plan is updated annually and is based on a number of factors, especially management’s assessment of risk (including that set out within the strategic and departmental risk registers) and our own risk assessment of the Council’s major systems and other auditable areas. This allows us to prioritise those areas to be included within the audit plan on the basis of risk.

2.2 The annual planning process has once again involved consultation with a range of stakeholders to ensure that their views on risks and current issues, within individual departments and corporately, are identified and considered. In order to ensure that the most effective use is made of available resources, to avoid duplication and to minimise service disruption, efforts will continue to be made to identify, and where possible, rely upon, other sources of assurance available. The following diagram sets out the various sources of information used to inform our 2023/24 audit planning process:



APPENDIX 1

2.3 Through this process, we have been able to identify key areas for audit activity in 2023/24, including strategic risks and issues, key priority projects and programmes, priority service reviews, key financial systems, and grant claims. The remainder of the direct audit days are earmarked as emerging risks/contingency which enables us to respond to the rapidly changing risk landscape across the Authority.

2.4 In order to ensure audit and assurance activity is properly focussed on supporting the delivery of the Council's priorities, the audit plan has taken into account the key corporate priority outcomes of the Council as set out within the Council Plan. These are:

- City to call home;
- City working for all;
- Stronger city;
- Growing and learning city;
- Sustainable city; and
- Healthy and caring city.

2.6 In producing the audit plan (which is set out in Appendix 2 to this report) the following key principles continue to be applied:

- Key financial systems are subject to a cyclical programme of audits covering, as a minimum, compliance against key controls;
- Previous reviews which resulted in 'minimal assurance' or 'partial assurance' audit opinions will be subject to a specific follow-up review to assess the effective implementation by management of agreed actions; and
- Any reviews which we were unable to deliver during the previous financial year will be considered once again as part of our audit planning risk assessment, and prioritised as appropriate.

2.7 It should be noted that the 2023/24 audit plan is more flexible than ever before. This is due to the changing nature of the risk landscape across the public sector. Given the likelihood of the plan needing to flex within the year ahead, we have identified at the end of Appendix 2 a number of additional assignments that may, on a risk prioritised basis, be drawn into our workload if planned audits are postponed or cancelled.

2.8 In addition, formal action tracking arrangements are in place to monitor the implementation by management of all individual high-priority agreed actions, with the results of this work reported to ELT and the Audit and Standards Committee on a quarterly basis.

2.9 Since 2018, Brighton and Hove City Council, East Sussex County Council and Surrey County Council have been working together to establish and develop the Orbis Internal Audit Partnership. In doing this, we are able to deliver high quality and cost effective assurance services to each partner, drawing upon the wide range of skills and experience from across the various teams. The size and scale of the partnership has also enabled us to invest in specialist IT Audit and Counter Fraud services, to the benefit of each partner council and external fee paying client.

3. Key Issues

3.1 In times of significant transformation, organisations must both manage change effectively and ensure that core controls remain in place. In order to respond to the continued reduction in financial resources and the increased demand for services, the Council needs to consider some radical changes to its service offer in many areas.

3.2 Internal Audit must therefore be in a position to give an opinion and assurance that covers the control environment in relation to both existing systems and these new developments. It is also essential that this work is undertaken in a flexible and supportive manner, in conjunction with management, to ensure that both risks and opportunities are properly considered. During 2023/24, a number of major organisational initiatives and/or risks areas will feature within the audit plan, with the intention that Internal Audit is able to provide proactive advice, support and assurance as these programmes progress. These include:

- Replacement of Back Office Systems
- Housing repairs works management system and supply chain

3.3 As explained previously, in recognition of current uncertainties and that in some cases, sufficient information regarding the full extent of future changes and associated risks may not yet be known, the 2023/24 audit plan will, as in previous years, include a proportion of time classified as 'Emerging Risks'. This approach has been adopted to enable Internal Audit to react appropriately throughout the year as new risks materialise and to ensure that expertise in governance, risk and internal control can be utilised early in the change process.

3.4 In view of the above, Internal Audit will continue to work closely with senior management and Members throughout the year to identify any new risks and to agree how and where audit resources can be utilised to best effect.

3.5 Other priority areas identified for inclusion within the audit plan include:

- Complex Care Placements for Children
- Transition from Children to Adults Services
- Early Help Services
- Housing allocations
- Housing Neighbourhoods and Communities – planned and major works
- Health and Adult Social Care Debt Management and Recovery
- Payroll
- Off payroll payments

3.6 The results of all audit work undertaken will be summarised within quarterly update reports to ELT and the Audit and Standards Committee, along with any common themes and findings arising from our work.

4. Counter Fraud

4.1 Managing the risk of fraud and corruption is the responsibility of management. Internal Audit will, however, be alert in all its work to risks and exposures that could allow fraud or corruption and will investigate allegations of fraud and corruption in line with the Council's Anti-Fraud and Corruption Strategy.

4.2 The Chief Internal Auditor should be informed of all suspected or detected fraud, corruption or irregularity in order to consider the adequacy of the relevant controls and evaluate the implication for their opinion on the control environment.

4.3 In addition, Internal Audit will promote an anti-fraud and corruption culture within the Council to aid the prevention and detection of fraud. Through the work of the Counter Fraud Team, Internal Audit will maintain a fraud risk assessment and deliver a programme of proactive and reactive counter fraud services to help ensure that the Council continues to protect its services from fraud loss. This will include leading on the National Fraud Initiative data matching exercise on behalf of the Council.

5. Matching Audit Needs to Resources

5.1 The overall aim of the Internal Audit Strategy is to allocate available internal audit resources so as to focus on the highest risk areas and to enable an annual opinion to be given on the adequacy and effectiveness of the Council's governance, risk and control framework.

5.2 In addition to this, resources have been allocated to the external bodies for whom Orbis Internal Audit also provide internal audit services, at an appropriate charge. These include Horsham District Council, Elmbridge District Council, East Sussex Fire Authority and South Downs National Park.

5.3 Internal audit activities will be delivered by a range of staff from across the Orbis Internal Audit Service, maximising the value from a wide range of skills and experience available. In the small number of instances where sufficient expertise is not available from within the team, mainly in highly technical or specialist areas, the option of engaging externally provided specialist resources will continue to be considered.

5.4 The following table summarises the level of audit resources expected to be available for the Council in 2023/24 (expressed in days), compared to the equivalent number of planned days in previous years. As can be seen, the overall level of resource has been increased for 2023/24 following an increase in funding from HNC to further support housing tenancy activities. Ultimately, this level of resource continues to be considered sufficient to allow Internal Audit to deliver its risk-based plan in accordance with professional standards¹ and to enable the Chief Internal Auditor to provide his annual audit opinion, albeit with this remaining dependent on our continued ability to recruit and retain high calibre staff (see Section & below).

¹ Public Sector Internal Audit Standards

Table 1: Annual Internal Audit Plan – Plan Days

	2020/21	2021/22	2022/23	2023/24
Plan Days	1540*	1660*	1660*	1815*

*includes the provision of additional audit days to deliver housing tenancy fraud work for HNC

6. Audit Approach

6.1 The approach of Internal Audit is to use risk-based reviews, supplemented in some areas by the use of compliance audits and themed reviews. All audits have regard to management’s arrangements for:

- Achievement of the organisation’s objectives;
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations and programmes;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures and contracts.

6.2 In addition to these audits, and the advice on controls given on specific development areas which are separately identified within the plan, there are a number of generic areas where there are increasing demands upon Internal Audit, some of which cannot be planned in advance. For this reason, time is built into the plan to cover the following:

- Contingency – an allowance of days to provide capacity for unplanned work, including special audits and management investigations. This contingency also allows for the completion of work in progress from the 2022/23 plan;
- Advice, Management, Liaison and Planning - an allowance to cover provision of ad hoc advice on risk, audit and control issues, audit planning and annual reporting, ongoing liaison with service management and Members, and audit management time in support of the delivery of all audit work, planned and unplanned.

6.3 In delivering this strategy and plan, we will ensure that liaison has taken place with the Council’s external auditors, Grant Thornton, to ensure that the use of audit resources is maximised, duplication of work is avoided, and statutory requirements are met.

7. Training and Development

7.1 The effectiveness of the Internal Audit Service depends significantly on the quality, training and experience of its staff. Training needs of individual staff members are identified through a formal performance and development process and are delivered and monitored through on-going management supervision.

7.2 The team is also committed to coaching and mentoring its staff, and to providing opportunities for appropriate professional development. This is reflected in the high proportion of staff holding a professional internal audit or accountancy qualification as well as numerous members of the team continuing with professional training during 2023/24.

8. Quality and Performance

8.1 With effect from 1 April 2013, all of the relevant internal audit standard setting bodies, including CIPFA, adopted a common set of Public Sector Internal Audit Standards (PSIAS). These are based on the Institute of Internal Auditors International Professional Practices Framework and replace the previous Code of Practice for Internal Audit in Local Government.

8.2 Included within the new Standards is the requirement for the organisation to define the terms 'Board' and 'senior management' in the context of audit activity. This has been set out within the Internal Audit Charter, which confirms the Audit and Standards Committee's role as the Board.

8.3 The PSIAS require each internal audit service to maintain an ongoing quality assurance and improvement programme based on an annual self-assessment against the Standards, supplemented at least every five years by a full independent external assessment. The outcomes from these assessments, including any improvement actions arising, will be reported to the Audit and Standards Committee, usually as part of the annual internal audit report. The results of our latest external assessment, completed by the Chartered Institute of Internal Auditors (IIA) in autumn 2022, were reported to Audit and Standards Committee in January 2023, confirming excellent compliance against the Standards.

8.4 For clarity, the Standards specify that the following core principles underpin an effective internal audit service:

- Demonstrates integrity;
- Demonstrates competence and due professional care;
- Is objective and free from undue influence (independent);
- Aligns with the strategies, objectives, and risks of the organisation;
- Is appropriately positioned and adequately resourced;
- Demonstrates quality and continuous improvement;
- Communicates effectively;
- Provides risk-based assurance;
- Is insightful, proactive, and future-focused;
- Promotes organisational improvement.

8.5 In addition, the performance of Orbis Internal Audit continues to be measured against key service targets focussing on service quality, productivity and efficiency, compliance with professional standards, influence and our staff. These are all underpinned by appropriate key performance indicators as set out in Table 2 below.

APPENDIX 1

8.5 At a detailed level, each audit assignment is monitored and customer feedback sought. There is also ongoing performance appraisals and supervision for all Internal Audit staff during the year to support them in achieving their personal targets.

8.6 In addition to the individual reports to management for each audit assignment, reports on key audit findings and the delivery of the audit plan are made to the Audit and Standards Committee on a quarterly basis. An Annual Internal Audit Opinion is also produced each year.

8.7 Whilst Orbis Internal Audit liaises closely with other internal audit services through the Sussex and Surrey audit and counter fraud groups, the Home Counties Chief Internal Auditors' Group and the Local Authority Chief Auditors' Network, we are continuing to develop joint working arrangements with other local authority audit teams to help improve resilience and make better use of our collective resources.

Table 2: Performance Indicators

Aspect of Service	Orbis IA Performance Indicators	Target
Quality	<ul style="list-style-type: none"> Annual Audit Plan agreed by Audit and Standards Committee Annual Audit Report and Opinion 	By end April
		By end July. To inform Annual Governance Statement (AGS)
	<ul style="list-style-type: none"> Satisfaction levels 	90% satisfied
Productivity and Process Efficiency	<ul style="list-style-type: none"> Audit Plan – completion to draft report stage by 31 March 2024 	90%
Compliance with Professional Standards	<ul style="list-style-type: none"> Public Sector Internal Audit Standards 	Conforms
	<ul style="list-style-type: none"> Relevant legislation such as the Police and Criminal Evidence Act, Criminal Procedures and Investigations Act 	Conforms
Outcomes and degree of influence	<ul style="list-style-type: none"> Implementation of management actions agreed in response to audit findings 	97% for high priority actions
Our Staff	<ul style="list-style-type: none"> Professionally Qualified/Accredited 	80%

Russell Banks
Orbis Chief Internal Auditor

Brighton & Hove City Council

**INTERNAL AUDIT PLAN
2023/24**



Planned Audit Reviews

Review Name	Outline Objective
Governance, People & Resources	
Debtors/ Accounts Receivable	To review the processes and key controls relating to the accounts receivable system, including those in place for ensuring the accuracy of customer details, completeness, accuracy and timeliness of invoicing, recording and matching payments to invoices, and debt recovery.
Business Rates (including 2023 Revaluation)	To provide assurance that controls over business rate revaluation and collection are effective including billing, collection, recovery and reliefs.
Council Tax	To provide assurance that controls over council tax collection are effective, including billing, collection, recovery and the award of discounts.
Revenue Budget Management	A review of the Council's budget management arrangements, to include an assessment of the extent to which planned savings are being delivered.
Payroll	To review controls in relation to the staff payment system, including those relating to payroll deductions, starters, leavers, temporary and permanent payments and variations of pay.
Off Payroll Payments	A review of the controls around appointing consultants and other individuals who are paid by invoice, including an assessment of compliance with IR35.
Corporate Governance	A review of the corporate governance controls, including those around ensuring financial sustainability.
Risk Management	This review will provide assurance over the effectiveness of the Council's Risk Framework, building upon audit work completed in 2022/23.
Procurement Contract Standing Orders	Regulatory changes will require changes to the Council's Procurement Contract Standing Orders. This review will review whether guidance and policies reflect these changes and appropriate arrangements are in place to help ensure compliance with them.
Information Governance (Subject Access Request (SAR) and Freedom of Information (FOI) Reporting Arrangements)	This audit will seek to provide assurance that controls are in place to allow the Authority to respond to all FOI and SAR requests in a timely manner and that there are sufficient reporting and governance processes in place to monitor and manage performance.

**INTERNAL AUDIT PLAN
2023/24**



Recovery and Resilience (including Cyber Security) Arrangements	This audit will review the key controls operating to ensure that Council arrangements are resilient and robust in the event of a cyber attack or other technology-related outage. The audit will also seek assurance over controls to allow the Authority to quickly recover from any technology-related disaster, focussing on corporate systems (supported by IT&D) as well as those procured and managed within departments.
Robotics (Governance Arrangements)	Robotic Process Automation (RPA) is a form of business process automation that allows a user to define a set of instructions for a robot to perform automatically, often repeating the task quickly. The review will evaluate the effectiveness of the controls to govern the use of Robotics within the Authority, including review of the controls to ensure the accuracy of all data processed by 'robots' and ensuring appropriate failure reports are built into the decision making routines.
Patch Management	We will review the controls in place to support effective patch management ensuring that patches and system updates are tested prior to being applied and that patches are applied in a timely manner.
Replacement of Back Office Systems	Provide independent advice, support and challenge on risk, control, probity and governance issues in respect of this programme, including the provision of post go-live activity as agreed with the Board.
Performance Development Plans's and 121's follow-up	To follow up on the previous audit which concluded Partial Assurance.
Working Time Directive follow-up	To follow up on the previous audit which concluded Partial Assurance.
Health & Safety follow-up	To follow up on the previous audit which concluded Partial Assurance.
Declaration of Interests Staff follow-up	To follow up on the previous audit which concluded Partial Assurance.

Review Name	Outline Objective
Families, Children and Learning	
Early Help Services	To review the revised arrangements for the delivery of Early Help Services. We will seek assurance that robust governance and processes are in place and that outcomes are as expected.

**INTERNAL AUDIT PLAN
2023/24**



Complex Care Placements for Children	To review arrangements in place for determining and resourcing suitable care placements, providing assurance that key controls are operating as intended.
Unaccompanied Asylum Seekers (Children)	To review arrangements in place where there are shared responsibilities with the Home office. Providing assurance that key controls are in place and operating effectively.
School Meals Contract follow-up	To follow up on the previous audit which concluded Partial Assurance.
Schools Audits	Allocation to include a sample of individual schools, general advice and the communication of guidance and best practice to schools.

Review Name	Outline Objective
Health and Adult Social Care	
Transition from Children to Adults	To review the arrangements in place over the process in place for the transition from children's to adult's services and provide assurance that key controls are operating as intended.
HASC Debt Management and Recovery	The Debt Management Project in HASC is coming to its completion. This audit will review the effectiveness of the Council's monitoring arrangements of debt and review the progress of the project.
Life Events- Income	To review the key controls around setting of fees and charges, receipt of income and budget management by the registrar and bereavement services.
Adult Services Data Handling	This audit will seek to ensure there is an appropriate Data Protection Impact Assessment (DPIA) in place and being complied with, appropriate permissions are sought, and data is encrypted in transit and deleted as appropriate.
Carelink	A review of the process and controls in place associated with the Carelink service, including service level agreements and recharging.
Eclipse Application Control	This application audit will review all major input, processing, and output controls, including access controls and the interfaces with any other systems and ensure appropriate system ownership and responsibilities are known.
ASC Income & Assessments follow-up	To follow up on the previous audit which concluded Partial Assurance.

INTERNAL AUDIT PLAN

2023/24



Review Name	Outline Objective
Environment, Economy and Culture	
Parking Enforcement	A review of the process and controls in place associated with parking enforcement and fines, including income collection, banking and reconciliation.
Accommodation Strategy and Workstyle Programme	This audit will focus on the strategy and programme to reduce office occupancy, including security/access and health and safety arrangements.
Surveillance Cameras follow-up	To follow up on the previous audit which concluded Partial Assurance.
EU Interreg Grant – Blueprint for a Circular Economy	To provide financial scrutiny and certification of the grant in accordance with the EU First Level Controller requirements.
Bus Subsidy Grants	To check and certify the grants in accordance with the requirements of the Department for Transport.
Transport Capital Grants	To check and certify the grant in accordance with the requirements of the Department for Transport.

Review Name	Outline Objective
Housing, Neighbourhoods and Communities	
Housing Allocations	To review the processes and controls over the allocation of properties to residents on the Council's waiting list.
Warmer Homes Programme	This audit will review the governance and key controls in this programme, including procurement of contractors.
Business Continuity Planning	To review the key controls and effectiveness of the process to ensure that the Council can continue to deliver key services in the event of a major incident which could prevent systems or staff operating as usual.
Homes for Ukraine	This audit will review the governance and key controls in this programme to ensure that payments are appropriately made to support refugees arriving from Ukraine and residents in the City who have opened their homes to host refugees.
Recommissioning of Supported Accommodation	Review the governance framework and provide assurance that the procurement of services is compliant and in accordance with Council strategy and controls are in place to monitor delivery to agreed timeframes.
Housing Major and Planned Works	To review the programme for major and planned works in light of regulatory changes following on from the Grenfell Tower enquiry and new legislation to tackle mould and damp in homes.

INTERNAL AUDIT PLAN

2023/24



Review Name	Outline Objective
Housing Repairs Works Management System and Supply Chain.	We will continue to provide independent advice, support and challenge on risk, control, probity and governance issues in respect of this programme, including post go-live assurance activity.
Housing Rents follow-up	To follow up on the previous audit which concluded Partial Assurance.
Seaside Homes follow-up	To follow up on the previous audit which concluded Minimal Assurance.
Home Upgrade Grant	To check and certify the grant in accordance with the requirements of the Department for Business, Energy and Industrial Strategy

Review Name	Outline Objective
Contingencies	
Anti-Fraud and Anti-Corruption	To deliver the 2023/24 Fraud Response Plan for BHCC which includes work on fraud awareness, data analytics, cyber fraud, conflicts of interest, excessive personal use of council IT equipment and ad hoc investigations.
Housing Tenancy Fraud	To deliver investigations into housing tenancy fraud and illegal subletting to help ensure that housing is provided to those most in need. The CIPFA Fraud and Corruption Tracker places housing fraud as the largest threat to local authorities. We receive funding from the Housing Revenue Account to fund investigator resource.
Emerging Risks	A contingency budget to allow work to be undertaken on new risks and issues identified by Orbis IA and/or referred by management during the year.
General Contingency	A contingency budget to allow for effective management of the annual programme of work as the year progresses..

Review Name	Outline Objective
Internal Audit Service Management and Delivery	
Action Tracking	Ongoing action tracking and reporting of agreed, high risk actions.

INTERNAL AUDIT PLAN

2023/24



Review Name	Outline Objective
Annual Internal Audit Report and Opinion and Annual Governance Statement	Creation of Annual Report and Opinion and assistance with preparation of the Annual Governance Statement.
Audit and Fraud Management	Overall management of all audit and counter fraud activity, including work allocation, work scheduling and Orbis Audit Manager meetings.
Audit and Fraud Reporting	Production of periodic reports to management and Audit Committee covering results of all audit and anti-fraud activity.
Audit Committee and other Member Support	Ongoing liaison with Members on internal audit matters and attending Audit Committee meetings and associated pre-meetings.
Client Service Liaison	Liaison with clients and departmental management teams throughout the year.
Client Support and Advice	Ad hoc advice, guidance and support on risk, internal control and governance matters provided to clients and services throughout the year.
Orbis IA Developments	Internal Audit and corporate fraud service developments, including quality improvement and ensuring compliance with Public Sector Internal Audit Standards.
Organisational Management Support	Attendance and ongoing support to organisational management meetings, e.g. Orbis Customer Board, Information Governance Board, Orbis Customer Board, Corporate Health and Safety meetings.
Strategy and Annual Audit Planning	Development and production of the Internal Audit Strategy and Annual Audit Plan, including consultation with management and Members.
System Development and Administration	Development and administration of Audit and Fraud Management systems.

Other Auditable Areas Identified During the Audit Planning Process

These are potential audits that could be drawn into the 2023/24 annual programme of work on a risk-basis should other audits be postponed or deferred, or should available contingency time allow for it.

Housing Void Properties

Health Protection Review

Educational Disadvantage

Out of Area Residential Rehabilitation

INTERNAL AUDIT PLAN

2023/24



Digital Data Preservation
Allocation of School Places
Microsoft cloud environment - Governance Review
Active Directory/Identity Management (incl 3rd party)
Data Breach Management
Supplier Failure
Apprenticeships
Childrens' Social Care Case Management
Federation Governance Arrangements
Planned Maintenance - Property Maintenance Budget
Events Management
City Clean Modernisation Programme
Departmental Transport Service
Sports Leisure Facilities

INTERNAL AUDIT CHARTER

1. Introduction

This Charter describes for the Council the purpose, authority and responsibilities of the Internal Audit function in accordance with the UK Public Sector Internal Audit Standards (PSIAS).

The PSIAS require that the Charter must be reviewed periodically and presented to “senior management” and “the board” for approval. For the purposes of this charter “senior management” will be the Executive Leadership Team (ELT) and the board will be the Audit and Standards Committee.

The Charter shall be reviewed annually and approved by ELT and the Audit and Standards Committee. The Chief Internal Auditor is responsible for applying this Charter and keeping it up to date.

2. Internal Audit Purpose

The mission of Internal Audit is to enhance and protect organisational value by providing risk-based and objective assurance, advice and insight.

Internal Audit is defined in the PSIAS as “an independent, objective assurance and consulting activity designed to add value and improve an organisation’s operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.”

Internal Audit supports the whole Council to deliver economic, efficient and effective services and achieve the Council’s vision, priorities and values.

3. Statutory Requirement

Internal Audit is a statutory service in the context of the Accounts and Audit Regulations 2015, which require every local authority to maintain 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.

These regulations require any officer or Member of the Council to:

- make available such documents and records; and
- supply such information and explanations;

as are considered necessary by those conducting the audit.

This statutory role is recognised and endorsed within the Council’s Financial Regulations.

In addition, the Council's S151 Officer has a statutory duty under Section 151 of the Local Government Act 1972 to establish a clear framework for the proper administration of the authority's financial affairs. To perform that duty the Section 151 Officer relies, amongst other things, upon the work of Internal Audit in reviewing the operation of systems of internal control and financial management.

4. Internal Audit Responsibilities and Scope

Annually, the Chief Internal Auditor is required to provide to the Audit and Standards Committee an overall opinion on the Council's internal control environment, risk management arrangements and governance framework to support the Annual Governance Statement.

Internal Audit is not responsible for control systems. Responsibility for effective internal control and risk management rests with the management of the Council.

Internal Audit activity must be free from interference in determining the scope of activity, performing work and communicating results.

The scope of Internal Audit includes the entire control environment and therefore all of the Council's operations, resources, services and responsibilities in relation to other bodies. In order to identify audit coverage, activities are prioritised based on risk, using a combination of Internal Audit and management risk assessment (as set out within Council risk registers). Extensive consultation also takes place with key stakeholders and horizon scanning is undertaken to ensure audit activity is proactive and future focussed.

Internal audit activity will include an evaluation of the effectiveness of the organisation's risk management arrangements and risk exposures relating to:

- Achievement of the organisation's strategic objectives;
- Reliability and integrity of financial and operational information;
- Efficiency and effectiveness of operations and activities;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures and contracts.

5. Independence

Internal Audit will remain sufficiently independent of the activities that it audits to enable auditors to perform their duties in a way that allows them to make impartial and effective professional judgements and recommendations. Internal auditors should not have any operational responsibilities.

Internal auditors will not review specific areas of the Council's operation in which they have previously worked, until a period of at least 12 months has elapsed.

Internal Audit is involved in the determination of its priorities in consultation with those charged with governance. The Chief Internal Auditor has direct access to, and freedom to report in their

own name and without fear of favour to, all officers and Members and particularly those charged with governance. This independence is further safeguarded by ensuring that the Chief Internal Auditor's formal appraisal/performance review is not inappropriately influenced by those subject to audit. This is achieved by ensuring that both the Chief Executive and the Chairman of the Audit and Standards Committee have the opportunity to contribute to this performance review.

All Internal Audit staff are required to make an annual declaration of interest to ensure that objectivity is not impaired and that any potential conflicts of interest are appropriately managed.

6. Appointment and Removal of the Chief Internal Auditor

The role of Chief Internal Auditor is a shared appointment across the 3 Orbis partner authorities (East Sussex County Council, Surrey County Council and Brighton & Hove City Council).

In order to ensure organisational independence is achieved, all decisions regarding the appointment and removal of the Chief Internal Auditor will be made following appropriate consultation with Member representatives from each of the authorities' audit committees.

7. Reporting Lines

Regardless of line management arrangements, the Chief Internal Auditor has free and unfettered access to report to the S151 Officer; the Monitoring Officer; the Chief Executive; the Audit and Standards Committee Chair; the Leader of the Council and the Council's External Auditor.

The Audit and Standards Committee will receive reports on a periodic basis – as agreed with the Chair of the Audit and Standards Committee – on the results of audit activity and details of Internal Audit performance, including progress on delivering the audit plan.

8. Fraud & Corruption

Managing the risk of fraud and corruption is the responsibility of management. Internal Audit will, however, be alert in all its work to risks and exposures that could allow fraud or corruption and will investigate allegations of fraud and corruption in line with the Council's Anti Fraud and Corruption Strategy.

The Chief Internal Auditor should be informed of all suspected or detected fraud, corruption or irregularity in order to consider the adequacy of the relevant controls and evaluate the implication for their opinion on the control environment.

Internal Audit will promote an anti-fraud and corruption culture within the Council to aid the prevention and detection of fraud.

9. Consultancy Work

Internal Audit may also provide consultancy services, generally advisory in nature, at the request of the organisation. In such circumstances, appropriate arrangements will be put in place to safeguard

the independence of Internal Audit and, where this work is not already included within the approved audit plan and may affect the level of assurance work undertaken; this will be reported to the Audit and Standards Committee.

In order to help services to develop greater understanding of audit work and have a point of contact in relation to any support they may need, Internal Audit has put in place a set of service liaison arrangements that provide a specific named contact for each service; and, regular liaison meetings. The arrangements also enable Internal Audit to keep in touch with key developments within services that may impact on its work.

10. Resources

The work of Internal Audit is driven by the annual Internal Audit Plan, which is approved each year by the Audit and Standards Committee. The Chief Internal Auditor is responsible for ensuring that Internal Audit resources are sufficient to meet its responsibilities and achieve its objectives.

Internal Audit must be appropriately staffed in terms of numbers, grades, qualifications and experience, having regard to its objectives and to professional standards. Internal Auditors need to be properly trained to fulfil their responsibilities and should maintain their professional competence through an appropriate ongoing development programme.

The Chief Internal Auditor is responsible for appointing Internal Audit staff and will ensure that appointments are made in order to achieve the appropriate mix of qualifications, experience and audit skills. The Chief Internal Auditor may engage the use of external resources where it is considered appropriate, including the use of specialist providers.

11. Due Professional Care

The work of Internal Audit will be performed with due professional care and in accordance with the UK Public Sector Internal Audit Standards (PSIAS), the Accounts and Audit Regulations (2015) and with any other relevant statutory obligations and regulations.

In carrying out their work, Internal Auditors must exercise due professional care by considering:

- The extent of work needed to achieve the required objectives;
- The relative complexity, materiality or significance of matters to which assurance procedures should be applied;
- The adequacy and effectiveness of governance, risk management and control processes;
- The probability of significant errors, fraud or non-compliance; and
- The cost of assurance in proportion to the potential benefits.

Internal Auditors will also have due regard to the Seven Principles of Public Life – Selflessness; Integrity, Objectivity; Accountability; Openness; Honesty; and Leadership.

12. Quality Assurance

The Chief Internal Auditor will control the work of Internal Audit at each level of operation to ensure that a continuously effective level of performance – compliant with the PSIAS, is maintained.

A Quality Assurance Improvement Programme (QAIP) is in place which is designed to provide reasonable assurance to its key stakeholders that Internal Audit:

- Performs its work in accordance with its charter;
- Operates in an effective and efficient manner; and,
- Is adding value and continually improving the service that it provides.

The QAIP requires an annual review of the effectiveness of the system of Internal Audit to be conducted. Instances of non-conformance with the PSIAS, including the impact of any such non-conformance, must be disclosed to the Audit and Standards Committee. Any significant deviations must be considered for inclusion in the Council's Annual Governance Statement.

February 2023

Brighton & Hove City Council

Audit and Standards Committee

Agenda Item 51

Subject: Annual Surveillance Report 2022

Date of meeting: 18th April 2023

Report of: Executive Director Finance Governance and Resources

Contact Officer: Name: Jo Player
Tel: 01273 292488
Email: jo.player@brighton-hove.gov.uk

Ward(s) affected: All

For general release

1. Purpose of the report and policy context

1.1 The purpose of this report is to appraise Committee of the activities undertaken utilising the Council's statutory powers to conduct covert surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA) since the last report to Committee in April 2022.

1.2 The report also introduces an updated Policy and Guidance document for Committee to review.

2. Recommendations

2.1 That Committee approves the continued use of covert surveillance as an enforcement tool to prevent and detect crime and disorder investigated by its officers, providing the activity is in line with the Council's Policy and Guidance and the necessity and proportionality rules are stringently applied.

2.2 That Committee notes the surveillance activity undertaken by the authority since the report to Committee in April 2022 as set out in paragraph 3.3

2.3 That Committee approves the continued use of the Policy and Guidance document as set out in Appendix 1 in its amended form.

3. Context and background information

3.1 The Regulation of Investigatory Powers Act 2000 (RIPA) as amended is the law governing the use of covert surveillance techniques by public authorities, including local authorities. RIPA was enacted as part of a suite of legislation flowing from the Human Rights Act 1997. RIPA requires that when public authorities need to use covert techniques to obtain information about someone, they may do so only where necessary and in a way which is compatible with human rights.

- 3.2 RIPA regulates the interception of communications, directed and intrusive surveillance and the use of covert human intelligence sources (informants). Local authorities may only carry out directed surveillance, access certain communications data and use informants, provided that strict criteria are met.
- 3.3 Statutory guidance on the use of RIPA is produced in the form of a detailed Code of Practice, which was last revised in December 2022. That provides that elected members should review the authority's use of the 1997 Act and the 2000 Act and set the policy at least once a year. The objective is to ensure that the Council's powers are being used in a way which is consistent with the local authority's policy, which remains fit for purpose. The Council has carried out no surveillance operations since the last report to Committee in April 2022.
- 3.4 The Protection of Freedoms Act was enacted in November 2012. Since then, approval must be sought from a Magistrate when local authorities wish to conduct surveillance activity, access communications data and/or use informants. This is in addition to the authorisation by an Authorising Officer who meets the criteria regarding their position within the authority.
- 3.5 In addition to seeking the approval of a Magistrate, all applications must meet the Serious Offence test. This stipulates that any directed surveillance is restricted to the investigation of offences that carry a custodial sentence of six months or more. The only offence where this will not apply is in regard to the investigation of underage sales of tobacco or alcohol.
- 3.6 In September 2022 the Investigatory Powers Commissioner's Office (previously the Office of the Surveillance Commissioner) audited the authority's use of RIPA in the last four years since the previous audit in 2018. The IPCO reported that she was satisfied that the authority's use of RIPA was appropriate and that our policies and procedures were good. Training for authorising officers was recommended and this was completed in November 2022.

4. Analysis and consideration of alternative options

- 4.1 While the Council could cease using its powers under RIPA completely, this is not considered an appropriate step.

5. Community engagement and consultation

- 5.1 There has been no consultation in the compilation of this report.

6. Conclusion

- 6.1 This Report provides reassurance that officers at this authority are equipped to use the Council's powers under RIPA where necessary and within the threshold set out in the Protection of Freedoms Act 2012, only after excluding all other methods of enforcement. An authorisation will only be

given by the relevant 'Authorising Officer' following vetting by the 'Gatekeeper'. There is now the additional safeguard of judicial sign off.

- 6.2 The implementation of the Annual review has made the whole process transparent and demonstrates to the public that the correct procedures are followed.

7. Financial implications

- 7.1 There are no financial implications arising from this report. Any covert surveillance undertaken needs to be met from within current budget resources.

Name of finance officer consulted: Mike Bentley Date consulted
24/03/23

8. Legal implications

- 8.1 The legal framework that governs the Council's use of its powers under RIPA and related legislation is described in the body of the Report. The annual review by this Committee of the Council's policy on these legal powers and of the use it makes of them (which in the last financial year was nil) is mandated by statutory guidance. This Report provides reassurance that the Council's powers are exercised lawfully and proportionately, and only where relevant criteria have been met.

Name of lawyer consulted: Victoria Simpson Date consulted 27.03.23

9. Equalities implications

- 9.1 The proper and consistent application of the RIPA powers should ensure that a person's basic human rights are not interfered with, without justification. Each application will be assessed by the gatekeeper for necessity and proportionality prior to the authorisation by a restricted number of authorising officers. The application will also be signed off by a Magistrate. This process aims to identify any inconsistencies or disproportionate targeting of minority groups and enable action to be taken to remedy any perceived inequality.

10. Sustainability implications

- 10.1 There are no sustainability implications

11. Other Implications

Crime & disorder implications:

- 11.1 If used appropriately, the activities described in this report should enhance our capacity to tackle crime and disorder

Supporting Documentation

1. Appendices

1. Policy and Guidance Document version January 2023



**Brighton & Hove
City Council**

Corporate Policy & Procedures Document on the Regulation of Investigatory Powers Act 2000 (RIPA)

- Use of Directed Surveillance
- Use of Covert Human Intelligence Sources
- Accessing Communications Data

Jo Player
Head of Safer Communities
Telephone: 01273 292488
Fax: 01273 292524
E-mail: jo.player@brighton-hove.gov.uk

Version: January 2023

Contents page

Introduction	3
Policy Statement	4
Senior Responsible Officer	4
Authorising Officers Responsibilities	5
General Information on RIPA	7
What RIPA Does and Does Not Do	8
Types of Surveillance	9
Conduct and Use of a Covert Human Intelligence Source (CHIS)	13
Online Covert Activity	14
Juvenile Sources and Vulnerable Individuals	17
Accessing Communications Data	19
Authorisation Procedures	20
Grounds for Authorisation	21
Serious Crime and Non RIPA Surveillance	21
Confidential Material	23
Duration	24
Working with Other Agencies	24
Record Management	25
Consequences of Non Compliance	26
Oversight by Members	26
Concluding Remarks	27
Appendix 1: List of Authorising Officers	28
Appendix 2: Flow chart outlining process	29
Appendix 3: List of Useful Websites	30
Appendix 4: Guidance for Authorising Officers	31
Appendix 5: Guidance for Applicants	34

The Regulation of Regulatory Powers Act 2000 refers to 'Designated Officers'. For ease of understanding and application this document refers to 'Authorising Officers'.

Introduction

This document is based on the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Home Office's Code of Practices for Directed Surveillance and Covert Human Intelligence Sources (CHIS) and Accessing Communications data. It takes into account the oversight provisions contained in the revised Code of Practice for Covert Surveillance and the revised Code of Practice that deals with Access to communications data that came into force on 6th April 2010. Officers should also bear in mind Procedures and Guidance issued by the Office of the Surveillance Commissioner in December 2014, and guidance issued in the revised code of practice in August 2018, when applying for, and authorising applications. This policy and procedures document sets out the means of compliance with, and use of, the Act by The Council. It is based upon the requirements of the Act and the Home Office's Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources, together with the Revised Draft Code of Practice on Accessing Communications Data

The authoritative position on RIPA is the Act itself and any Officer who is unsure about any aspect of this document should contact the Head of Safer Communities or the Head of Law, for advice and assistance.

This document has been approved by elected members and is available from the Head of Safer Communities.

The Head of Safer Communities will maintain the Central Register of all authorisations, reviews, renewals, cancellations and rejections. It is the responsibility of the relevant Authorising Officer to ensure that relevant form is submitted, for inclusion on the register, within 1 week of its completion.

This document will be subject to an annual review by the Head of Safer Communities and will be approved by elected members.

In terms of monitoring e-mails and internet usage, it is important to recognise the interplay and overlap with the Council's Information Technology policies and guidance, the Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000, the Data Protection Act 1998 and its Code Of Practice and the General Data Protection Regulations. RIPA forms should only be used where **relevant** and they will only be **relevant** where the **criteria** listed are fully met.

Policy Statement

The Council takes its statutory responsibilities seriously and will at all times act in accordance with the law and takes necessary and proportionate action in these types of matters. In that regard the Head of Safer Communities is duly authorised to keep this document up to date and amend, delete, add or substitute relevant provisions, as necessary. For administrative and operational effectiveness, the Head of safer Communities is authorised to add or substitute Authorising Officers with the agreement of the Senior Responsible Officer.

It is this Council's Policy that

- All covert surveillance exercises conducted by the Council should comply with the requirements of RIPA
- An Authorisation will only be valid if initialled by a gatekeeper and signed by an authorising officer.
- Authorising 'Access to Communications data' will be restricted to the Head of Safer Communities. The National Anti Fraud Network will become the Single Point of Contact for purposes of Access to Communications Data.

Senior Responsible Officer

The revised Code of Practice recommends that each public authority appoints a Senior Responsible Officer. This officer will be responsible for the integrity of the process in place within the public authority to authorise directed surveillance; compliance with the relevant Acts and Codes of Practice; 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.

The Senior Responsible Officer should be a member of the corporate management team and for the purposes of this policy the Executive Director Finance Governance and Resources has been so delegated. It is the responsibility of the Senior Responsible Officer to ensure that all authorising officers are of an appropriate standard in light of any recommendations in the inspection reports prepared by the Office of the Surveillance Commissioners. Where an inspection report highlights concerns about the standards of authorising officers, it is the responsibility of the Senior Responsible Officer to ensure these concerns are addressed.

Authorising Officers Responsibilities

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 and the Regulation of Investigatory Powers (Communications Data) Order 2010, specify the seniority of officers who are able to authorise surveillance activity and access to communications data. These are Directors, Head of Service, Service Manager or equivalent.

It is essential that Senior Managers and Authorising Officers take personal responsibility for the effective and efficient operation of this document.

It is the responsibility of the Senior Responsible Officer in conjunction with the Head of Safer Communities to ensure that sufficient numbers of Authorising Officers receive suitable training on RIPA and this document, and that they are competent.

It will be the responsibility of those Authorising Officers to ensure that relevant members of staff are also suitably trained as 'Applicants'.

An authorisation must not be approved until the Authorising Officer is satisfied that the activity proposed is necessary and proportionate.

However it will be the responsibility of the gatekeeper to review any applications prior to submission to the Authorising Officer. They should ensure that the correct form has been used. These are the latest Home Office forms and are available on the HO website and that the applicant has obtained a Unique Reference Number (URN) from the Partnership Support Officer Safer Communities Services. The gatekeeper should also ensure that the form has been correctly completed and contains sufficient detail and information to enable the authorising officer to make an informed decision whether to authorise the application. The gatekeeper should also scrutinise the form to ensure that it complies with the necessity and proportionality requirements before the authorising officer receives the form. A gatekeeper should be a person with sufficient knowledge and understanding of the enforcement activities of the relevant public body, who should vet the applications as outlined above. Once the gatekeeper is satisfied with the application they should initial the form and submit any comments on the application in writing to the Authorising Officer and provide necessary feedback to the applicant. In order that there is consistency with the quality of applications the Head of Safer Communities and Principal Trading Standards Officer will act as gatekeepers for the Council. It should be noted that the Head of Safer Communities will not act as gatekeeper and Authorising Officer on the same application.

- **Necessary** in this context includes consideration as to whether the information sought could be obtained by other less invasive means, and that those methods have been explored and been unsuccessful or could have compromised the investigation. The Authorising Officer must be satisfied that there is necessity to use covert surveillance in the proposed operation. In order to be satisfied there must be an identifiable offence to prevent or detect before an authorisation can be granted on the grounds falling within sec 28(3)(b) and 29(3)(b) of RIPA and ss6(3) and 7(3) of RIP(S)A. The application should identify the **specific offence** being investigated (**including the Act and section**) and the **specific point(s) to prove** that the surveillance is intended to gather evidence about. The applicant must show that the operation is **capable of gathering that evidence** and that such **evidence is likely to prove** that part of the offence.
- Deciding whether the activity is **proportionate** includes balancing the right to privacy against the seriousness of the offence being investigated. Consideration must be given as to whether the activity could be seen as excessive. An authorisation should demonstrate how the

Authorising Officer has reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate to what it seeks to achieve. A potential model answer would make it clear that the 4 elements of proportionality had been fully considered.

1. Balancing the size and scope of the operation against the gravity and extent of the perceived mischief,
2. Explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others,
3. That the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result and,
4. Evidencing what other methods had been considered and why they were not implemented.

Authorising Officers must pay particular attention to Health & Safety issues that may be raised by any proposed surveillance activity. Approval must not be given until such time as any health and safety issue has been addressed and/or the risks identified are minimised.

Authorising Officers must ensure that staff who report to them follow this document and do not undertake any form of surveillance, or access communications data, without first obtaining the relevant authorisation in compliance with this document.

Authorising Officers must ensure when sending copies of any forms to the Head of Safer Communities for inclusion in the Central Register, that they are sent in **sealed** envelopes and marked **Strictly Private & Confidential**.

General Information on RIPA

The Human Rights Act 1998 (which brought much of the European Convention on Human Rights and Fundamental Freedoms 1950 into UK domestic law) requires the City Council, and organisations working on its behalf, to respect the private and family life of citizens, his home and his correspondence.

The European Convention did not make this an absolute right, but a qualified right. Therefore, in certain circumstances, the City Council may interfere in an individual's right as mentioned above, if that interference is:-

- a. **In accordance with the law;**
- b. **Necessary;** and
- c. **Proportionate.**

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a statutory mechanism (i.e. 'in accordance with the law') for authorising **covert surveillance** and the use of a '**covert human intelligence source**' ('CHIS') – e.g. undercover agents, and **Accessing Communications data**. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, the RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

Directly employed Council staff and external agencies working for the City Council are covered by the Act for the time they are working for the City Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf must be properly authorised by an Authorising Officer after scrutiny by a gatekeeper.

A list of officers who may authorise Directed Surveillance is kept by the Head of Safer Communities and the current list is attached at **Appendix 1**. This list will be updated annually. The designated gatekeepers for the Council are the Principal Trading Standards Officer and the Head of Safer Communities. For the purposes of Accessing Communications Data the Designated Persons (Authorised Officers) is the Head of Safer Communities.

If the correct procedures are not followed, evidence may be dis-allowed by the courts, a complaint of mal-administration could be made to the Ombudsman, and/or the Council could be ordered to pay compensation. Such action would not, of course, promote the good reputation of the City Council and will, undoubtedly, be the subject of adverse press and media interest.

A flowchart of the procedures to be followed appears at **Appendix 2**. A list of useful websites is available at **Appendix 3**.

What RIPA Does and Does Not Do

RIPA does:

- Requires prior authorisation of directed surveillance
- Prohibits the Council from carrying out intrusive surveillance
- Requires authorisation of the conduct and use of a CHIS
- Require safeguards for the conduct and use of a CHIS
- Requires proper authorisation to obtain communication data
- Prohibits the Council from accessing 'traffic data'

RIPA does not:

- Make unlawful conduct which is otherwise lawful
- Prejudice or dis-apply any existing powers available to the City Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, it does not affect the Council's current powers to obtain information via the DVLA or to get information from the Land Registry as to the ownership of a property.

If the Authorising Officer or any Applicant is in any doubt, they should ask the Head of Safer Communities or the Head of Law before any directed surveillance, CHIS, or Access to Communications is authorised, renewed, cancelled or rejected.

Types of Surveillance

'Surveillance' includes

- Monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications.
- Recording anything mentioned above in the course of authorised surveillance
- Surveillance, by or with, the assistance of appropriate surveillance device(s).

Surveillance can be overt or covert.

Overt Surveillance

Most surveillance activity will be done overtly, that is, there will be nothing secretive, clandestine or hidden about it. In many cases, officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. a Neighbourhood Warden walking through the estate).

Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner/proprietor to check that the conditions are being met.

The following are NOT normally Directed Surveillance:

- Activity that is observed as part of normal duties, e.g. by an officer in the course of day-to-day work.
- CCTV cameras (unless they have been directed at the request of investigators) – these are overt or incidental surveillance, and are regulated by the Data Protection Act.

Covert Surveillance

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place. (Section 26(9)(a) RIPA) It is about the intention of the surveillance, not about whether they are actually aware of it; it is possible to be covert in Council uniform where, for example, the person is intended to mistake the reason for the officer being there.

RIPA regulates two types of covert surveillance, (Directed Surveillance and Intrusive Surveillance) and the use of Covert Human Intelligence Sources (CHIS).

Directed Surveillance

Directed Surveillance is surveillance which: -

- Is covert; and
- Is not intrusive surveillance;
- Is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it; and
- It is undertaken for the purpose of a **specific investigation** or **operation** in a manner **likely to obtain private information** about an individual (whether or not that person is specifically targeted for purposes of an investigation).

Private information in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact, or associates, with.

Examples of Expectations of Privacy:

Two people are holding a conversation on the street and, even though they are talking together in public, they do not expect their conversation to be overheard and recorded by anyone. They have a 'reasonable expectation of privacy' about the contents of that conversation, even though they are talking in the street.

The contents of such a conversation should 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 and otherwise than by way of an immediate response to events.

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.

For the avoidance of doubt, only those officers designated as 'Authorising Officers' for the purpose of RIPA can authorise 'Directed Surveillance' IF, AND ONLY IF, the RIPA authorisation procedures detailed in this document, are followed.

Reconnaissance- Examples

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. If the officers chanced to see illegal activities taking place, these could be recorded and acted upon as 'an immediate response to events'. If, however, the officers intended to carry out the exercise at a specific time of day, when they expected to see unlawful activity, this would not be reconnaissance but directed surveillance, and an authorisation should be considered. Similarly, if the officers wished to conduct a similar exercise several times, 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 or persons and a directed surveillance authorisation should be considered.

Intrusive Surveillance

This is when it: -

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

Only police and other law enforcement agencies can carry out this form of surveillance.

Council Officers must not carry out intrusive surveillance.

Notes about 'Intrusive'

Surveillance is generally 'Intrusive' only if the person is on the same premises or in the same vehicle as the subject(s) of the surveillance. Carrying out surveillance using private residential premises (with the consent of the occupier) as a 'Static Observation Point' does not make that surveillance 'Intrusive'. A device used to enhance your external view of property is almost never an *intrusive* device. A device would only become *intrusive* where it provided a high quality of information from inside the *private residential premises*. A device used to enhance your external view of property is almost never an *intrusive* device. A device would only become intrusive where it provided a high quality of information from inside the *private residential premises*. If premises under surveillance are known to be used for legally privileged communications, that surveillance must also be treated as *intrusive*.

Examples:

Officers intend to use an empty office to carry out surveillance on a person who lives opposite. As the office is on the 4th floor, they wish to use a long lens and binoculars so that they can correctly identify and then photograph their intended subject covertly. This is NOT intrusive surveillance, as the devices do not provide high quality evidence from inside the subject's premises. Officers intend using a surveillance van parked across the street from the subject's house. They could see and identify the subject without binoculars but have realised that, if they use a 500mm lens, as the subject has no net curtains or blinds, they should be able to see documents he is reading. This IS intrusive surveillance, as the evidence gathered is of a high quality, from inside the premises, and is as good as could be provided by an officer or a device being on the premises.

Examples of different types of Surveillance

Type of Surveillance	Examples
<u>Overt</u>	<ul style="list-style-type: none"> • Police Officer or Parks Warden on patrol • Sign-posted Town Centre CCTV cameras (in normal use) • Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. • Most test purchases (where the officer behaves no differently from a normal member of the public).
<u>Covert</u> but not requiring prior authorisation	<ul style="list-style-type: none"> • CCTV cameras providing general traffic, crime or public safety information.
<u>Directed</u> (must be RIPA authorised)	<ul style="list-style-type: none"> • Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit or off long term sick from employment. • Test purchases where the officer has a hidden camera or other recording device to record information that might include information about the private life of a shop-owner, e.g. where s/he is suspected of running his business in an unlawful manner.
<u>Intrusive</u>	<ul style="list-style-type: none"> • Planting a listening or other device (bug) in a person's home or in their private vehicle. <p style="text-align: center;">THE COUNCIL CANNOT CARRY OUT THIS ACTIVITY AND FORBIDS ITS OFFICERS FROM CARRYING IT OUT</p>

Conduct and Use of a Covert Human Intelligence Source (CHIS)

Who is a CHIS?

A Covert Human Intelligence Source (CHIS) is someone who establishes or maintains a personal or other relationship for the covert purpose or facilitating anything falling under the following bullet points;

- Covertly uses such a relationship to obtain information or to provide access to any information to another person or,
- Covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

RIPA may or may not apply in circumstances where members of the public volunteer information to the Council or to contact numbers set up to receive such information (such as benefit fraud hotlines). It will often depend on how the information was obtained. If an individual has obtained the information in the course of or as a result of a personal or other relationship it may be that they are acting as a CHIS. The contrast is between such a person and one who has merely observed the relevant activity from 'behind his (actual or figurative) net curtains.

A relationship is covert if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of its purpose.

If a person who volunteers information is then asked to obtain further information, it is likely that they would either become a CHIS or that a directed surveillance authorisation should be considered.

Examples of a CHIS may include:

- Licensing officers, working with the Police, covertly building a business relationship with a cab company which is believed to be using unlicensed drivers.
- Food safety officers posing as customers to get information on what is being sold at premises and developing a relationship with the shopkeeper beyond that of supplier and customer

What must be authorised?

Officers must not create or use a CHIS without prior authorisation. If there is any doubt as to whether an individual is acting as a CHIS advice should be sought from the Head of Safer Communities.

- Creating (or "Conduct of") a CHIS means procuring a person to establish or maintain a relationship with a person so as to secretly obtain and pass on information. The relationship could be a personal or 'other' relationship (such as a business relationship) and obtaining the information may be either the only reason for the relationship or be incidental to it. Note that it can also include asking a person to continue a relationship which they set up of their own accord.

- Use of a CHIS includes actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

Online Covert Activity

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. See above.

Example 1: *A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest 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 2: *A customs 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. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)*

Example 3: *A public authority 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 or deployment. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an on-going operation or investigation, authorisation should be considered.*

In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation (see paragraph 4.32).

Example: *Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed*

surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance.

It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws.

Juvenile Sources and Vulnerable Individuals

Juvenile Sources

Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). **On no occasion can a child under 16 years of age be authorised to give information against his or her parents.**

Authorisations for juvenile CHIS must not be granted unless: -

- A risk assessment has been undertaken as part of the application, covering the physical dangers and the psychological aspects of the use of the child
- The risk assessment has been considered by the Authorising Officer and he is satisfied that any risks identified in it have been properly explained; and
- The Authorising Officer has given particular consideration as to whether the child is to be asked to get information from a relative, guardian or any other person who has for the time being taken responsibility for the welfare of the child.

Only the Chief Executive may authorise the use of Juvenile Sources.

Vulnerable Individuals

A Vulnerable Individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

A Vulnerable Individual will only be authorised to act as a source in the most exceptional of circumstances.

Only the Chief Executive may authorise the use of Vulnerable Individuals.

Test Purchases

Carrying out test purchases will not require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also directed surveillance.

Please also see below under 'Serious Crime'

Anti-social behaviour activities (e.g. noise, violence, racial harassment etc)

Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues.

Placing a covert stationary or mobile video camera outside a building to record anti social behaviour on residential estates will require prior authorisation.

Accessing Communications Data

Local authority employees will no longer be able to use their powers under relevant legislation and the exemption under the Data Protection Act 1998. The disclosure of communications data by Communication service providers will now only be permitted if a Notice to obtain and disclose (or in certain circumstances an Authorisation for an Officer to obtain it themselves) has been issued by the 'Designated person'.

Authorities are required to nominate Single Point of Contacts (SPOC) and that person(s) must have undertaken accredited training.

'Designated Persons' within the Council is now limited to the Head of Safer Communities.

Local authorities may only access to Customer Data or Service Data. **They cannot access 'traffic data'.**

Customer data (Subscriber)

Customer data is the most basic information about users of communication services.

It includes:-

- The name of the customer
- Addresses for billing, etc.
- Contact telephone numbers
- Abstract personal records provided by the customer (e.g. demographic information or sign up data)
- Account information (bill payment arrangements, bank or credit/debit card details)
- Services subscribed to.

Service Data (Service user)

This relates to the use of the Service Provider services by the customer, and includes:-

- Periods during which the customer used the service
- Information about the provision and use of forwarding and re-direction services
- Itemised records of telephone calls, internet connections, etc
- Connection, disconnect and re-connection
- Provision of conference calls, messaging services, etc
- Records of postal items, etc
- Top-up details for pre-pay mobile phones.

Traffic Data

This is data about the communication. It relates to data generated or acquired by the Service Provider in delivering or fulfilling the service. **Local authorities do not have access to this data.**

Authorisation Procedures

Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation. **Appendix 2** provides a flow chart of the process to be followed.

Authorising Officers

Directed surveillance and or the use of CHIS can only be authorised by the officers listed in this document attached at appendix 1. Authorising officers should ensure that they undertake at least one refresher training course on RIPA during each calendar year. The list will be kept up to date by the Head of Safer Communities and amended as necessary. The SRO can add, delete or substitute posts to this list as required.

Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and internal departmental Schemes of Management. RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete or about to expire.

Only the Chief Executive can authorise the use of a CHIS who is a juvenile or a vulnerable person or in cases where it is likely that confidential information will be obtained through the use of surveillance.

Authorising Officers–Access to Communications data

The Head of Safer Communities are the 'Designated persons' permitted to authorise the obtaining and disclosing of communications data. The National Anti Fraud Network will be the Single Point of Contact.

Training Records

A certificate of attendance will be given to anyone undertaking training in relation to the use of RIPA. Training will be recorded on their individual learning and development plan.

Single Points of Contact under Part 1 of the Act are required to undertake accredited training. A record will be kept of this training and any updating. This record is kept by NAFN. Designated persons are also required to be suitably trained.

Application Forms

Only the currently approved forms, available on the Home Office website, may be used. Any other forms will be rejected by the gatekeeper/authorising officer. Applications for communications data should be made via the NAFN website. Please contact NAFN for further information on this process – contact details on the Wave.

A gatekeeper role will be undertaken by either the Head of Safer Communities or the Principal Trading Standards Officer who will check that the applications have been completed on the correct forms, have a URN and that they contain sufficient grounds for authorisation. They will provide feedback to the applicant and will initial the forms before being submitted to the authorising officer.

The Head of Safer Communities can fulfil both the role as gatekeeper and authorising officer but will not fulfil both roles for an individual application.

Grounds for Authorisation

Directed Surveillance or the Conduct and Use of the CHIS and Access to Communications Data can be authorised by an Authorising Officer where he believes that the authorisation is necessary in the circumstances of the particular case. For local authorities the only ground that authorisation can be granted is;

- For the prevention or detection of crime

Serious Crime and Non RIPA Surveillance

Serious Crime

From 1st November 2012, the Protection of Freedoms Act introduced an additional requirement for officers seeking to use directed surveillance or CHIS. From this date, with the exception of Trading Standards' work regarding test purchases for alcohol and tobacco, all applications must meet the 'serious crime' threshold. This has been identified as any offence for which the offender could be imprisoned for 6 months or more. An analysis of relevant offences indicates that covert surveillance may therefore be used by, Trading Standards (various offences including doorstep crime and counterfeiting), Waste Enforcement (fly tipping), Fraud against the Council and Child Protection and Adult Safeguarding issues. Where an offence meets the serious crime threshold, the applicant will apply to the Authorising Officer in the normal way via a gatekeeper, but will then need to attend Magistrate's Court to obtain judicial sign off.

Non RIPA Surveillance

This new process will automatically restrict the use of surveillance activity under the RIPA framework by a number of our services as the offences they deal with do not meet the serious crime threshold.

RIPA does not grant any powers to carry out surveillance, it simply provides a framework that allows authorities to authorise surveillance in a manner that ensures compliance with the European Convention on Human Rights. Equally, RIPA does not prohibit surveillance from being carried out or require that surveillance may only be carried out following a successful RIPA application.

Whilst it is the intention of this Authority to use RIPA in all circumstances where it is available, for a Local Authority, this is limited to preventing or detecting crime and from 1st November 2012 to serious crime. The Authority recognises that there are times when it will be necessary to carry out covert directed surveillance when RIPA is not available to use. Under such circumstances, a RIPA application must be completed and clearly endorsed in red 'NON-RIPA SURVEILLANCE' along the top of the first page. The application must be submitted to a RIPA Authorising Officer in the normal fashion, who must consider it for Necessity and Proportionality in the same fashion as they would a RIPA application. The normal procedure of timescales, reviews and cancellations must be followed. Copies of all authorisations or refusals, the outcome of reviews or renewal applications and eventual cancellation must be notified to the Head of Safer Communities who will keep a

separate record of Non-RIPA activities, and monitor their use in the same manner as RIPA authorised activities.

Assessing the Application Form

Before an Authorising Officer authorises an application, **they must**

Be mindful of this Corporate Policy & Procedures Document

Satisfy themselves that the RIPA authorisation is

- **in accordance with the law,**
- **Necessary** in the circumstances of the particular case on the ground specified above; and
- **Proportionate** to what it seeks to achieve

This means that they must consider

- whether other less invasive methods to obtain the information have been considered. The least intrusive method will normally be considered the most proportionate unless for example it is impractical or would undermine the investigation.
- balance the right of privacy against the seriousness of the offence under investigation. When considering necessity and proportionality, an authorising officer should spell out in terms of the 5 W's, (who, what, why, where, when and how) what specific activity is being sanctioned.
- Take account of the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (**Collateral Intrusion**).
- Ensure that measures are taken wherever practicable to avoid or minimise collateral intrusion.
- Set a date for review of the authorisation and review on only that date where appropriate.
- Ensure that the form carries a unique reference number
- Ensure that the applicant has sent a copy to the Head of Safer Communities for inclusion in the Central Register within 1 week of the authorisation.
- Ensure that the application is cancelled when required.

NB the application **MUST** make it clear how the proposed intrusion is necessary and how an absence of this evidence would prejudice the outcome of the investigation. If it does not then the application **SHOULD** be refused. Some guidance on how to complete the form for both authorising officers and applicants is available at **Appendix 4** and **Appendix 5**

Retention and Destruction of the Product

Where the product of surveillance could be relevant to pending or future legal proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period. This should be in line with any subsequent review. Attention should be drawn to the requirements of the Code of Practice issued under the Criminal Procedures and Investigations Act 1996. This states that material obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

There is nothing in RIPA 2000 which prevents material obtained from properly authorised surveillance being used in other investigations. However we must be mindful to handle store and destroy material obtained through the use of covert surveillance appropriately. It will be the responsibility of the Authorising Officer to ensure compliance with the appropriate data protection

requirements and to ensure that any material is not retained for any longer than is necessary. It will also be the responsibility of the Authorising Officer to ensure that the material is disposed of appropriately.

Confidential Material

Particular care should be taken where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved.

Confidential Information consists of matters subject to legal privilege, confidential personal information or confidential journalistic information. So for example extra care should be taken where through the use of surveillance, it would be possible to obtain knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality, or legal privilege may be involved.

Where it is likely, through the use of surveillance, that confidential information will be obtained, authorisation can only be granted by Heads of Service or in their absence the Chief Executive.

Descriptions of what may constitute legally privileged information are set out in section 98 of Police Act 1997 and further guidance is set out in Paragraphs 3.4-3.9 of the Home Office Code of Practice on Covert Surveillance.

Confidential Personal Information and Confidential Journalistic Information

Similar considerations to those involving legally privileged information must also be given to authorisations that involve the above. 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. This information can be either written or oral and might include consultations between a doctor and patient or information from a patient's medical records. Spiritual counselling means conversations between an individual and a Minister of Religion acting in an official capacity, where the individual being counselled is seeking or the Minister is imparting forgiveness, absolution or the resolution of conscience with the authority of the Divine Being(s) of their faith.

Confidential journalistic material includes material acquired or created for the purpose of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

Further information or guidance regarding Confidential Information can be obtained from the Head of Law or the Head of Safer Communities.

Additional Safeguards when Authorising a CHIS

When authorising the conduct or use of a CHIS, the Authorising Officer **must also**

- Be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved;

- Be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment; At all times there will be a person designated to deal with the CHIS on behalf of the authority and for the source's security and welfare. This person should be in at least the position of Head of Service.
- Consider the likely degree of intrusion of all those potentially affected;
- Consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and
- Ensure **records** contain particulars and are not available except on a need to know basis

Records must be kept that contain the information set out in Statutory Instrument 2000/2725 – The Regulation of Investigatory Powers (Source Records) Regulations 2000. Further guidance on the requirements can be obtained from the Head of Safer Communities.

Duration

The application form **must be reviewed in the time stated and cancelled** once it is no longer needed. The 'authorisation' to conduct the surveillance lasts for a maximum of 3 months for Directed Surveillance and 12 months for a Covert Human Intelligence Source. In respect of a notice or authorisation to obtain communications data the period is one month.

Authorisations can be renewed in writing when the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred.

The renewal will begin on the day when the authorisation would have expired.

Urgent authorisations, if not ratified by written authorisation, will cease to have effect after 72 hours, beginning from the time when the authorisation was granted.

Working with Other Agencies

If an officer wishes to utilise the CCTV system operated by the Police

Directed Surveillance Authorisation must be obtained before an approach is made to the Control Room. If immediate action is required an Authorisation must be obtained within 72 hours of the request being made.

When some other agency has been instructed on behalf of the City Council to undertake any action under RIPA, this Document and the Forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

When another Enforcement Agency (e.g. Police, HMRC etc): -

Wish to use the City Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures. Before any Officer agrees to allow the City Council's resources to be used for the other agency's purposes, they must obtain a copy of that agency's RIPA form, or written confirmation that a Directed Surveillance Authorisation is in place.

Wish to use the City Council's premises for their own RIPA action, the Officer should, normally, co-operate with the same, unless there is security or other good operational or managerial reasons as to why the City Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the City Council's co-operation in the agent's RIPA operation. In such cases, however, the City Council's own RIPA forms should not be used as the City Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

Record Management

A Central Register of all Authorisation Forms will be maintained and monitored by the Head of safer Communities.

Records maintained in the Department

- A copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- A record of the period over which the surveillance has taken place;
- The frequency of reviews prescribed by the Authorising Officer;
- A record of the result of each review of the authorisation;
- A copy of any renewal of an authorisation, together with supporting
- Documentation submitted when the renewal was requested;
- The date and time when any instruction was given by the Authorising Officer;
- The Unique Reference Number for the authorisation (URN).

Central Register maintained by Safer Communities

Authorising Officers must forward details of each form to The partnership support officer Safer Communities for the Central Register, **within 1 week of the authorisation, review, renewal, cancellation or rejection.**

Records will be retained for six years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) and the Interception Commissioner can audit/review the City Council's policies and procedures, and individual authorisations.

Consequences of Non Compliance

Where covert surveillance work is being proposed, this Policy and Guidance must be strictly adhered to in order to protect both the Council and individual officers from the following:

- **Inadmissible Evidence and Loss of a Court Case / Employment Tribunal / Internal Disciplinary Hearing** – there is a risk that, if Covert Surveillance and Covert Human Intelligence Sources are not handled properly, the evidence obtained may be held to be inadmissible. Section 78 of the Police and Criminal Evidence Act 1984 allows for evidence that was gathered in a way that affects the fairness of the criminal proceedings to be excluded. The Common Law Rule of Admissibility means that the court may exclude evidence because its prejudicial effect on the person facing the evidence outweighs any probative value the evidence has (probative v prejudicial).
- **Legal Challenge** – as a potential breach of Article 8 of the European Convention on Human Rights, which establishes a “right to respect for private and family life, home and correspondence”, incorporated into English Law by the Human Rights Act (HRA) 1998. This could not only cause embarrassment to the Council but any person aggrieved by the way a local authority carries out Covert Surveillance, as defined by RIPA, can apply to a Tribunal – see section 15.
- **Offence of unlawful disclosure** – disclosing personal data as defined by the DPA that has been gathered as part of a surveillance operation is an offence under Section 55 of the Act. Disclosure can be made but only where the officer disclosing is satisfied that it is necessary for the prevention and detection of crime, or apprehension or prosecution of offenders. Disclosure of personal data must be made where any statutory power or court order requires disclosure.
- **Fine or Imprisonment** – Interception of communications without consent is a criminal offence punishable by fine or up to two years in prison.
- **Censure** – the Office of Surveillance Commissioners conduct regular audits on how local authorities implement RIPA. If it is found that a local authority is not implementing RIPA properly, then this could result in censure.

Oversight by Members

- Elected Members shall have oversight of the Authority’s policy and shall review that policy annually.
- The report to members shall be presented to the Elected Members by the SRO. The report must not contain any information that identifies specific persons or operations.
- Alongside this report, the SRO will report details of ‘Non-RIPA’ surveillance in precisely the same fashion
- Elected Members may not interfere in individual authorisations. Their function is to, with reference to the reports; satisfy themselves that the Authority’s policy is robust and that it is being followed by all officers involved in this area. Although it is elected members who are accountable to the public for council actions, it is essential that there should be no possibility of political interference in law enforcement operations.

Concluding Remarks

Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure may be that the action (and the evidence obtained), is held to be inadmissible by the Courts pursuant to Section 6 of the Human Rights Act 1998.

Obtaining an authorisation under RIPA and following this document will ensure, therefore, that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.

Authorising Officers should be suitably competent and must exercise their minds every time they are asked to sign the request. They must never sign or rubber stamp form(s) without thinking about their personal and the City Council's responsibilities.

Any boxes not needed on the Form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and the form retained for future audits.

For further advice and assistance on RIPA, please contact the Head of Safer Communities.

Directed Surveillance/CHIS Forms can be obtained from the Home Office website or from NAFN in relation to Access to Communications Data.

Appendix 1: List of Authorising Officers

List of Authorised Officers

Post	Name
Head of Safer Communities	Jo Player
Head of Revenues and Benefits	Graham Bourne

Designated Person for Approving a Notice in Respect of Access to Communications Data

- Head of Safer Communities: Jo Player

Single Point of Contact for Accessing Communications Data

- National Anti Fraud Network (NAFN)

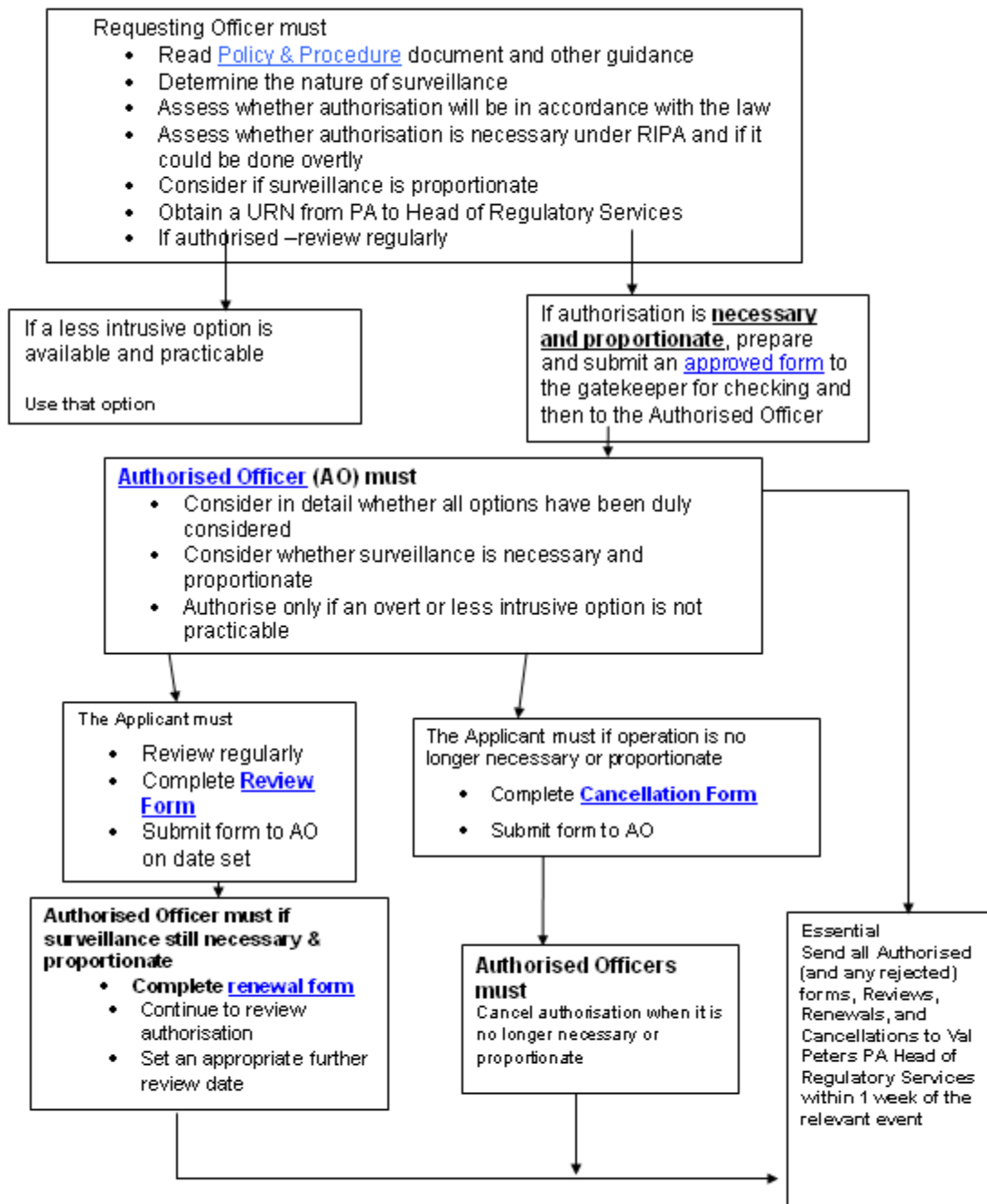
Gatekeepers

- Head of Safer Communities: Jo Player
- Principal Trading Standards Officer: John Peerless

Please contact Charlotte Farrell for a URN

Appendix 2: Flow chart outlining process

Authorising Directed Surveillance Process



Appendix 3: List of Useful Websites

RIPA Forms, Codes of Practice and Advice

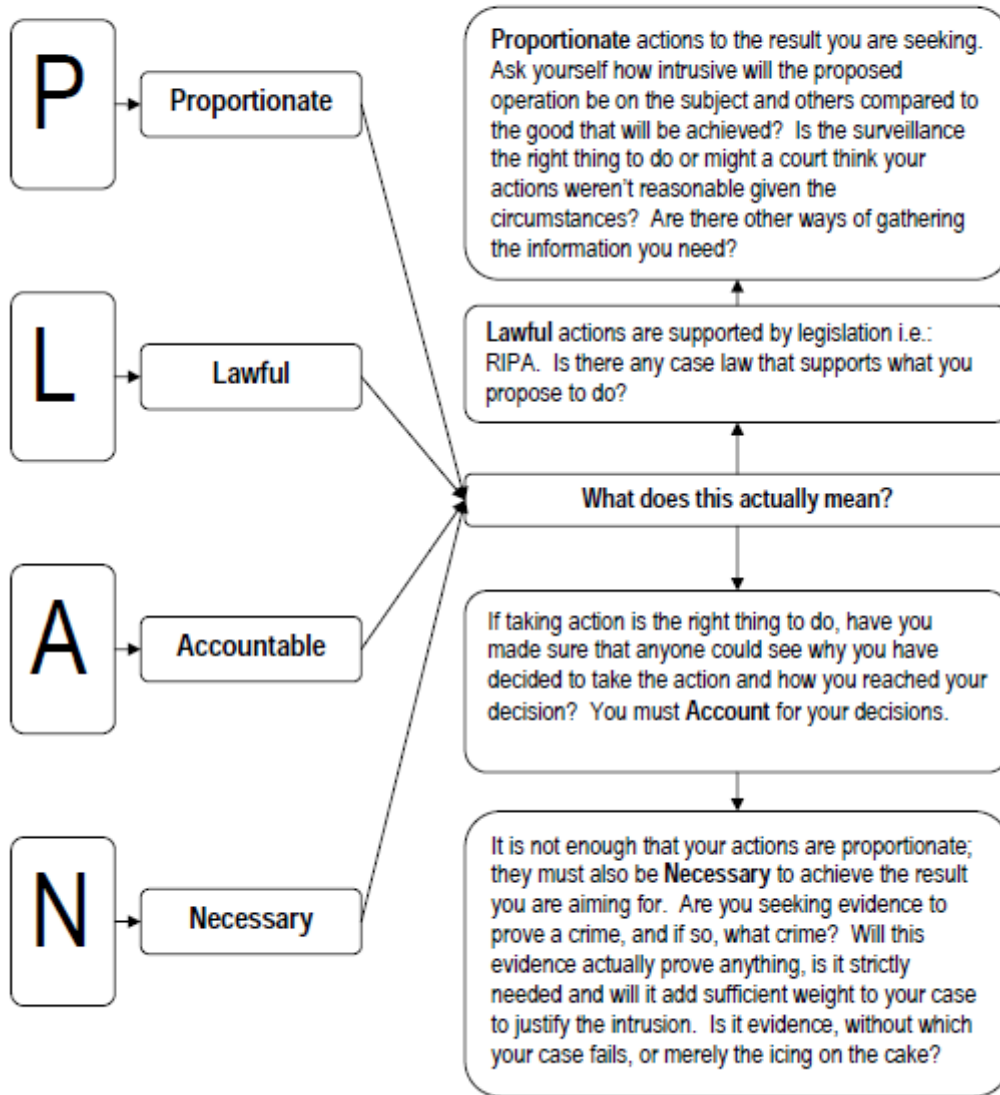
The policy requires you to use the most up-to-date versions of forms and codes of practice. Rather than reproduce forms and codes of practice that are subject to change, we have provided links to the currently approved versions. You should access the document you require by following the relevant link.

- The most up-to-date RIPA forms must always be used. These are available from the Home Office website and may be found by following this link :
<http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/>
- The full text of the Codes of Practice are available here :
<http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/>
- The Act is available here:
<http://www.legislation.gov.uk/ukpga/2000/23/contents>
- The Office of Surveillance Commissioners website has some useful information and advice and is available here :
<http://surveillancecommissioners.independent.gov.uk/>

Appendix 4: Guidance for Authorising Officers

APPENDIX FOUR

Notes for Guidance for Authorisation – Directed Surveillance



Authorised Officer's Statement

<p>12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who, What, Where, When, Why and the following box.]</p> <p>I hereby authorise directed surveillance defined as follows: [Why is the surveillance necessary directed against, Where and When will it take place, What surveillance activity/equipment is achieved?]</p>	<p>You must start by fully explaining what operation you are authorising. State why the surveillance is necessary to the case, what will be achieved, how it will be carried out, how many people used, what equipment / vehicles / technology you authorise the use of and where the operation will happen.</p> <p>Make sure it is clear <u>exactly</u> what it is that you are authorising.</p>
<p>13. Explain why you believe the directed surveillance is necessary. [Code paragraph 2.4] Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. [Code paragraph 2.5]</p>	

Now you must explain your decision. Simply stating that you "agree with the officer who applied for the reasons they gave" is not acceptable. You must give, in your own words, a detailed account of how you came to decide that the operation was necessary and proportionate. Make sure that you review the guidance in section seven and show how the evidence is necessary to the offence, and how the offence is one that it is necessary to investigate. Now ensure that you demonstrate how the officer has shown the need to obtain the evidence to be proportionate, when balanced against the person's expectation of privacy, the privacy of innocent third parties and the seriousness of the offence.

If you have completed a surveillance authorisation worksheet, go back over this as you should have already stated your reasons there.

You must explain why you feel it is in the public interest to carry out the action; is it serious, prevalent in the area, an abuse of position, premeditated? Why do you think that the investigation will be prejudiced without surveillance? Are you certain there is no other obvious and less intrusive way of obtaining the information? Does it need to be done? Record everything in this section.

This section must stand on its own, if you are called to court to justify your authorisation.

Authorised Officer's Statement

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with 3.1 to 3.12		This section is to be completed only by the Senior Authorised Officer if confidential information might be obtained. They should explain why they felt it to be appropriate for the surveillance to be carried out. To comply with the codes, show how further measures, such as more regular reviews and stricter limitations, have been put in place due to the particularly sensitive nature of the operation.	
Date of first review		This should be no more than four weeks from the date of authorisation. If you wish to restrict the length of time an officer may carry out surveillance for, you can use this box to set an early review date.	
Programme for subsequent reviews of this authorisation: [Code paragraph 4.22]. Only complete dates after first review are known. If not or inappropriate to set additional review dates then leave blank.			
Use this box to record dates for review. The normal review period is no longer than every four weeks. It doesn't have to be completed but is useful to do so, especially when a shorter review period is appropriate.			
Name (Print)	Grade / Rank		
Signature	Date and time		
Expiry date and time [e.g.: authorised on 30 June 2005, 23.59]		Expiry date and time [e.g.: authorised on 1 April 2005 - expires]	
Finally, write your name, sign the form giving the date and time. You must also record the expiry date. This is always three months, to the minute, from the date that the authorisation was given, no longer, or shorter. The operation can be cancelled before this date if appropriate. (See 7.14 (above) for guidance.)			

Sections 15 and 16:

These sections relate to oral authorisations that may be granted or renewed only in urgent cases. In the case that an oral authorisation is granted, the AO should record the reasons why they considered the case urgent and why they believed it was not practicable to delay in order for the investigator to complete an application. Urgent oral authorisations last for seventy-two hours from the time of the authorisation. The officer carrying out the surveillance must complete a written application at the earliest opportunity, not necessarily at the end of the seventy-two hours.

Appendix 5: Guidance for Applicants

The RIPA 1 Form – Guidance Notes on Completion

Directed Surveillance Unique Reference Number (URN) (to be supplied by the central monitoring officer).

Unique reference number. This must be provided by the Authorising Officer

PART II OF THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) 2000

APPLICATION FOR AUTHORISATION TO CARRY OUT DIRECTED SURVEILLANCE

Public Authority (including full address)

What public body do you work for? Record it here

Unit/Branch/Division

What dept / unit do you work in? Record it here.

Full address

Full address of your dept / office / building.

Contact details

Give a phone number, email address and / or fax number to contact you on.

Investigation/Operation Name (if applicable)

You can give the operation a name if you wish.

Investigating Officer (if a person other than the applicant)

If the person who is the investigator in the case is someone other than you, record their name here.

Details of application:

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003; No. 3171. For local authorities exact position of the authorising officer should be given. For example, Head of Trading Standards.

You must give the position of the Authorised Officer who will be reviewing the application. You do not need to give their name. This should be their full job title, rank or position.

Page Two

Enter a summary of the reason for the operation and what you are planning to do. Be brief: what will you do, why are you doing it and what will you get out of it?

2. Describe the purpose of the specific operation or investigation.

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.

What methods will you use for the surveillance?
What are the technical aspects? Who, what, when, where, how long, how many, equipment etc. Mention everything. You will not be authorised to do things you don't mention here.

4. The identities, where known, of those to be subject of the directed surveillance.

Name:
• Address:
• DOB:
• Other information as appropriate:

Who are you intending to gather evidence on?
If you do not know the identity of all parties you must describe them as best as you are able.

5. Explain the information that it is desired to obtain as a result of the directed surveillance.

What evidence do you intend to obtain from the surveillance? Specify exactly what you intend to get, how much and what types. This is so a judgement can be made on the weight of the evidence that you will get. Be careful what you write here: when you have achieved these aims the surveillance must stop immediately.

Page Three

<p>Specify the offences that you are investigating or preventing. State why the information has to be obtained by surveillance, why do you need it for the reason you specified? How is it essential to the case?</p>	<p>6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA. Delete that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on. (SI 2003 No 3171)</p>	<p>Cross out the conditions that do not apply to you. In the case of a local authority, the only one that <i>does</i> is prevention or detecting crime or disorder.</p>
	<ul style="list-style-type: none">• In the interests of national security;• For the purpose of preventing or detecting crime or of preventing disorder;• In the interests of the economic well-being of the United Kingdom;• In the interests of public safety;• for the purpose of protecting public health;• for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;	
	<p>7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 2.4]</p>	
	<p>8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 2.6 to 2.10.] Describe precautions you will take to minimise collateral intrusion</p>	
	<p>Collateral intrusion is where the operation interferes with the private lives of those not intended to be subject to the surveillance. This could be members of the suspect's family, their partners, colleagues or members of the public. You must identify where there is a risk that you will gather this sort of information. You must take steps to minimise this risk and show that the risk left is unavoidable: what times are you conducting surveillance? Can you avoid catching others on camera? Do you have facilities to remove identifying features? The AO must be satisfied that the need to carry out the operation outweighs this risk.</p>	

Page Four

This is where you must justify your actions as proportionate. You should have completed a planner and decided that surveillance is necessary and the last resort. Record here what you have done already and what you cannot do as it'll prejudice the investigation. Tell the AO why the need to carry out the action outweighs the suspect's right to privacy. How serious is the matter? How intrusive will the operation be on the suspect and on others? What might happen if you don't carry out surveillance? Why can't you get the information in other ways? What will be achieved by gathering the evidence?

9. Explain why this directed surveillance is proportionate to what it s
be on the subject of surveillance or on others? And why is this
surveillance in operational terms or can the evidence be obtained
2.5]

...ive might it
by the need for
...? (Code paragraph
2.5]

10. Confidential information [Code paragraphs 3.1 to 3.12].

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION.

11. Applicant's details

Name (print)		Tel No:	
Grade/Rank		Date	
Signature			

Confidential information is *special knowledge* of a person's religious, political or medical life or information of a confidential journalistic nature (journalistic sources). Communications subject to legal privilege are also confidential. If there is a chance that you might gather this sort of information, indicate the risk here. The authorisation can then only be given by the person within your public body designated by the RIPA code of practice for this purpose.

Finish by giving your name, telephone number, job title or rank. Date the form and sign it.

Brighton & Hove City Council

Audit & Standards Committee

Agenda Item 52

Subject: Standards Update

Date of meeting: 18 April 2023

Report of: Executive Director, Governance, People & Resources

Contact Officer: Name: Victoria Simpson
Tel: 01273 294687
Email: Victoria.simpson@brighton-hove.gov.uk

Ward(s) affected: All

1. Purpose of the report and policy context

- 1.1 To provide an update on Standards-related matters, including regarding complaints received in alleging that Members have breached the Code of Conduct for Members.

2. Recommendations

- 2.1 That the Committee notes the report.

3. Context and background information

- 3.1 The Council is required by the Localism Act 2011 to have in place arrangements for dealing with complaints against elected and co-opted Members. Brighton & Hove City Council regularly reviews the arrangements it has in place, including its Code of Conduct for Members and related Procedure and guidance. It is transparent about those arrangements and also makes data regarding the complaints received in about member conduct publicly available via the reports to this Committee.
- 3.2 At Brighton & Hove City Council, the Audit & Standards Committee has delegated authority for leading in discharging the statutory requirement that the Council maintain and promote high standards of conduct by Members. This Committee receives quarterly reports on complaints against members as well as information on the training and briefings offered to assist Members in discharging their responsibilities according to the expectations of the Nolan Principles.
- 3.3 This quarterly Report provides data on the complaints received in since the last Report, as well as updates on those complaints which were still being considered/ have been determined. In this way, it provides reassurance that recent complaints are being considered and dealt with pursuant to the Council's processes.

4. Update on current complaints

Complaints previously reported to this Committee

4.1 In accordance with the last report to this Committee, this data is provided in the attached Appendix 1, at table 1.

Complaints received in since the last Update

4.2 This data is provided in table 2 of Appendix 1.

4.3 All of the complaints referred to in this section are being progressed by the Monitoring Officer in accordance with the Procedure which governs member complaints.

5. Member Training

5.1 Appendix 2 provides data on member attendance at Standards-related training held in the last twelve months, in accordance with the steer given at the last meeting of this Committee.

5.2 In the last twelve months the training offered has included:

- Code of Conduct training: three alternative refresher sessions to enable members to recap on the Council's standards arrangements and to update themselves including the modifications made in summer 2021
- Social media and the Code of Conduct: two alternative training sessions delivered by an external trainer on the use of social media, highlighting the challenges and opportunities for those members who use social media in their roles as councillors.
- Standards Panel training: two alternative sessions for members of the Audit and Standards Committee, delivering training mandatory for any member participating in a Standards Panel.

5.3 More detailed information can be provided in future regarding member attendance at training over the last four years/ during the next term should members wish it. That could include the numbers of individual members who are not recorded as having attended any training and/or a breakdown of attendance which reflects Group affiliation (if any).

6 Analysis and consideration of alternative options

6.1 The Council is obliged under the Localism Act to make arrangements for maintaining high standards of conduct among members and to make arrangements for the investigation of complaints. This Council's arrangements are regularly reviewed. This Report draws attention to the wider picture without recommending specific options.

7 Community engagement & consultation

- 7.1 Recent reviews of the Council's Standards arrangements have been carried out by its elected Members assisted by officers and the Council's Independent Persons, whose familiarity with process in this area has been helpful. The local community has not been consulted or provided input, although this would be an option for future reviews.

8 Conclusion

- 8.1 Members are asked to note the contents of this Report, which aims to assist the Council in discharging its responsibilities for overseeing that high standards of conduct are maintained in a way which is compliant with local requirements

9 Financial implications

- 9.1 There are no additional financial implications arising from the recommendation in this Report. All activity referred to has been, or will be, met from existing budgets.

Name of finance officer consulted: Nigel Manvell Date consulted 27/03/23

10 Legal implications

- 10.1 The legal implications are dealt with in the body of this Report.

Name of lawyer consulted: Victoria Simpson Date consulted 1.4.23

Supporting Documentation

1. Appendices

Appendix 1 – data on member complaints
Appendix 2 – data on member training attendance

2. Background documents [delete if not applicable]

None

Appendix 1: Complaint data

Table 1: Complaints previously reported to this Committee (at its January 2023 meeting)

Case No	Date	Status of complaint	If concluded, basis on which decision was taken	Compl aint Topic	Additional notes
				<i>*note see end of table 2 for key</i>	
A/2022	January 2022	Ongoing	Not concluded.	D	Following a formal investigation which resulted in the investigating officer's indicative finding that one or more breach(es) of the Code of Conduct had occurred, and having consulted with one of the Independent Persons, the Monitoring Officer decided to refer the complaints to a cross party Standards Panel for determination. However a date on which all Panel members were able to attend could not be identified before the start of the pre election period on 17.3.23. As a result, the complaint has not been determined.
E/2022	February 2022	Ongoing	Not concluded.	D	As per A/2022 above
J/2022	February 2022	Ongoing	Not concluded.	D	As per A/2022 above
W/2022	October 2022	Determined by decision to take no action at preliminary assessment stage	Complaint ultimately determined by decision that – although the member's communications had potential to breach the Code – it would not be in the public interest to refer this complaint for formal investigation.	B	The complaint alleged that the member's responses to them on a ward matter had breached the Code.

X/2022	October 2022	Determined by decision to take no action at preliminary assessment stage	Complaint ultimately determined by decision that – although the member’s communications had potential to breach the Code – it would not be in the public interest to refer this complaint for formal investigation.	B	The complaint alleged that the member’s responses to them on a ward matter had breached the Code.
Z/2022	October 2022	Determined by decision to take no action at preliminary assessment stage	Insufficient evidence was identified regarding those parts of the complaint which alleged incorrect process. While an email comm was found to raise concerns that appropriate standards of respectfulness had not been observed, it was not considered to be in the public interest to refer this part of the complaint for formal investigation.	A	Multi faceted complaint regarding a member’s activities in their ward which required information to be obtained from a series of sources at preliminary assessment.

Table 2: Complaints received in since [the Report to the January 2023 meeting of this Committee](#)

Case No	Date	Status of complaint	If concluded, basis on which decision was taken	Complaint Topic	Additional notes
				<i>* note see end of table 2 for updated key</i>	
A/2023	Jan - Feb 2023	Remains at preliminary assessment stage	N/A	A	Complainant alleged that member had acted in a way toward them which exhibited prejudice and bias.
B/2023	Jan 2023	Determined by decision to take no action at preliminary assessment stage	Insufficient evidence of conduct contrary to the Code was identified to merit referral of complaint for formal investigation.	A	Complainant alleged disrespectfulness and rudeness by the member during a disagreement while they were canvassing.

C/2023	Jan 2023	Decision taken to refer complaint for formal investigation.	N/A	A	Complainant alleged that member had engaged in conduct contrary to the Code which failed to meet appropriate standards of respect and courtesy.
D/2023	Feb 2023	Determined by decision to take no action at preliminary assessment stage	Insufficient evidence of conduct contrary to the Code was identified to merit referral of complaint for formal investigation.	B	Complaint made by one member against another alleged that comments made during a Council meeting about the political party of which the complainant was a member were disrespectful and abusive.
E/2023	Feb 2023	Determined by decision to take no action at preliminary assessment stage	Insufficient evidence of conduct contrary to the Code was identified to merit referral of complaint for formal investigation.	B	Complaint made by one member against another alleged that the comments made during a Council meeting about the political party of which the complainant was a member were disrespectful and abusive.
F/2023	Feb 2023	Determined by decision to take no action at preliminary assessment stage	Insufficient evidence of conduct contrary to the Code was identified to merit referral of complaint for formal investigation.	B	Complainant alleged that the way in which the member responded to a member of the public during a Council meeting failed to exhibit the appropriate standards of respect and courtesy.
G/2023	Feb 2023	Determined by decision to take no action at preliminary assessment stage	Insufficient evidence of conduct contrary to the Code was identified to merit referral of complaint for formal investigation.	B	Complainant alleged that the way in which the member responded to a member of the public during a Council meeting failed to exhibit the appropriate standards of respect and courtesy.
H/2023	March 2023	Remains at preliminary assessment stage	N/A	A	Complainant alleges rudeness and a lack of courtesy toward him in relation to a matter which should have been referred to Council officers.
I/2023	March 2023	Remains at preliminary assessment stage	N/A	A	Complaint alleges that the member's communications via social media were misleading and did not accurately represent the Council's decisions.
J/2023	March 2023	Remains at preliminary assessment stage	N/A	A	Complaint by one member against another alleges that a social media post about standing for re-election breached the Code

					in the way in which it referred to the complainant.
--	--	--	--	--	---

Key to Complaint topics

NB tracked changes indicate updated (more inclusively worded) description of topic A

Code	Description of type of conduct complained about
A	Complaints about members' <u>conduct in their wards, including when discharging</u> ing <u> of their ward responsibilities (including by or otherwise communicating with constituents or other stakeholders).</u>
B	Complaints about comments or conduct either at council meetings, or at meetings at which members are representing BHCC
C	Complaints about conduct relating to council business or other members made outside council meetings, including on social media
D	Complaints about a member's conduct or position on an issue which is not council business or a ward matter, including conduct or a statement reported in the press or made on social media

Appendix 2: Member attendance at Standards-related training

Table 1 – Member attendance at Standards training offered between January 2022 and January 2023

Training description	Number of alternative slots of same training offered	Total number of members who attended a training session
<p>Code of Conduct training: one hour sessions offered via Teams with aim of:</p> <ul style="list-style-type: none"> • Updating on changes to the Code and Procedure made in June 2021, and • Providing a refresher re the framework 	3	25
<p>Social media and the Code of Conduct: 90 minute sessions offered via Teams by an external trainer in response to member ask for training on how BHCC members might best use SM within the expectations of the Code of Conduct</p>	2	7
<p>Standards panel training: one hour sessions offered to Audit & Standards Committee members only:</p> <ul style="list-style-type: none"> • Focused training on the procedure specific to Standards panels 	2	6 (nb there are normally 8 Committee members)

Bar chart showing alternative representation of data in table 1

Note: while training on the Code of Conduct and on Social Media and the Code of Conduct was made available to all fifty four elected members of BHCC, Standards Panel training was offered only to members of Audit & Standards Committee (which is only 8 at any given time but has included different members in the past year).

