



Essex County Council

# **Audit, Governance and Standards Committee**

|              |                                     |   |
|--------------|-------------------------------------|---|
| <b>10:00</b> | <b>Monday, 10<br/>December 2018</b> | <b>Committee Room<br/>1,<br/>County Hall,<br/>Chelmsford, CM1<br/>1QH</b> |
|--------------|-------------------------------------|---|

**For information about the meeting please ask for:**

Andy Gribben, Senior Democratic Services Officer

**Telephone:** 033301 34565

**Email:** [democratic.services@essex.gov.uk](mailto:democratic.services@essex.gov.uk)

|          |  | <b>Pages</b>   |
|----------|--|----------------|
| <b>1</b> | <b>Membership Substitutions and Declarations</b>   | <b>4 - 4</b>   |
| <b>2</b> | <b>Minutes of the meeting held on 17 September 2018</b>  | <b>5 - 8</b>   |
| <b>3</b> | <b>Welcome and Introduction</b><br>The Chairman to introduce Mr David Eagles, Partner,<br>Public Sector Assurance of BDO LLP, the Council's<br>external auditors |                |
| <b>4</b> | <b>Internal Audit and Counter Fraud Progress Report<br/>December 2018</b>  | <b>9 - 33</b>  |
| <b>5</b> | <b>Regulation of Investigatory Powers Act 2000 - review of<br/>activity</b>  | <b>34 - 55</b> |
| <b>6</b> | <b>Date of Next Meeting</b><br>To note that the next meeting will be held on<br>Monday 25 March 2018, at 10:00am in Committee Room 1                             |                |

## **Exempt Items**

(During consideration of these items the meeting is not likely to be open to the press and public)

To consider whether the press and public should be excluded from the meeting during consideration of an agenda item on the grounds that it involves the likely disclosure of exempt information as specified in Part I of Schedule 12A of the Local Government Act 1972 or it being confidential for the purposes of Section 100A(2) of that Act.

In each case, Members are asked to decide whether, in all the circumstances, the public interest in maintaining the exemption (and discussing the matter in private) outweighs the public interest in disclosing the information.

## **Essex County Council and Committees Information**

All Council and Committee Meetings are held in public unless the business is exempt in accordance with the requirements of the Local Government Act 1972. If there is exempted business, it will be clearly marked as an Exempt Item on the agenda and members of the public and any representatives of the media will be asked to leave the meeting room for that item.

The agenda is available on the Essex County Council website, <https://www.essex.gov.uk>. From the Home Page, click on 'Your Council', then on 'Meetings and Agendas'. Finally, select the relevant committee from the calendar of meetings.

### **Attendance at meetings**

Most meetings are held at County Hall, Chelmsford, CM1 1LX. A map and directions to County Hall can be found at the following address on the Council's website: <http://www.essex.gov.uk/Your-Council/Local-Government-Essex/Pages/Visit-County-Hall.aspx>

### **Access to the meeting and reasonable adjustments**

County Hall is accessible via ramped access to the building for people with physical disabilities.

The Council Chamber and Committee Rooms are accessible by lift and are located on the first and second floors of County Hall.

Induction loop facilities are available in most Meeting Rooms. Specialist headsets are available from Reception.

With sufficient notice, documents can be made available in alternative formats, for further information about this or about the meeting in general please contact the named officer on the agenda pack or email [democratic.services@essex.gov.uk](mailto:democratic.services@essex.gov.uk)

### **Audio recording of meetings**

Please note that in the interests of improving access to the Council's meetings, a

sound recording is made of the public parts of many of the Council's Committees. The Chairman will make an announcement at the start of the meeting if it is being recorded.

If you are unable to attend and wish to see if the recording is available you can visit this link <https://cmis.essexcc.gov.uk/Essexcmis5/CalendarofMeetings> any time after the meeting starts. Any audio available can be accessed via the 'On air now!' box in the centre of the page, or the links immediately below it.

Should you wish to record the meeting, please contact the officer shown on the agenda front page

---

## Agenda item 1

**Committee:** Audit, Governance and Standards Committee

**Enquiries to:** Andy Gribben, Senior Democratic Services Officer

### **Membership, Apologies, Substitutions and Declarations of Interest**

#### **Recommendations:**

To note

1. The membership of the committee (as shown below)
2. Apologies and substitutions
3. Declarations of interest to be made by Members in accordance with the Members' Code of Conduct

#### **Membership**

(Quorum: 3)

|                       |               |
|-----------------------|---------------|
| Councillor T Cutmore  | Chairman      |
| Councillor P Channer  |               |
| Councillor A Davies   |               |
| Councillor A Erskine  |               |
| Councillor T Hedley   | Vice-Chairman |
| Councillor R Mitchell |               |
| Councillor R Moore    |               |
| Councillor M Platt    |               |
| Councillor K Smith    |               |
| Councillor A Turrell  |               |

## **Minutes of the meeting of the Audit, Governance and Standards Committee, held in Committee Room 1 County Hall, Chelmsford, CM1 1QH on Monday, 17 September 2018**

### **Present:**

#### **Members:**

|                        |                                    |
|------------------------|------------------------------------|
| Councillor G Butland   | substitute for Councillor Dr Moore |
| Councillor P Channer   |                                    |
| Councillor T Cutmore   | Chairman                           |
| Councillor A Davies    |                                    |
| Councillor A Erskine   |                                    |
| Councillor C Guglielmi | substitute for Councillor Mitchell |
| Councillor M Maddocks  | substitute for Councillor Platt    |
| Councillor K Smith     |                                    |
| Councillor A Turrell   |                                    |

#### **Also Present:**

|                  |  |
|------------------|--|
| Janine Combrinck | Director and representative of BDO (external auditors) |
|------------------|--|

#### **ECC Officers:**

|                   |   |
|-------------------|---|
| Georgia Chimbani  | Director of Local Delivery                                |
| Paula Clowes      | Head of Assurance   |
| Christine Golding | Chief Accountant  |
| Andy Gribben      | Senior Democratic Services Officer (clerk to the meeting) |
| Chris Martin      | Director, of Strategic Commissioning and Policy           |
| Paul Turner       | Director, Legal and Assurance (Monitoring Officer)        |

### **1. Welcome and Introduction**

The Chairman welcomed to the meeting members of the committee, officers in attendance, the representative from the external auditors and members of the public to the meeting.

He reminded members that the meeting was being broadcast live over the internet and that the full discussion would be publicly available on the County Council's website after the meeting.

### **2. Membership, Apologies, Substitutions and Declarations of Interest.**

The report of Membership, Apologies and Declarations was received, and it was noted that:

1. The membership of the Audit, Governance and Standards Committee was as shown in the report.

2. Apologies for absence had been received from Councillors Hedley, Mitchell, Moore and Platt. Councillors Butland, Guglielmi and Maddocks attended as substitutes.
3. Councillor Butland declared a Code Interest as a non-remunerated Director of North Essex Garden Communities as referred to in the Audit Annual Report. The Chairman reminded members that any interests must be declared during the meeting if the need to do so arose.

### **3 Minutes and Matters Arising**

The minutes of the meeting held on 30 July 2018 were approved as a correct record and signed by the Chairman subject to a correction being made to show that Councillor Channer had conveyed her apologies.

There were no matters arising.

### **4 Annual Audit Letter – Year ending 31 March 2018**

Members received a report (AGS/20/18 and appendix) from Margaret Lee, Executive Director for Corporate and Customer Services, the External Auditor's Annual Audit Letter for the year ending 31 March 2018 presented by Christine Golding, Chief Accountant.

The report informed members of the detailed findings from the audit work performed by the external auditors Ernst and Young in relation to the financial year 2017/18 which were reported to the Committee on 30 July 2018.

Members were informed that the Annual Audit Letter, which will be published on the Council's website, contained no new information but provided a roundup of the key issues already reported upon by Ernst and Young in relation to their 2017/18 audit and draws the 2017/18 audit to an end.

#### **Resolved:**

That the report be noted

### **5 Internal Audit and Counter Fraud Progress Report**

Members received the Internal Audit and Counter Fraud Progress Report (AGS/21/18 and appendices 1, 2 and 3) from Paula Clowes, Head of Assurance.

Members noted that there was one 'No Assurance' report, ten reports of 'Limited Assurance' as well as five 'Critical' and seven 'Major' recommendations that had moved beyond their agreed due date. There was also a Counter Fraud update.

The 'No Assurance' report related to the Essex Partnership University NHS Foundation Trust. (EPUT) an audit of which was carried out at the request of the Director, Adult Social Care following concerns about the effectiveness and working practices of the Partnership arrangement with EPUT.

Members were advised that three critical issues had been identified and they received further details from Chris Martin, Director of Strategic Commissioning and Policy and Georgia Chimbani, Director of Local Delivery. The committee requested that an update on these matters be brought back to the meeting to its meeting scheduled for 3 June 2019.

**Resolved:**

That the report be noted.

## **6 Declarations of Interest**

Members received a report (AGS/22/18) from Paul Turner, Director, Legal and Assurance, a noting the results of a recent all-member consultation and seeking approval to make a recommendation to Council to amend the Code of Conduct for Members.

Members were advised that, overall, members were broadly in favour of the proposal but it was not supported by some members and the Leader of the Labour Group.

Councillor Butland offered to take to a future meeting of the Essex Leaders and Chief Executives a proposal that the Monitoring Officers in Essex work towards an alignment of their individual Codes of Members Conduct. This was generally supported by members of the committee.

**Resolved:**

That the Committee recommend to Council that paragraphs 24.8.3 and 24.8.4 of the Code of Conduct for Members be amended to read as follows and that paragraph 24.8.4 of the Constitution becomes 24.8.5:

*24.8.3 In addition you must withdraw from the room during the consideration of an item of business and must not participate in any debate or vote on that item of business if:*

*(a) you have a **Disclosable Pecuniary Interest** in that business; or*

*(b) you have a **Code interest** which is one that a member of the public with knowledge of the relevant facts would reasonably regard as so significant that it is likely to prejudice your judgement of the public interest.*

*24.8.4 Paragraph 24.8.3 does not apply where:*

- 
- (a) *A member has received a dispensation from the Monitoring Officer or the Audit, Governance and Standards Committee; or*
- (b) *A meeting is operating to a procedure which would permit a member of the public to address the committee whether on the invitation of the Chairman or otherwise, but this exemption only applies for as long as the Member is either addressing the committee or answering questions asked by any member of the committee.*

## **7 Work Programme**

Members received the AGS Work Programme (AGS/23/18) from Paul Turner, Director, Legal and Assurance

The draft programme of work, which was requested by the Committee at its meeting in June, was the first such programme for the committee in its new guise as the Audit, Governance and Standards Committee. Members were advised that the programme would be flexible in order to address any matters which might arise.

## **8 Date of Next Meeting**

Members noted that the next meeting of the committee was scheduled to be on Monday 10 December 2018 at 10.00am in Committee Room 1

The meeting closed at 11.48am.

.....  
**Chairman**  
**10 December 2018**

|  |  |                        |
|--|--|------------------------|
| <b>Report title:</b> Internal Audit and Counter Fraud Progress Report  |  | AGS/24/18              |
| <b>Report to:</b> Audit, Governance and Standards Committee  |  |                        |
| <b>Report author:</b> Paula Clowes – Head of Assurance   |  |                        |
| <b>Date:</b> 10 December 2018  |  | <b>For:</b> Discussion |
| <b>Enquiries to:</b> Paula Clowes – Head of Assurance <a href="mailto:paula.clowes@essex.gov.uk">paula.clowes@essex.gov.uk</a> |  |                        |
| <b>County Divisions affected:</b> All Essex  |  |                        |

## 1. Purpose of Report

- 1.1 This report provides the Audit, Governance and Standards Committee with the current position regarding Internal Audit and Counter Fraud activity in relation to the 2018/19 Internal Audit Plan (approved by the Audit, Governance and Standards Committee in March 2018). It reflects the situation as at 30 November 2018.

## 2. Recommendation

- 2.1 That the report be noted.

## 3. Details of Internal Audit and Counter Fraud Activity

### 3.1 Final Internal Audit Reports Issued

- 3.1.1 When Internal Audit issues a report it gives an overall assurance rating which is either 'Good' 'Adequate' 'Limited' or 'No' Assurance. The final reports issued since the September 2018 Audit, Governance and Standards Committee are listed below. Executive Summaries for those reports receiving 'Limited Assurance' or 'No Assurance' are set out in Appendix 2. Full reports are available to Members on request.

|                 |   |
|-----------------|---|
| <b>No</b>       | <ul style="list-style-type: none"> <li>• None</li> </ul>  |
| <b>Limited</b>  | <ul style="list-style-type: none"> <li>• Personal Budgets (families)</li> <li>• De La Salle School</li> </ul>   |
| <b>Adequate</b> | <ul style="list-style-type: none"> <li>• Programme and Project Delivery</li> <li>• Delays in Transfer of Care</li> </ul>  |
| <b>Good</b>     | <ul style="list-style-type: none"> <li>• Analytical Review of School Year End Balances</li> </ul>   |
| <b>Other</b>    | <ul style="list-style-type: none"> <li>• Troubled Families Grant</li> <li>• Registrars – health check review</li> <li>• DfT Integrated Transport Grant</li> </ul> |

### 3.2 Review of the 2018/19 Internal Audit Plan

3.2.1 At the end of September 2018, the Head of Assurance carried out a full half year review of the Internal Audit and Counter Fraud Plan. Required changes were reported to the Executive Director of Corporate and Customer Services (Section 151 officer) and are listed below.

| Plan Ref                 | Audit Title   | Justification for cancelling / deferring   |
|--------------------------|---|--|
| <b>Cancelled Audits:</b> |   |  |
| C1                       | Gifts & Hospitality (Members and Officers) (Monitoring Officer) | Good Assurance rating received for last three years. No system changes in current year.  |
| C11                      | Employee exit arrangements                                      | Risks will be covered to a certain extent by leavers testing in Payroll audit and C12 Employment Termination Payments review   |
| C17                      | Business Support  | Intended scope was to carry out a health check to assess whether the new structure, staffing and working practices are effective. However, the new Design Authority approved structure is not due to be fully implemented until late 2019. This will be reconsidered in 2018/19 when new service design agreed.  |
| C19                      | Organisational Design Phase 2                                   | Audit was intended to take place following the end of the Organisational Design programme, to assess whether the Council has established robust means to monitor whether the desired outcomes are achieved and is able to control further changes to structure and staffing. This will be deferred until 2020/21 |
| C20                      | Staff Performance Management                                    | From 2018/19 it is no longer mandatory for Supporting Success to be recorded and monitored using Perform and staff performance management is under review corporately. This will be reconsidered when planning for 2019/20.  |
| KF2                      | Payment Processes   | Good Assurance in 2017/18. Coverage of controls over online banking will be picked up in our Accounts Payable/Oracle Integrated Assurance audit and Treasury Management review as appropriate  |
| ICT4                     | Bring Your Own Device (BYOD)                                    | The focus of the BYOD programme at this time does not add significant risk with take up currently low.   |
| IE3                      | Waste Management  | There is currently a contractual dispute and an Internal Audit is not feasible at this time. The risks are being managed via the Strategic Risk Register.  |

|                                    |   |   |
|------------------------------------|---|---|
| IE4                                | PFI Schemes   | Commercial reviewed PFI Schemes in 2017/18, including benchmarking and outcome of review was favourable. External audit also review as part of their annual audit of the accounts.  |
| E5                                 | Education Management System Capita One                      | Good Assurance in 2017/18 - finalised in December 2017. Some enhancements made to system in current year but not expected to materially affect the risks.   |
| ASC5                               | Early Intervention and Prevention - Organisational Redesign | A number of other audits in the Plan will provide assurance in this area eg budgetary control, personal budgets, quality assurance framework. New organisational design not sufficiently embedded yet so timing would not be right for a separate audit on this. There has also been a corporate wide lessons learned process.  |
| CF2                                | Supported Independent Living                                | Not required as at the scoping of this review stage it was discovered that another review is going on in this area at present which duplicates what we were going to do and also has more resources devoted to it than we could provide.  |
| <b>Deferred to 2019/20 Audits:</b> |   |   |
| ICT5                               | Asset Management  | We are monitoring progress made implementing the most recent recommendations from the Internal Audit of Asset Management and will provide challenge when recommendations are stated by the service as implemented. Procurement for the supplier of asset management services was abandoned so they are not further forward implementing the recommendations at this time. |
| C13                                | Information Governance                                      | Last audit report was issued in June 2018 and received Adequate Assurance. The IG Team is currently going through organisational redesign.  |
| C16                                | Absence Management  | Limited Assurance in 2017/18 - final report issued in July 2018 and recommendations arising from that review are being tracked. Some implementation dates are not due until end of 2018/19 financial year.  |
| C18                                | Workforce Planning  | Deferred to 2019/20 given roll out of Corporate Workforce Strategy.   |

|     |   |   |
|-----|---|---|
| C21 | HR Business Partners advice and guidance      | Audit coverage was to assess whether there are comprehensive and clear employee relations processes for line management to follow and whether there is sufficient material / guidance / support to facilitate the effective discharge of the roles. New structure very recently implemented and has had no time to embed. Will be considered for 2019/20. |
| C23 | Project and Programme Management              | Partly covered by the savings delivery audit in 2018/19 and Adequate Assurance was given in late 2017/18.   |
| CF3 | Personal Budgets (Families) (Direct Payments) | Deferring to early next financial year as 2017/18 follow up audit was only finalised in October 2018. It was Limited Assurance and progress in implementing recommendations is being tracked via TeamCentral.   |

### 3.3 Implementation of Internal Audit Recommendations

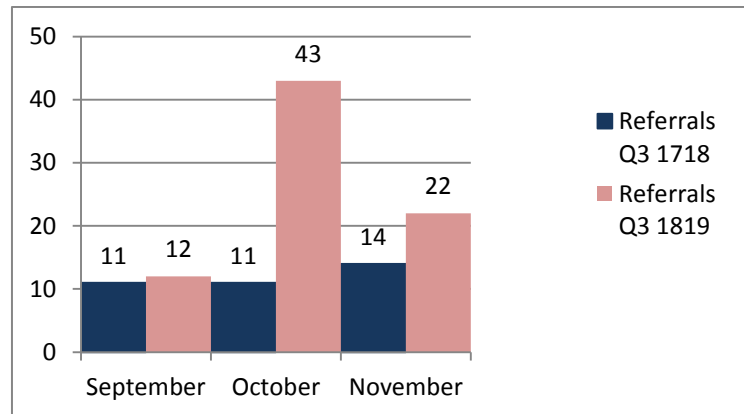
- 3.3.1 Whenever any recommendations are made in an audit report, Managers are asked to agree what activity they will undertake to address the recommendations and to agree timescales for implementation.
- 3.3.2 Progress on the implementation of recommendations is monitored by the Internal Audit service.
- 3.3.3 Critical or Major recommendations which have not been implemented within the agreed timescale are reported to the Audit, Governance and Standards Committee. Reports on outstanding recommendations are provided to Functional Leadership Teams (FLT) quarterly.
- 3.3.4 As at 21 November 2018 there were 8 Critical and 26 Major recommendations open, of which 1 Critical and 12 Major recommendations have moved beyond their latest agreed due date. See Appendix 3 for further detail.
- 3.3.5 The current assessment rationale for grading the priority of recommendations made and the level of assurance (audit opinion) for each individual audit review is attached at Appendix 1.

### 3.4 Counter Fraud Activity

- 3.4.1 The Counter Fraud Team (2.6fte) has a remit to prevent, detect and investigate fraud. In some cases we will pursue sanction through the civil or criminal courts and where possible seek to recover lost/stolen monies.

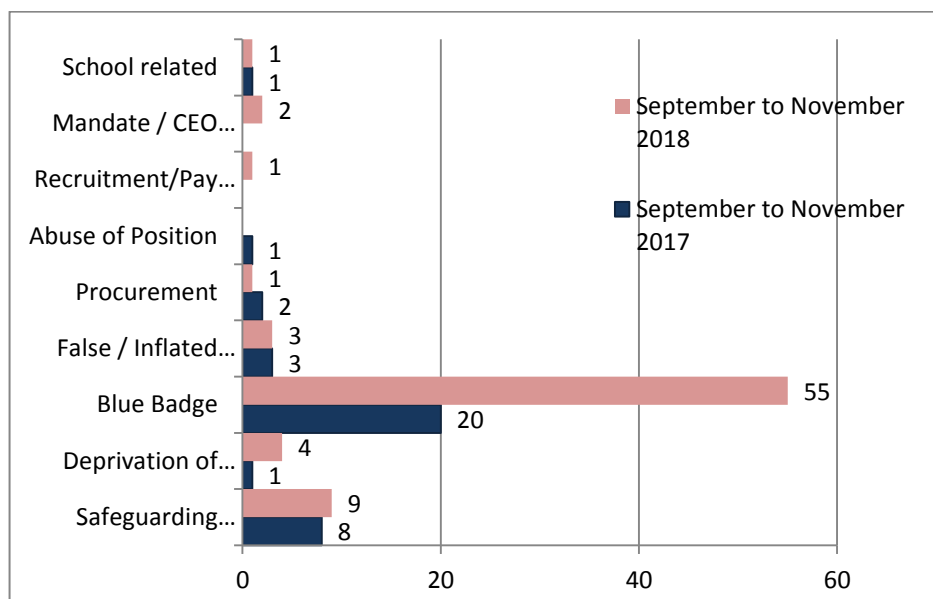
## Fraud Referrals

3.4.2 During the 3 month period 1 September to 30 November 2018, 77 fraud referrals were received (including blue badge referrals). The table below shows how this compares to the same period last year and demonstrates that the number of referrals received this year is higher than last year (36 referrals received during the same period last year). Fraud Awareness Training sessions for the Parking Enforcement Officers may account for the increase in blue badge referrals.



## Types of Referrals

3.4.3 The bar chart below demonstrates the type of referrals received, with a comparison to the referrals received last year.



## Current Themes

3.4.4. During the last quarter the Counter Fraud Team have seen an increased number of phishing and bank mandate frauds. One Essex primary school made payment to a supplier after receiving a notification that the bank details

had been changed. The payment of £81,787.80 was paid to a rogue account as the notification was fraudulent and the supplier had not changed their account details. The Counter Fraud Team is pursuing the investigation in conjunction with the ECC Financial Investigator.

Three other Essex schools have received fraudulent invoices purporting to be from Zurich for insurance cover. The issue has been reported to Action Fraud and a general notification issued to all Essex schools informing them of the scam. We have not received any reports of any payments being made to the fraudulent bank account.

### **Internal Data Matching**

3.4.5 In May 2018 the Counter Fraud team started an internal data matching exercise, focussing on Adult Social Care data. Adult Social Care payments have been recognised nationally as a significant fraud risk to local authorities who have reported significant fraud losses<sup>1</sup>. The objective of this data matching exercise is to:

- Identify and rectify duplicated packages – i.e. open domiciliary & residential care packages (where a cash payment is being made)
- Identify and stop payments that are being paid to service users who are deceased
- Identify and stop payments that are being made to service users who are in receipt of health funding (and no longer entitled to social care funding)

3.4.6 A further data matching exercise was added during Q2/3 to match recipients of ECC pensions to service users in receipt of a social care package. The aim of the match was to ensure that income had been accurately declared and recorded during the financial assessment.

3.4.7 This project is in its infancy but early results suggest that significant savings and recoveries can be realised using this approach. Investigation work is ongoing, although savings of **£57,256** were identified in quarter 1. Further data matching exercises have been completed at the end of quarter 2, with the resultant matches being investigated.

### **Essex Council Tax Data Matching Initiative**

3.4.7 The Council is supporting an Essex-wide data matching project that involves all councils providing data to ensure that income received from council tax is maximised. ECC provides data sets to support the data matching which is now undertaken on a monthly basis and the Counter Fraud Team provides support to districts in dealing with the output. Total cumulative savings recorded as at 30 November 2018 (from July 2017) are **£780,425**.

---

<sup>1</sup> <http://www.cipfa.org/services/counter-fraud-centre/fraud-and-corruption-tracker>

### **National Fraud Initiative Data Matching Exercise**

- 3.4.8 The National Fraud Initiative is a biennial exercise overseen by the Cabinet Office. This is a mandatory exercise which all public sector bodies participate in, submitting prescribed data sets to the Cabinet Office to facilitate a national data matching exercise to be completed. The Counter Fraud Team submitted all data sets to the Cabinet Office at the beginning of October 2018 and anticipates that resultant matches will be returned for investigation during January and February 2019.

### **Fraud Awareness Training**

- 3.4.9 The Council re-launched the corporate e-learning in 2017. At present, 85% of all ECC staff have completed the e-learning modules relating to:

- Anti-fraud and corruption
- Anti-bribery and money laundering.

- 3.4.10 In addition, the Counter Fraud Team have completed fraud awareness sessions for the following teams:

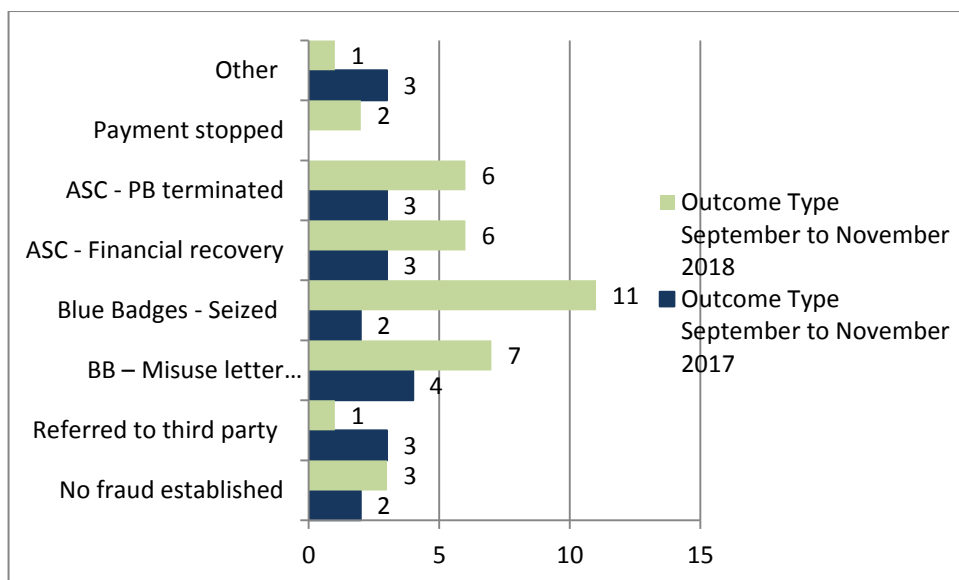
- Customer Service Centre
- Civil Enforcement Officers - ie those who enforce parking and other traffic contraventions.

### **International Fraud Awareness Week 11 – 17 November 2018**

- 3.4.11 The Counter Fraud Team promoted International Fraud Awareness week during week commencing 12 November 2018. Internal communications were posted to the intranet, and a stall with posters and leaflets was manned in the atrium at County Hall. Staff were reminded of the need to remain vigilant at all times, informed of ways to protect themselves from becoming a victim of fraud and reminded of how to report issues should they suspect fraud.

### **Outcomes**

- 3.4.12 During the period 1 September to 30 November 2018, the following outcomes and sanctions have been achieved:



### CIPFA Counter Fraud Assessment Tool

3.4.14 .The Councils counter fraud arrangements have been assessed against the CIPFA Counter Fraud Code of Practice by using the CIPFA self-assessment tool. A set of 68 statements of performance are graded to provide an overall summary of the Council's position. The assessment is divided into 5 main areas:

- Acknowledge Responsibility
- Identify Risks
- Develop a Strategy
- Provide Resources
- Take Action

The overall summary reported that: *'The organisation has reached a good level of performance against the CIPFA Code of Practice on Managing the Risk of Fraud and Corruption. This means that the organisation has put in place effective arrangements across many aspects of the counter fraud code and is taking positive action to manage its risks. The organisation is performing well against the counter fraud code and is actively working towards its resilience to fraud and to manage its fraud risks. There are some areas of weakness which could undermine resilience and these should be reviewed. In addition, the organisation should consider further opportunities to develop and extend the effectiveness of its counter fraud arrangements.'*

The 5 areas for improvement identified as a result of this assessment have been included at Appendix 4 of this report, with action points and target dates for implementation.

## **Financial Recoveries**

- 3.4.15 In addition to the savings identified during the data matching exercise, this period **£85,616** (*year to date £109,645*) was recovered related to fraud matters and a further **£26,319** (*year to date £139,490*) was identified and in the process of being recovered.
- 3.4.16 It is estimated that during the reporting period **£204,991** future losses were prevented. These mainly related to personal budgets (adult social care) which have been reduced or terminated during the year due to fraud or misrepresentation of circumstances, such as care needs have been overstated, misuse of funds, deprivation of assets. Future losses are estimated as the annual value of a personal budget (i.e. the cost to ECC if the personal budget had continued to be paid until the next social care review).
- 3.4.17 Notional savings of £8,050 (year to date £20,700) have been identified as 14 (year to date 36) expired blue badges have been taken out of circulation, each badge being attributed a value of £575 (figure determined by the Cabinet Office).

## **4. Financial Implications**

- 4.1 There are no financial implications as the Internal Audit and Counter Fraud activity 2018/19 will be met within existing resources.

## **5. Legal Implications**

- 5.1 Internal Audit is a key way in which councillors can be assured that the Council is using its resources effectively and that the Council is discharging its fiduciary duties concerning taxpayers' money. It helps services to design systems which have appropriate controls and also helps identify and respond to breaches if they occur. This report seeks to update the Audit, Governance and Standards Committee on the activities of the Council's Internal Audit and Counter Fraud service for the purposes of providing further assurance.

## **6. Equality and Diversity Implications**

- 6.1 Section 149 of the Equality Act 2010 creates the public sector equality duty which requires that when ECC makes decisions it must have regard to the need to:
- (a) Eliminate unlawful discrimination, harassment and victimisation and other behaviour prohibited by the Act
  - (b) Advance equality of opportunity between people who share a protected characteristic and those who do not

- (c) Foster good relations between people who share a protected characteristic and those who do not including tackling prejudice and promoting understanding.
- 6.2 The protected characteristics are age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, gender and sexual orientation. Equality and diversity matters have been considered in the production of the progress report.

## **7. List of Appendices**

Appendix 1 - Current assessment rationale for grading the priority of recommendations in Internal Audit reports.

Appendix 2 - Executive Summaries of 'Limited Assurance' and 'No Assurance' Internal Audit reports.





Appendix 3 – Critical and Major Recommendations which are overdue for implementation as at 13 November 2018

Appendix 4 - Summary of results against the CIPFA Counter Fraud Code of Practice.

## **8. List of Background Papers**



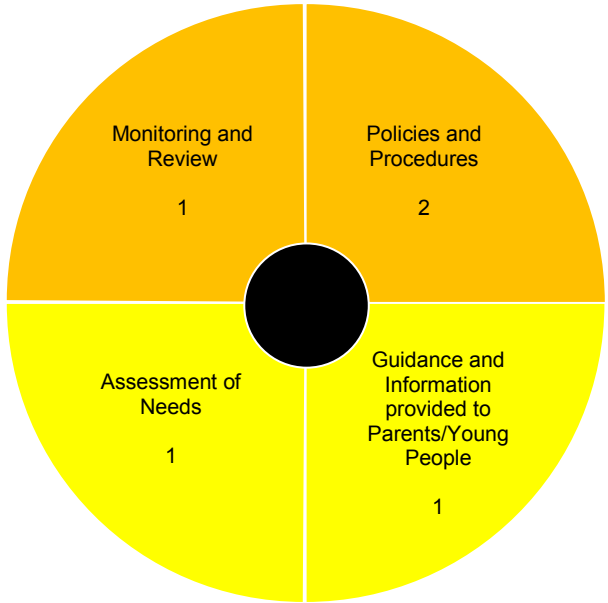




Internal Audit reports

## Internal Audit Assessment Rationale

| Risk rating  | Assessment rationale  |
|--|---|
|  Critical | <p>Critical and urgent in that failure to address the risk could lead to one or more of the following occurring:</p> <ul style="list-style-type: none"> <li>▪ Significant financial loss (through fraud, error, poor value for money)</li> <li>▪ Serious safeguarding breach</li> <li>▪ Life threatening or multiple serious injuries</li> <li>▪ Catastrophic loss of service</li> <li>▪ Failure of major projects</li> <li>▪ Critical Information loss leading to Information Commissioner's Office (ICO) referral</li> <li>▪ Reputational damage – Intense political and media scrutiny i.e. front-page headlines, television coverage.</li> <li>▪ Possible criminal, or high profile, civil action against the Council, Members or officers.</li> <li>▪ Intervention by external agencies</li> </ul> <p><b>Remedial action must be taken immediately</b></p> |
|  Major    | <p>Major in that failure to address the issue or progress the work would lead to one or more of the following occurring:</p> <ul style="list-style-type: none"> <li>▪ High financial loss (through fraud, error, poor value for money)</li> <li>▪ Safeguarding breach</li> <li>▪ Serious injuries or stressful experience requiring medical treatment, many work days lost.</li> <li>▪ Significant disruption to service (Key outcomes missed, some services compromised. Management action required to overcome medium term difficulties)</li> <li>▪ Major Information loss leading to internal investigation</li> <li>▪ Reputational damage – Unfavourable external media coverage. Noticeable impact on public opinion.</li> <li>▪ Scrutiny required by external agencies</li> </ul> <p><b>Remedial action must be taken urgently</b></p>                    |
|  Moderate | <p>Moderate in that failure to address the issue or progress the work would lead to one or more of the following occurring:</p> <ul style="list-style-type: none"> <li>▪ Medium financial loss (through fraud, error or poor value for money)</li> <li>▪ Significant short-term disruption of non-core activities</li> <li>▪ Scrutiny required by internal committees.</li> <li>▪ Injuries or stress level requiring some medical treatment, potentially some work days lost</li> <li>▪ Reputational damage – Probable limited unfavourable media coverage.</li> </ul> <p><b>Prompt specific action should be taken</b></p>   |
|  Low    | <p>Low in that failure to address the issue or progress the work would lead to one or more of the following occurring:</p> <ul style="list-style-type: none"> <li>▪ Low financial loss (through error or poor value for money)</li> <li>▪ Minor errors in systems/operations or processes requiring action or minor delay without impact on overall service delivery schedule. Handled within normal day to day routines.</li> <li>▪ Reputational damage – Internal review, unlikely to have a wider impact.</li> </ul> <p><b>Remedial action is required</b></p>   |
| Assurance Level  | Description   |
| Good   | <p><b>Good assurance</b> – there is a sound system of internal control designed to achieve the objectives of the system/process and manage the risks to achieving those objectives. Recommendations will normally only be of Low risk rating. Any Moderate recommendations would need to be mitigated by significant strengths elsewhere.</p>   |
| Adequate   | <p><b>Adequate assurance</b> – whilst there is basically a sound system of control, there are some areas of weakness, which may put the system/process objectives at risk. There are Moderate recommendations indicating weaknesses but these do not undermine the system's overall integrity. Any Critical recommendation will prevent this assessment, and any Major recommendations relating to part of the system would need to be mitigated by significant strengths elsewhere.</p>  |
| Limited  | <p><b>Limited assurance</b> – there are significant weaknesses in key areas in the systems of control, which put the system/process objectives at risk. There are Major recommendations or a number of moderate recommendations indicating significant failings. Any Critical recommendations relating to part of the system would need to be mitigated by significant strengths elsewhere.</p>   |
| No   | <p><b>No assurance</b> – internal controls are generally weak leaving the system/process open to significant error or abuse or reputational damage. There are Critical recommendations indicating major failings</p>  |


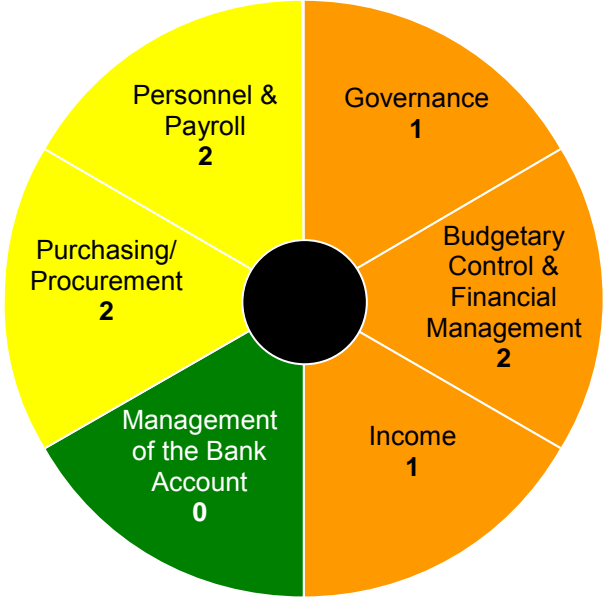




# Final Internal Audit Report 2017/18 – Personal Budgets (Families) (Direct Payments) – Follow up (C2)

## 1. Executive Summary

|  |   |  |   |  |
|--|---|--|---|--|
| <p><b>Function:</b> Children and Families<br/> <b>Audit Sponsor:</b> Helen Lincoln, Executive Director, Children, Families and Education<br/> <b>Distribution List:</b> Helen Lincoln; Russel Breyer, Director Local Delivery (South); Gaye Cole, Service Manager (Mid); Sukriti Sen, Director, Local Delivery (C&amp;F); Christina Pace, Head of Strategic Commissioning and Policy; Sue Moorhouse, Service Manager (West); James Rice, Service Manager (North); Tamsyn Basson, Service Manager (South); Caroline Tandy, Service Manager (Transitions); Tracey Kelsbie, Head of IS Service Delivery; Joel Gandy, Senior Finance Business Partner; Cllr Madden, Cabinet Member for Children and Families; Margaret Lee, Executive Director, Corporate and Customer Services; Gavin Jones, Chief Executive Officer; Cllr Finch, Leader of the Council<br/> <b>Final Report Issued:</b> 10 October 2018<br/> <b>Date of last review:</b> November 2016</p> | <p><b>Overall Opinion</b></p> <p><b>LIMITED ASSURANCE</b> </p> <hr/> <p><b>Direction of Travel</b></p> <p>Control environment has improved since our previous audit </p>  | <p><b>Number of Control Design Issues Identified</b></p> <p><b>0</b> Critical<br/> <b>2</b> Major<br/> <b>3</b> Moderate<br/> <b>0</b> Low</p> | <p><b>Number of Control Operating in Practice Issues Identified</b></p> <p><b>0</b> Critical<br/> <b>0</b> Major<br/> <b>0</b> Moderate<br/> <b>0</b> Low</p> | <p><b>Number of Recommendations</b></p> <p><b>5</b> Made<br/> <b>0</b> Rejected<br/> <b>N/A</b> Critical Rejected<br/> <b>N/A</b> Major Rejected</p> |
| <p><b>Scope of the Review and Limitations:</b></p>   | <p>This review focused on the implementation status of the recommendations agreed in the previous audit report. It therefore does not provide continued assurance on the controls in place to mitigate all the potential risks identified in our previous review.</p>   |  |   |  |
| <p><b>Critical and Major Findings and Recommendations</b></p> <p>The previous audit report issued in November 2016 gave a Limited Assurance opinion. There were three major and two moderate priority recommendations made.</p> <p>This follow-up concludes that there has been an improvement in the control environment since our prior year review and there are now two major and three moderate priority recommendations outstanding.</p> <p>The Director for Local Delivery (South) has advised that as a result of actions and work that has progressed since the audit fieldwork (carried out in early 2018) he believes that the risk ratings for the two major recommendations have reduced and that moderate ratings are now more reflective of the current risks.</p>  | <p><b>Each risk area for this review is shown as a segment of the wheel. The key to the colours on the wheel is as follows:</b></p>  <ul style="list-style-type: none"> <li> Critical priority Control Design or Control Operating in Practice issues identified</li> <li> Major priority Control Design or Control Operating in Practice issues identified</li> <li> Moderate priority Control Design or Control Operating in Practice issues identified</li> <li> No / Minor Control Design or Control Operating in Practice Issues identified</li> </ul> |  |   |  |

# Final Internal Audit Report 2018/19 – De La Salle School (E101)

## 1. Executive Summary

|   |   |   |  |
|---|---|---|--|
| <p><b>Function:</b> Education</p> <p><b>Audit Sponsor:</b> Clare Kershaw, Director , Education</p> <p><b>Distribution List:</b> Clare Kershaw; Catherine Burnett, Headteacher; Robin Marcus, Chair of IEB; Margaret Lee, Executive Director. Corporate &amp; Customer Services; Andrew Page, Head of Finance; Schools Finance Monitoring Team; Yannick Stupples-Whyley, Finance Business Partner; Lyn Wright, Head of Education &amp; Early Years; Cllr Ray Gooding, Cabinet Member for Education and Skills</p> <p><b>Final Report Issued:</b> October 2018<br/><b>Date of last review:</b> September 2011</p> | <p><b>Overall Opinion</b></p> <p><b>LIMITED ASSURANCE</b> </p> <p><b>Direction of Travel</b></p> <p>NA - the scope is not consistent with our prior audit</p>  | <p><b>Number of Issues Identified</b></p> <p><b>0</b> Critical</p> <p><b>3</b> Major</p> <p><b>5</b> Moderate</p> <p><b>0</b> Low</p> | <p><b>Number of Recommendations</b></p> <p><b>8</b> Made</p> <p><b>1</b> Rejected</p> <p><b>N/A</b> Critical Rejected</p> <p><b>1</b> Major Rejected</p> |
| <p><b>Scope of the Review and Limitations:</b></p>  | <p>The overall objectives of the audit were to ensure that an adequate control framework is in place to manage or mitigate the school's financial, fraud and governance risks. Lettings income collection processes were not tested.</p>  |   |  |
| <p><b>Critical and Major Findings and Recommendations</b></p> <p>Major priority findings and subsequent recommendations have been raised in this report, in the following areas:</p> <ul style="list-style-type: none"> <li>governance;</li> <li>financial monitoring; and</li> <li>income.</li> </ul>  | <p><b>Each risk area for this review is shown as a segment of the wheel. The key to the colours on the wheel is as follows:</b></p>  <p>  Critical priority Control Design or Control Operating in Practice issues identified<br/>  Major priority Control Design or Control Operating in Practice issues identified<br/>  Moderate priority Control Design or Control Operating in Practice issues identified<br/>  No / Minor Control Design or Control Operating in Practice Issues identified         </p> |   |  |

## Appendix 3

### Overdue Critical and Major Internal Audit Recommendations as at 21 November 2018

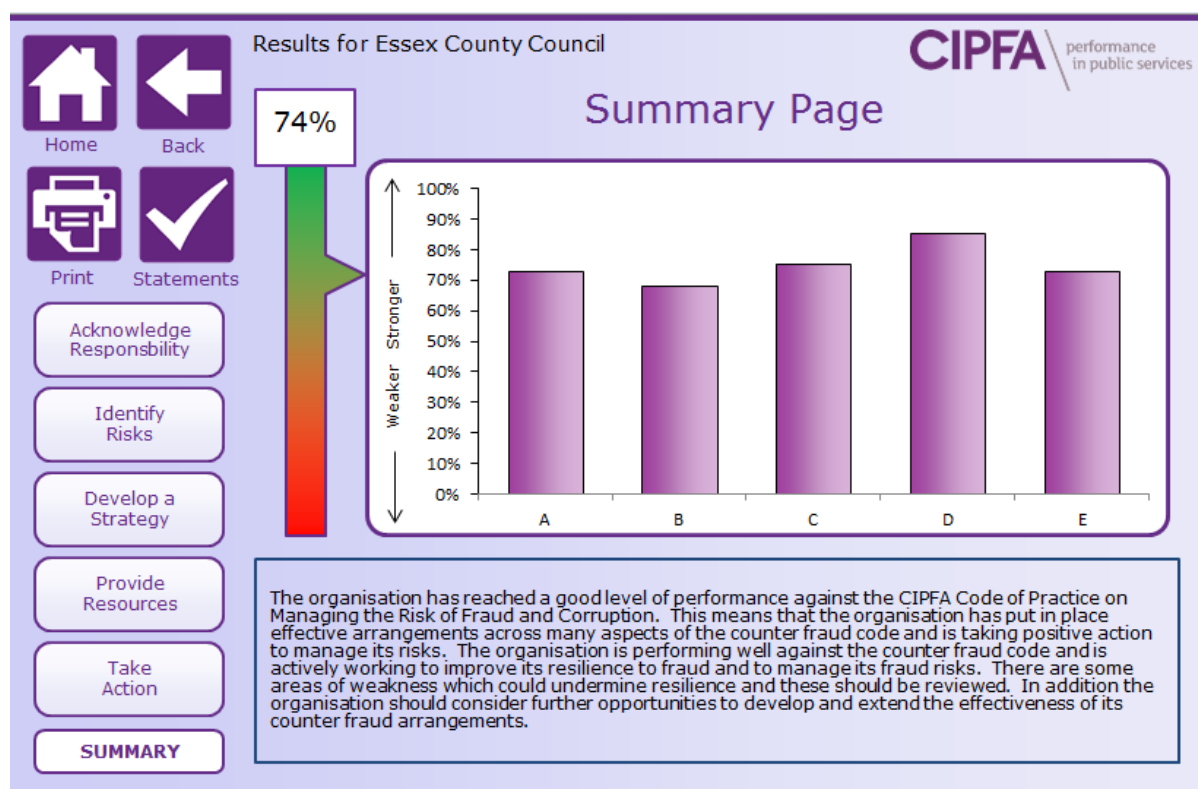
| Audit Review Title   | Function          | Recommendation  | Latest Target Date | Last Status Update  | Owner  | Rating        |
|--|-------------------|---|--------------------|---|--|---------------|
| Essex Partnership University NHS Foundation Trust (ASC16 1819) | Adult Social Care | <b>Safeguarding Referral Pathways</b><br>There is a lack of clarity surrounds the referral pathways for raising safeguarding incidents.                                 | 31/10/18           | No update provided.<br><br><b>Audit Comment:</b><br>1 monthly request to the recommendation owner for an update has been sent but none provided.  | Director, Safeguarding & Quality Assurance (ASC)       | Critical Risk |
| Continuing Healthcare Funding (ASC7 1718)                      | Adult Social Care | <b>Recording on Mosaic</b><br>Introduce quality assurance checks to ensure that relevant details are recorded on Mosaic and that an adequate case record is maintained. | 30/04/18           | <b>Update as at 7 August 2018:</b><br>Managers currently using the available quality checking tools. The development of the revised practice guidance will support timely checking and clarity about responsibilities and timeframes. Confirmation of revised process for notification to ECC of CHC funding from CCG's is due for agreement in August 2018. ECC process under development to ensure more efficient practice following CCG notification to accurate recording on the finance system.<br><br><b>Audit Comment:</b><br>A follow up Internal Audit review is currently being undertaken. | Director for Local Delivery, Adult Operations          | Major Risk    |
| Continuing Healthcare Funding (ASC7 1718)                      | Adult Social Care | <b>Progression of Checklists, Assessments and Eligibility Validation</b><br>Be transparent regarding delays in the assessment process which is variable                 | 31/05/18           | <b>Update as at 7 August 2018:</b><br>Review of practice guidance has been undertaken and a standard process has been developed to ensure workers identify potential CHC eligibility and are clear about processes for referral, timescales for decisions and where required escalation. In addition work is underway to refresh the wider S75 arrangements   | Service Manager, Adult Social Care - Quality Assurance | Major Risk    |

| Audit Review Title                        | Function              | Recommendation   | Latest Target Date | Last Status Update  | Owner  | Rating     |
|---|-----------------------|--|--------------------|---|--|------------|
|   |                       | across the quadrants and share best practice.  |                    | to ensure they are fit for purpose and reflect the new National Framework for Continuing Healthcare due for implementation later in the year.<br><br><b>Audit Comment:</b><br>A follow up Internal Audit review is currently being undertaken.  |  |            |
| Deprivation of Liberty (DoLS) (ASC6 1718) | Adult Social Care     | <b>Timeliness of DoLS Decisions</b> Best endeavours need to be made to ensure DoLS assessments and decisions are progressed promptly and issued within the statutory timescales, in a cost efficient way, having regard to the financial budget available. | 31/07/18           | <b>Update as at 22 November 2018:</b><br>Actions to be taken:<br>1. Triage system review: DoLS team are now adding the oldest historic cases to the priority list so this is now up to 2016.<br>2. Work with external agency: Allocation of 40 cases per month since to external agency since December 2017. Current progress means online with projection to complete 500 cases. Regular meetings with ECC DoLS Team and the provider.<br>3. Review of targeted use of BIA's: Frontline staff (social workers) prioritised for this years training to achieve maximum potential allocations. Due to re-organisation in ASC, some qualified staff were displaced and others moved into new roles resulting in less capacity to complete assessments. Reduced volume of re-approvals BIA's as a result.<br>4. Financial penalty: Learning agreement completed by staff on undertaking the training is now strengthened to support accountability for allocations, awaiting ALT approval. | Director, Safeguarding & Quality Assurance (Adult Social Care) | Major Risk |
| Social Media (1718 COR4)                  | Corporate Development | Approving access to and awareness of social media application use  | 30/09/18           | Portal cannot be updated in Supportworks, IG team providing individual discussions with officers. New social media team being appointed and discussions to progress 1C due.   | Communications and Marketing Manager                           | Major Risk |
| Social Media (1718 COR4)                  | Corporate Development | Security of social media accounts – password sharing.  | 31/10/18           | No update provided.<br><br><b>Audit Comment:</b><br>3 monthly requests to the recommendation owner for updates have been sent but none provided.  | Communications and Marketing Manager                           | Major Risk |

| Audit Review Title                 | Function                            | Recommendation   | Latest Target Date | Last Status Update   | Owner                                 | Rating     |
|------------------------------------|-------------------------------------|--|--------------------|--|---------------------------------------|------------|
| Absence Management (1718 COR5)     | Organisation Development and People | Completeness of return to work action.   | 30/09/18           | No update provided.<br><br><b>Audit Comment:</b><br>2 monthly requests to the recommendation owner for updates have been sent but none provided.   | Head of People Insight and Technology | Major Risk |
| Absence Management (1718 COR5)     | Organisation Development and People | Inconsistent / Incorrect Usage of Oracle (TCS).  | 30/09/18           | No update provided.<br><br><b>Audit Comment:</b><br>2 monthly requests to the recommendation owner for updates have been sent but none provided.   | Head of People Insight and Technology | Major Risk |
| Absence Management (1718 COR5)     | Organisation Development and People | Notifications to Line Managers/ Management Information on Compliance.  | 30/09/18           | No update provided.<br><br><b>Audit Comment:</b><br>2 monthly requests to the recommendation owner for updates have been sent but none provided.   | Head of People Insight and Technology | Major Risk |
| Asset Management (1718 ICT4)       | Corporate Development               | <b>Asset Register</b><br>A baseline data set is created.<br>The data is cleansed and all erroneous data removed.<br>A complete and accurate asset database is then put in place.<br>ECC's position is determined regarding the laptops which cannot be found, both in terms of any data security breach and or loss of the assets. | 31/10/18           | Baseline data - this is being established with clean data being produced as part of the Win10 roll out. This is ongoing and will be complete in July 2019. ECC position on missing assets - baseline is required from Audit to determine the parameters of our missing assets report. This will enable TS to establish the assets which require recovery. TS Management Team are standing up a 'device amnesty' to support recovery plans Security incidents to be raised as we work through the missing assets list to close out audit point effectively and stand up any new processes required as a lessons learnt. Additionally, a quarantined assets report is produced and measures are being implemented to close any open audit gaps. This will be the remit of the new Asset Manager, for which we are currently out to market. | Programme/Senior Project Manager      | Major Risk |
| Facilities Management (1718 COR15) | Infrastructure and Environment      | <b>Capacity</b><br>Report to the new line management for EPF on the team's current   | 1/11/18            | The recruitment programme is progressing and we now have 2 property and facilities officers commenced roles, 2 further recruits are identified and will commence roles in September 2018. the remaining roles are currently being advertised apart from the  | Head of Facilities Management         | Major Risk |

| Audit Review Title   | Function                            | Recommendation   | Latest Target Date | Last Status Update   | Owner                        | Rating     |
|--|-------------------------------------|--|--------------------|--|------------------------------|------------|
|  |                                     | resources to clearly articulate: <ul style="list-style-type: none"> <li>any risks this poses to delivering required facilities management tasks and the consequences of any non-delivery</li> <li>any benchmarking of in-house client-side management of similar contracts in similar organisations</li> </ul> The risk of current or foreseeable future resource capacity should either be clearly accepted or further action taken to manage the risk. |                    | apprentice role which is scheduled for January 2019  |                              |            |
| Declarations of Interests (members and officers) (1718 COR2) | Organisation Development and People | Devise a robust process to ensure consultants, interims and agency workers declarations their interests where appropriate to do so (and proportionate to risk)   | 1/10/18            | No update provided.<br><br><b>Audit Comment:</b><br>1 monthly request to the recommendation owner for an update has been sent but none provided.   | Senior Resourcing Consultant | Major Risk |
| Social Care Case Management (1718 C4)                        | Corporate and Customer              | Mosaic Compliance with General Data Protection Regulation (GDPR)   | 9/11/18            | The version of Mosaic that can hold the correct GDPR recording is not implemented. The due date is 6th Nov and at this point developments can be made to capture the required information. | Head of Democratic Services  | Major Risk |

**Appendix 4 – Summary of results re Assessment of ECC's counter fraud arrangements against the CIPFA Counter Fraud Code of Practice**

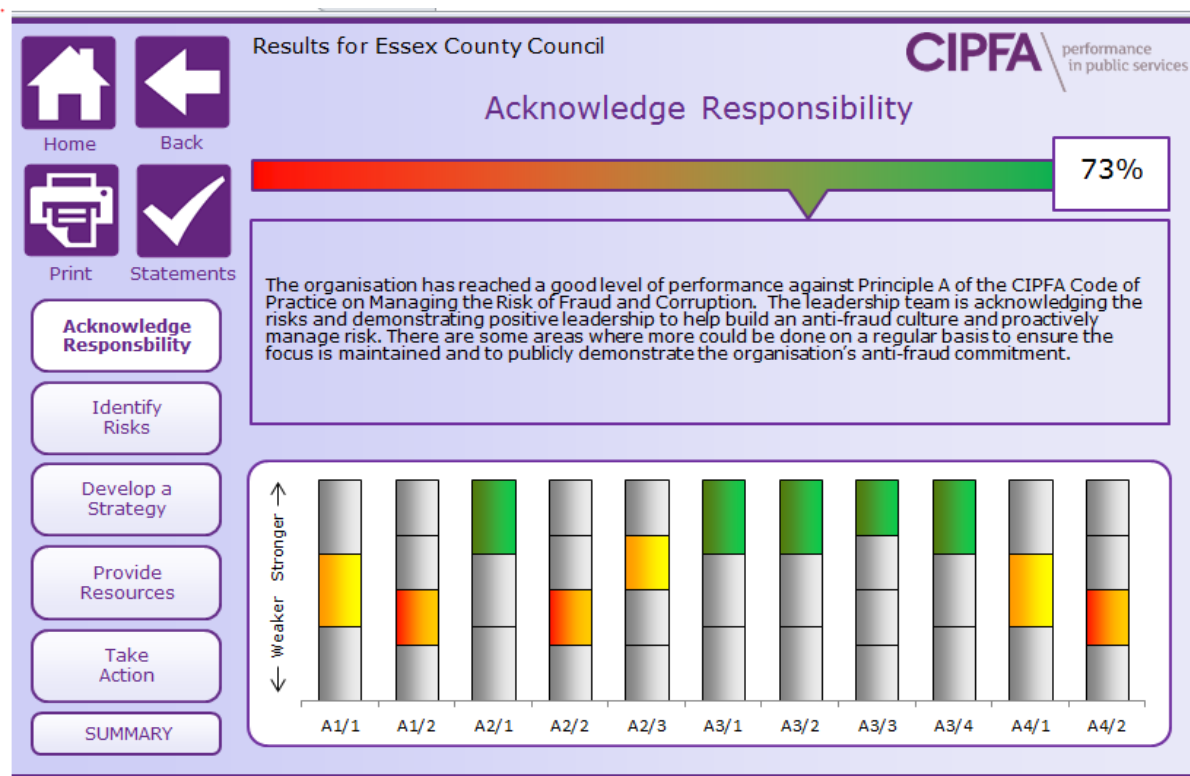


**Action Points to Address:**

| Statement  | Action to be taken and target date  |
|--|---|
| The organisation's risk management policy includes reference to risks arising from fraud & corruption and guidance on how the risks should be assessed.  | A review of the Risk Management Strategy is scheduled for 2019 and reference to fraud risks will be included. To be completed by December 2019  |
| The strategy sets out which body will have responsibility to review performance against the strategy and to make recommendations.  | The strategy states that the effectiveness of the strategy is subject to review by the Head of Assurance and the AGS Committee – need to expand this section in the strategy in order to comply with the CIPFA Code of Practice. To be completed by March 2019. |
| Internal audit reviews of counter fraud have included the availability of capacity and skills to manage fraud & corruption risks.  | Internal Audit review of Counter Fraud scheduled for 2019/20  |
| Internal audit or another independent assurance provider undertakes an independent assessment over the adequacy of the organisation's management of fraud risks, including how it identifies risks, its strategy, resources allocated and whether performance against this code has been assessed. | Internal Audit review of Counter Fraud scheduled for 2019/20  |
| There is an annual review of the effectiveness of the organisation's whistleblowing arrangements with findings reported to the audit committee.  | Reviewed by Internal Audit regularly but not on an annual basis. To consider as part of the planning process in January 2019.   |

## Areas of Assessment:

### A. Acknowledge Responsibility



#### A Acknowledge Responsibility

*The Governing Body should acknowledge its responsibility for ensuring that the risks associated with fraud & corruption are managed effectively across all parts of the organisation*

##### Statement:

A1/1 There is a current statement from the leadership team that identifies the specific threats of fraud & corruption faced by the organisation

A1/2 Statements by the leadership team on the threats of fraud and corruption include identification of the harm that could arise from the threat

A2/1 The current governance framework of the organisation includes the adoption and maintenance of effective counter fraud and anti-bribery arrangements

A2/2 The leadership team regularly refers to the importance of values and behaviours that support enhanced awareness and mitigation of fraud & corruption risks

A2/3 The leadership team publically supports steps to improve awareness of fraud & corruption risks and promote appropriate behaviours

A3/1 There is a current statement from the leadership team that acknowledges the responsibility of the team for taking action in response to the risks of fraud & corruption

A3/2 The leadership team has put in place appropriate delegated authority or has nominated an accountable person to lead on the organisation's approach

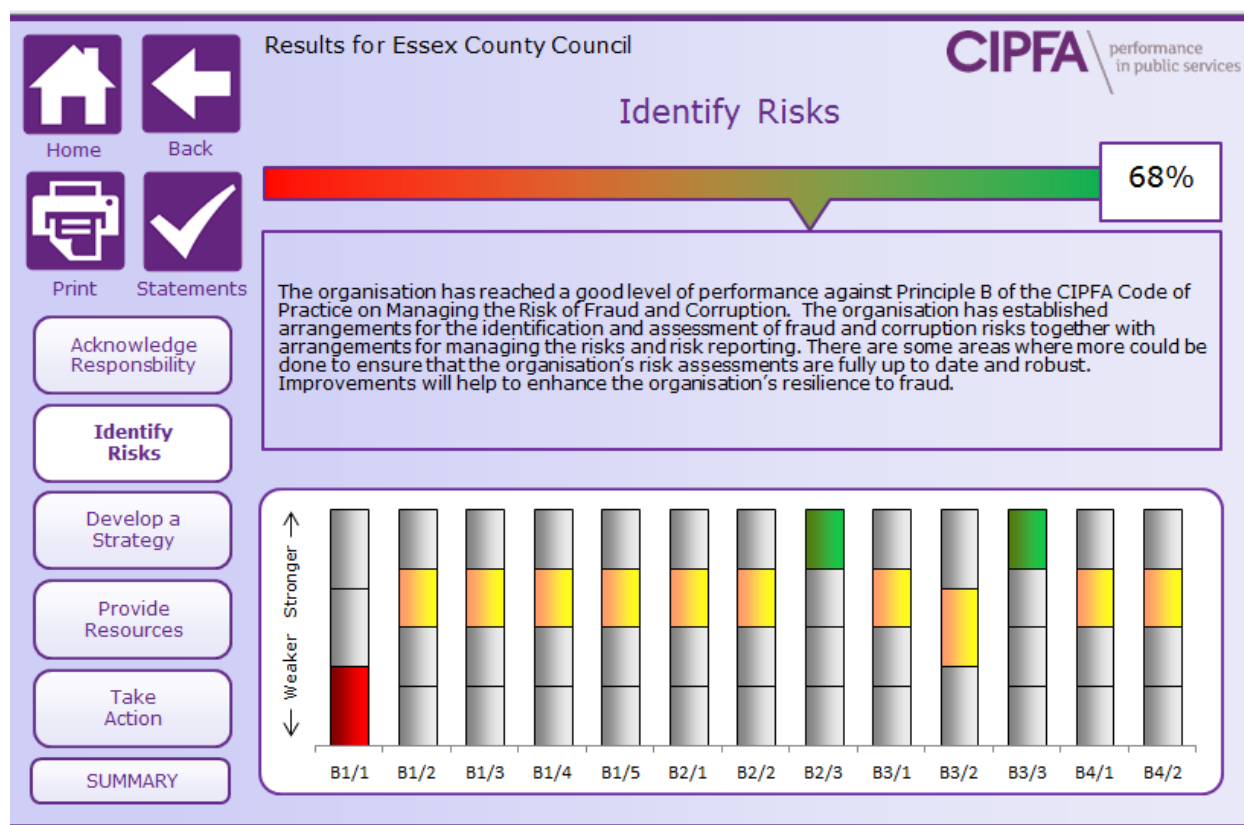
A3/3 The leadership team are supportive of the investigation of allegations and the application of sanctions where recommended

A3/4 The latest annual governance report includes an assessment of how effectively the body is addressing its fraud and corruption risks

A4/1 The governing body has approved a specific goal in relation to the resilience of the organisation to fraud and corruption

A4/2 Opportunities To improve resilience and achieve financial savings as a result of enhanced fraud detection or prevention initiatives are actively explored and supported by the leadership team

## B Identify Risks



### B Identify Risks

*Fraud risk identification is essential to understand specific exposures to risk, changing patterns in fraud and corruption threats and the potential consequences to the organisation and its service users.*

#### Statement:

B1/1 The organisation's risk management policy includes reference to risks arising from fraud and corruption and guidance on how the risks should be assessed.

B1/2 Fraud risk assessments of principal activities are undertaken

B1/3 Fraud risk assessment is undertaken for significant new operations or changes to processes

B1/4 Fraud risk reporting is made regularly and there is a clear allocation of responsibility for managing the risks

B1/5 Escalation of concerns relating to significant or increasing fraud risks are made to senior managers and those that can advise on the mitigation of the risk

B2/1 The organisation identifies the main area of activity where the risk of corruption is present

B2/2 Guidance and values on good governance values, behaviours and codes of conduct include explicit reference to counter fraud and avoidance of corruption

B2/3 Training and awareness sessions are undertaken to support the adoption of good ethical conduct by both staff and members of the governing body

B3/1 The organisation identifies appropriate fraud loss estimates that are appropriate for its sector or fraud risk types. It uses these to inform its fraud risk assessment and to quantify the value of fraud prevention

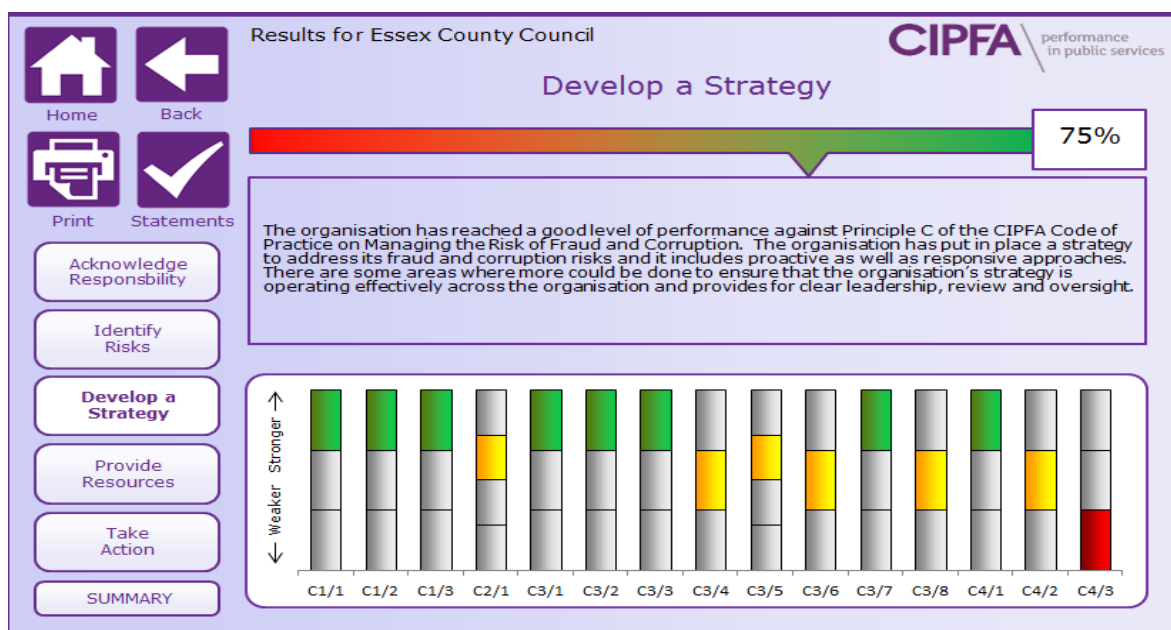
B3/2 Where the organisation has significant fraud risk exposures it adopts a methodology to measure its fraud losses

B3/3 The organisation participates in comparative or benchmarking activities with other organisations to evaluate its experience of fraud and the effectiveness of its fraud risk management

B4/1 As part of a fraud risk assessment it is made clear where the harm caused by fraud lies

B4/2 The potential harm from fraud is communicated to customers/clients/stakeholders/employees to raise awareness and to educate them that fraud is not a victimless crime

## Develop a Strategy



### C Develop a Strategy

*An organisation needs a counter fraud strategy setting out its approach to managing its risks and defining responsibilities for action*

#### Statement:

C1/1 The organisation has an up to date counter fraud and corruption strategy that has been approved by the governing body

C1/2 The strategy identifies actions to address the key fraud and corruption risks to which the organisation is exposed

C1/3 The strategy links to the overall business / operational objectives of the organisation and the overall goal of improving or maintaining resilience to fraud

C2/1 The organisation evaluates how it can best work with other organisations to address the fraud risk exposures

C3/1 The strategy includes a range of responses and actions appropriate for the organisation's risks

C3/2 The strategy sets out plans to raise and maintain awareness of the risk of fraud and corruption in the organisation amongst staff, members of the governing body and other key partners

C3/3 The strategy sets out how internal control measures will be used to prevent fraud occurring or to aid early detection

C3/4 The strategy sets out how the organisation plans to proactively detect fraud and attempted fraud or provide assurance that fraud has not taken place

C3/5 The strategy sets out how the organisation will publicise its anti-fraud and corruption activities to its staff, contractors and customers, including its commitment to tackle fraud and corruption and the outcomes of successful cases

C3/6 The strategy considers whether its whistleblowing arrangements adequately support counter fraud and corruption. Where appropriate the strategy includes actions to improve the effectiveness of its whistleblowing arrangements

C3/7 The strategy sets out the organisation's overall approach to sanctions, including the approach to prosecution of offences. Where appropriate a different approach may apply for different types of fraud

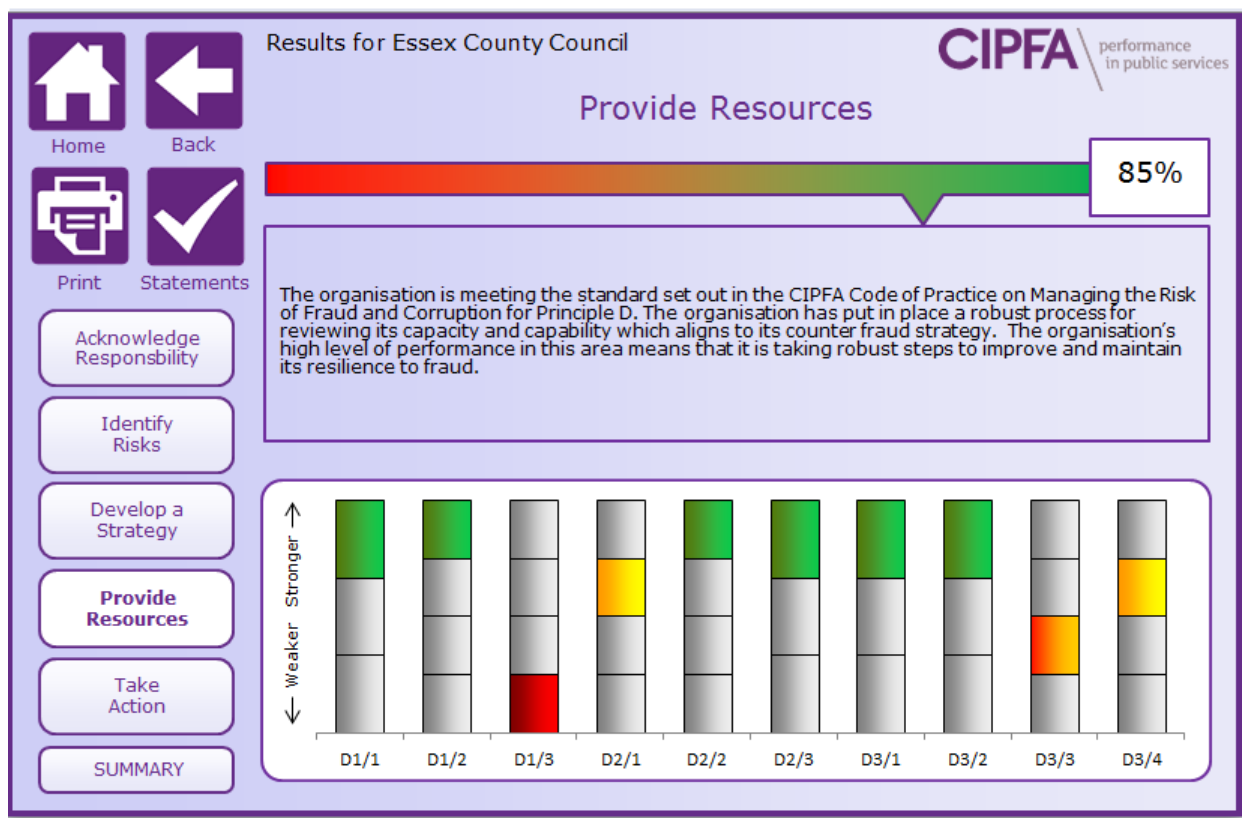
C3/9 The strategy sets out the organisation's overall approach to recovery of losses resulting from fraud, including the possibility for the recovery of expenses for the cost of investigation etc

C4/1 The strategy nominates the person with overall responsibility for implementing the strategy, plus others with significant responsibility

C4/2 The strategy sets out arrangements for accounting for the delivery of the strategy on a regular basis so that performance may be monitored and significant deviation from the strategy accounted for

C4/3 The strategy sets out which body will have responsibility to review performance against the strategy and make recommendations

## Provide Resources



### D Provide Resources

*The organisation should make arrangements for appropriate resources to support the counter fraud strategy*

#### Statement:

D1/1 The available resources are sufficient to implement the agreed counter fraud strategy and reflect the risks identified for the organisation

D1/2 The accountable person for the strategy regularly reviews the level of resources available to implement the strategy and considers whether that is appropriate for the current fraud risk profile. Reports on the conclusions are made to the audit committee or other equivalent body

D1/3 Internal audit reviews of counter fraud have included the availability of capacity and skill to manage fraud and corruption risks

D2/1 The resource planning that supports the strategy identifies the skills and experience required from the identified resources

D2/2 Staff undertaking investigation work or bought in to conduct an investigation have appropriate training in fraud investigation, including professional accreditation for investigatory work

D2/3 The organisation makes provision for training and development of in house staff that undertake any role in delivering the counter fraud strategy

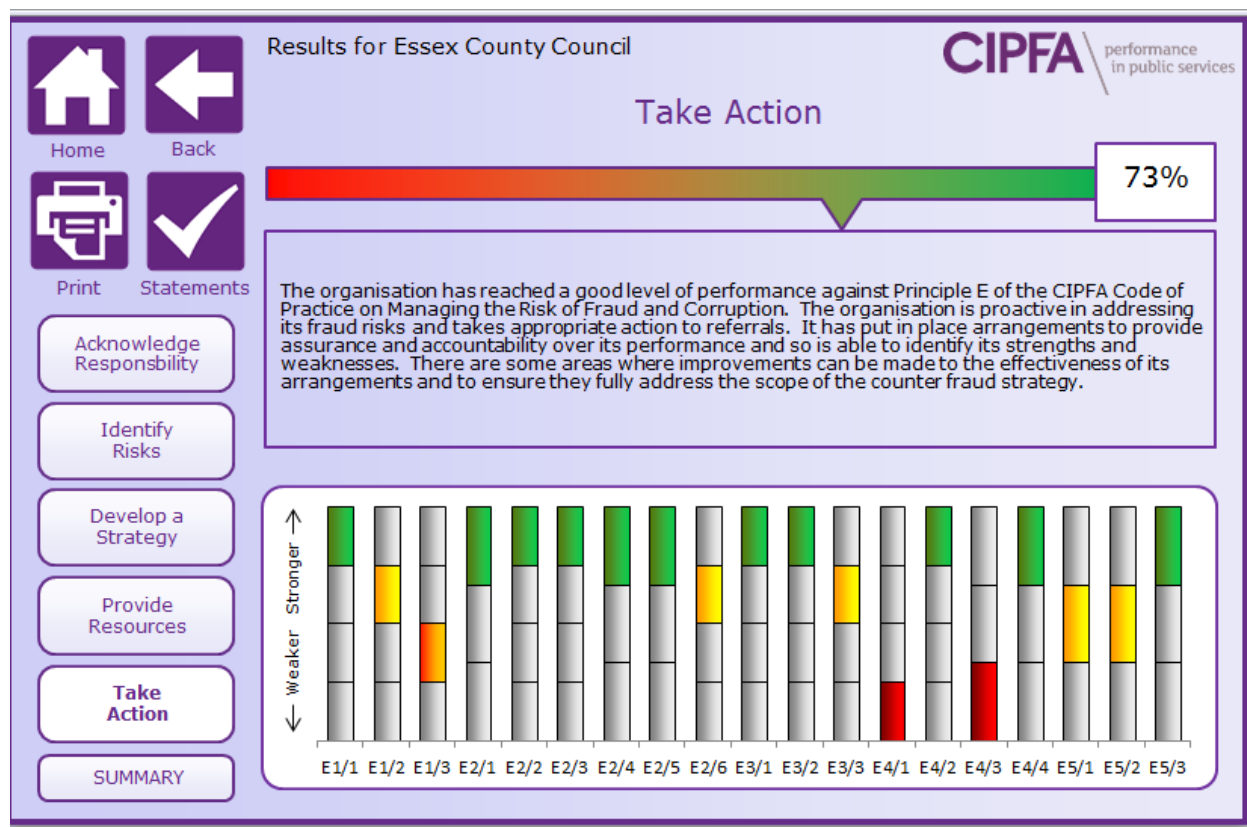
D3/1 Policies are in place to ensure that investigation staff are able to access the required information and staff to conduct the investigation. Protocols are in place to ensure that such access is proportionate and necessary

D3/2 Access rights are in place covering outsourced activities, shared services and partnership arrangements so that an investigator is able to conduct appropriate enquiries

D4/1 Where counter fraud activities are to be conducted on a collaborative basis or where there is a sharing of counter fraud resources, the organisation has agreements in place to set out the terms of the arrangement. Responsibilities are clearly identified

D4/2 Agreements are regularly reviewed and updated and reports are made to the appropriate oversight body

## Take Action



### E Take Action

*The governing body should acknowledge its responsibility for ensuring that the risks associated with fraud and corruption are managed effectively across all parts of the organisation*

#### Statement:

E1/1 The organisation has policies in place that are up to date and regularly updated for the following: Counter Fraud Policy, Whistleblowing Policy, Anti-Bribery Policy, Anti-Corruption Policy, Gifts & Hospitality Policy and register; Pecuniary Interests and Conflicts of Interest policies and register; Codes of Conduct and ethics, Information Security Policy and Cyber Security Policy

E1/2 The organisation has arrangements in place to ensure that all appropriate staff are aware of the policies and understand their responsibilities under the policies

E1/3 The effectiveness of the organisation's policies is reviewed regularly and action taken to remedy any defects / weaknesses

E2/1 Arrangements and responsibilities for undertaking an investigation of a fraud referral are in place and up to date

E2/2 Where intelligence or allegations are received action is taken to analyse the data and plan appropriate action

E2/3 Counter fraud and anti-corruption operations during the year are in accordance with those planned in the agreed strategy or reflect new, emerging risks and opportunities

E2/4 The organisation is satisfied that its performance in managing fraud and corruption risks over the years has been effective

E2/5 Investigations undertaken are considered to be effective. They comply with legislation and internal regulations, they are conducted efficiently and have resulted in clear recommendations for action

E2/6 A programme of actions is underway to prevent fraud through the application of appropriate controls and building an anti-fraud culture in the organisation

E3/1 The organisation takes part in initiatives that will help it detect or prevent fraud

E3/2 When undertaking data matching appropriate data protection notices and data sharing protocols are put in place in accordance with agreed protocols

E3/3 The effectiveness of any data sharing initiative is assessed and judged to be satisfactory

|   |
|---|
| E4/1 Internal audit or another independent assurance provider undertakes an independent assessment over the adequacy of the organisation's management of fraud risks, including how it identifies risks, its strategy, resources allocated and whether performance against this code has been assessed.   |
| E4/2 Results of internal audit or consultant reports and any recommendations are reported to the audit committee  |
| E4/3 There is an annual review of the effectiveness of the organisation's whistleblowing arrangements with findings reported to the audit committee.  |
| E4/4 Audit Committee terms of reference include review of counter fraud strategy and annual report  |
| E5/1 An annual report is prepared that covers the following: Any changes made to the strategy during the year, performance against the strategy and summary of principal actions undertaken, assessment of resources availability in the year, conclusions on whether any actions taken are effective in helping to achieve the overall goal, action plan for next year, results of an assessment of performance against the CIPFA Code |
| E5/2 The governing body receives an annual report on performance against the strategy   |
| E5/3 Taking into account the annual report and the internal audit report the organisation makes an appropriate disclosure in its annual governance report   |

|  |  |                  |
|--|--|------------------|
| <b>Report title: Regulation of Investigatory Powers Act 2000</b>   |  | <b>AGS/25/18</b> |
| <b>Report to:</b> Audit, Governance and Standards Committee  |  |                  |
| <b>Report author:</b> Paul Turner – Director, Legal and Assurance  |  |                  |
| <b>Date:</b> 11 December 2018  |  | For: Discussion  |
| <b>Enquiries to:</b> Karen Bellamy -Counter Fraud Manager email <a href="mailto:Karen.Bellamy@essex.gov.uk">Karen.Bellamy@essex.gov.uk</a> or Paul Turner – Director, Legal and Assurance <a href="mailto:paul.turner@essex.gov.uk">paul.turner@essex.gov.uk</a> |  |                  |
| <b>County Divisions affected:</b> All Essex  |  |                  |

## 1. Introduction

- 1.1 The Council has limited powers to authorise the use of ‘covert surveillance’ activity and to use ‘covert human intelligence sources’ (CHIS). These powers are quite limited (see later in the report).
- 1.2 The Council very seldom uses these powers but the fact that we have these powers means that we must have a policy about their use.
- 1.3 There have been recent changes to the law and to the statutory Code of Practice which means we must update the policy.
- 1.4 This report also updates the Committee on the recent use (or non use) of the powers.

## 2. Recommendations

- 2.1 That the updated policy at Appendix 1 be approved.
- 2.2 That the Director, Legal and Assurance continues to have delegated authority to make minor amendments amend the policy.
- 2.3 That the Committee notes that no applications for directed surveillance or the use of a CHIS have been made by anyone at ECC since the last report in March 2018.

## 3. Background

### Regulation of Investigatory Powers Act 2000

- 3.1 The Council operates many statutory services which have an element of enforcement. Most such activities are undertaken within the trading standards service, but the need for investigations may arise within the highways service and, at least in theory, within social services. All these matters may involve serious fraud or other wrongdoing.

- 3.2 As part of an investigation the Council may occasionally want to undertake surveillance or use an informant. The Regulation of Investigatory Powers Act 2000 states that these activities are always lawful if they are authorised in accordance with the Act. These activities did not previously have a statutory basis and, although there was no law against these activities, there was an argument that the lack of a statutory basis mean that there was a risk of infringing the ‘right to respect for private and family life’ – a right which is enshrined in the European Convention on Human Rights and Fundamental Freedoms.
- 3.3 The Act provides for local authorities to undertake these activities if properly authorised, and if it is necessary and proportionate to prevent or detect serious crime. Serious crime means offences which carry a maximum penalty of six months imprisonment (or underage sale of alcohol or tobacco to minors). Since 2012 the council has been required to obtain approval from a magistrate before an authorisation takes effect.
- 3.4 The Council is subject to regular inspections by the Investigatory Powers Commissioner to ensure that the Council is properly authorising activities and also to ensure that staff are aware of which activities need to be authorised and that the Council is in a state of readiness to use the powers.

### **Policy Update**

- 3.5 The Home Secretary issues statutory codes of practice on surveillance and the use of a CHIS. The codes of practice are subject to Parliamentary approval and were updated in August 2018. The Council’s Policy and Procedures on Covert Surveillance and Covert Human Intelligence Sources has been revised and updated in line with the amended Codes. The revised draft is at appendix 1.
- 3.6 The main revisions to the policy include:
- Authorisation periods for juvenile sources increased from one month to four months – to reflect a change in the law;
  - The Councils use of investigatory powers is now regulated by the Investigatory Powers Commissioner’s Office (IPCO) and not the Office of Surveillance of Commissioners (OSC);
  - Senior Responsible Officer’s duties updated to include the oversight and reporting of errors to the IPCO;
  - Paragraph inserted regarding the use of agents by public authorities;
  - Updated section on surveillance etc by monitoring social media postings;
  - Updated section on authorisations and central register logging requirements;
  - Additional paragraphs on errors since there is now a greater emphasis on noting and reporting errors to IPCO.

## **The Council's Surveillance Activity/use of CHIS**

- 3.7 The Council does not generally undertake surveillance or use CHISs which needs to be authorised under the Act. The last written report to the committee was made in March 2018, when a report that no authorisations had been sought or granted during the previous year. Similarly, between March 2018 and 30 November 2018 no authorisations have been sought or granted by ECC.
- 3.8 The Council has worked with the police on joint operations. In these cases the Police would be the lead organisation and would normally obtain the authorisation. In these cases Council officers satisfy themselves that they are covered by an authorisation issued by the Police.
- 3.9 The Council takes the view that the 'test purchasing' activities it undertakes by sending a minor to shops to purchase alcohol or tobacco do not need to be authorised under RIPA. This is because the activities take place in a public place and are undertaken overtly. This view has not been tested in court and some authorities take a more cautious approach.
- 3.10 The Council provides regular training to staff who may need to undertake enforcement activities to ensure that they are aware what needs to be authorised.

## **4. Financial Implications**

- 4.1 Use of RIPA has no financial implications

## **5 Legal Implications**

- 5.1 The legal implications of RIPA are set out in section 3 of this report. The Council may have to pay damages if interferes with someone's right to respect for their family and private life without such interference being authorised under RIPA. However, the risk of this is very low if we

## **6 Equality and Diversity Implications**

- 6.1 Section 149 of the Equality Act 2010 creates the public sector equality duty which requires that when ECC makes decisions it must have regard to the need to:
- (a) Eliminate unlawful discrimination, harassment and victimisation and other behaviour prohibited by the Act
  - (b) Advance equality of opportunity between people who share a protected characteristic and those who do not

- (c) Foster good relations between people who share a protected characteristic and those who do not including tackling prejudice and promoting understanding.

6.2 The protected characteristics are age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, gender and sexual orientation. Equality and diversity matters have been considered in the production of this report.

## **7 List of Appendices**

Appendix 1 – Updated Policy on the Use of the Regulation of Investigatory Powers Act 2000 on the undertaking of Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS).

## **8 List of Background Papers**

Covert surveillance and property interference Code of Practice, dated August 2018

Covert human intelligence sources Code of Practice, dated August 2018

## Essex County Council

# POLICY AND PROCEDURES ON COVERT SURVEILLANCE AND THE COVERT HUMAN INTELLIGENCE SOURCES

### Executive Summary

This document sets out Essex County Council's policy and procedures about the use of covert surveillance and using Covert Human Intelligence Sources (informant or undercover officer). It applies to all parts of the Council.

Some activities need to be authorised under the Regulation of Investigatory Powers Act 2000 (broadly, these are investigations into alleged criminal offences).

Sometimes, for example in HR investigations, the Council will want to undertake these activities when it is not possible to authorise the activities under RIPA. This policy also deals with these activities.

**ALL** Covert Surveillance or use of a Covert Human Intelligence Source must be authorised by an authorising officer. Any authorisation granted under RIPA must additionally be approved by a Magistrate. All authorisations and refused applications must be recorded in the ECC central register which is held within Internal Audit. There is also a short 'Guidance Note for Officers' about RIPA and a separate policy covering acquiring of communications data.

### Policy

#### 1. Background

- 1.1 In order to carry out its statutory responsibilities, the Council sometimes needs to carry out investigations. Investigations may sometimes need covert surveillance or covert human intelligence sources to be used.
- 1.2 As a public authority the Council must respect people's human rights as set out in the European Convention on Human Rights. Article 8 of the Convention requires the state to respect people's private and family life. This is not an absolute right. The state can interfere with this right in order to prevent or detect crime or disorder. Any such interference has to be in accordance with the law.
- 1.3 The Regulation of Investigatory Powers Act 2000 provides a legal framework which allows the Council to undertake:
  - the acquisition of communications data (e.g. billing data);
  - non-intensive covert surveillance in the course of specific operations;
  - the use of covert human intelligence sources (agents, informants, undercover officials).
- 1.4 The Act sets out a legal process. If the process is followed, these activities are 'in accordance with the law'. The Council's use of investigatory powers is regulated by the Investigatory Powers Commissioners Office (IPCO).

- 1.5 There is a separate policy document in ECC which relates to acquisition of communications data.

## 2. Record Keeping

- 2.1 Record keeping is important to demonstrate compliance with RIPA. Each service maintains a local record. A central record is maintained by the Monitoring Officer.
- 2.2 The Council also maintains a central record of technical equipment used for directed surveillance.

## 3. Codes of Practice

- 3.1 The Secretary of State has issued Codes of Practice for directed surveillance and the use of CHIS.
- 3.2 More about the legislation and the codes of practice are to be found on gov.uk at this [link](#)

## 4. Roles

- 4.1 This policy defines four roles in the authorisation process.
- 4.2 **Applicants:** Anyone may apply for a RIPA or non RIPA authorisation.
- 4.3 **Authorising Officers:** Authorisations may be approved only by those named at appendix 1. Once approved the application must then be approved by a Magistrate.
- 4.4 **Senior Responsible Officer** ('SRO') who is responsible for compliance, the integrity and management of the process to minimize the risk of errors, including oversight and reporting of any errors to the IPCO, and liaison with the Commissioner. The Senior Responsible Officer is the Director, Legal and Assurance.
- 4.5 **Co-ordinating Officer:** Responsible for maintaining the central record on behalf of the SRO. The Co-ordinating officer is the Counter-fraud Manager.

## 5. Joint Working and use of Contractors

- 5.1 Where the Council works jointly with another investigating agency, either organisation may obtain RIPA authorisations. The lead organisation must ensure that RIPA compliance has been secured.
- 5.2 In some circumstances it may be appropriate or necessary for the Council to work with third parties who are not public authorities (such as a non-governmental organisation, company, individual or private detective). Where that third party is working in partnership or under the direction of the Council then they are working as an agent of the Council. Any act that the third party conducts should be considered for authorisation, particularly if the Council wishes to make use of any material obtained.
- 5.3 Anyone working on the investigation must see a copy of the authorisation (or at least the relevant parts of it) so that they know what has been authorised.

- 54 Where ECC staff undertake activities authorised by an authorisation which wasn't granted by the Council, a copy of the authority of the other agency must be retained and recorded on ECC's central register.

## **6. Surveillance Board**

- 6.1 The Surveillance Board is chaired by the Senior Responsible Officer and there are representatives from all directorates. The Surveillance Board has the following terms of reference:
1. To have oversight of appropriate arrangements for authorising and carrying out surveillance including covert directed surveillance, use of covert human information sources, prosecutions relating to recovery of proceeds of crime and use of cctv/ vehicle number plate recognition cameras.
  2. To review the following policy as required and at least annually: Operational Policy and Procedural Guidance on the Use of Covert Surveillance and the Use of Covert Human Intelligence Sources.
  3. To react to reports or audits that relate to surveillance and to ensure that recommendations of the Office of Surveillance Commissioners are implemented.
  4. To ensure that a training programme is in place for officers involved in surveillance.
  5. To ensure that officers who need to be are aware of the existence of the policy and are able to access it.
  6. To monitor that the Council keeps accurate and up to date records as required.
  7. To report to Audit, Governance and Standards Committee annually with statistics and to ensure that the Audit, Governance and Standards Committee reviews the surveillance policy at least annually.

## **7. Member Involvement**

- 7.1 The Code of Practice recommends that members are involved in review of this policy at least annually, and that statistical information about RIPA authorisation is provided to members at least quarterly. At Essex the Audit, Governance and Standards Committee has oversight of this issue. The Co-ordinating Officer is responsible for reporting to the committee in relation to the annual review and provision of statistics.

## **8. Use of material as evidence in court proceedings**

- 8.1 Subject to the usual rules of evidence, material obtained through covert surveillance (or through a CHIS) may be used as evidence.
- 8.2 Material obtained through surveillance or the use of a CHIS is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996. There are legal procedures which can protect the identity of a CHIS from disclosure.

## **9. Covert surveillance of Employees etc outside RIPA**

- 9.1 The Investigatory Powers Tribunal<sup>1</sup> has decided that RIPA authorisations may only be granted when an organisation is carrying out its core functions, and not when it

---

<sup>1</sup> C and (1) THE POLICE (2) HOME SECRETARY  
DEPARTMENT 14 November 2006 No: IPT/03/32/H

is acting as employer. However, surveillance of employees may still potentially be viewed as infringing their article 8 rights.

- 9.2 Where surveillance relating to a matter which is either not an offence or where prosecution does not form part of the Council's core business is required, officers are required to complete the appropriate form (headed 'Non-RIPA Authorisation') and seek appropriate internal authorisation. One example of this would be if the Council seeks to undertake surveillance on employees as part of a disciplinary case. Non-RIPA authorisations will last for 3 months and appropriate action must be taken to review, renew and cancel authorisations.
- 9.3 The authorising officers will apply the same tests of necessity and proportionality for non-RIPA authorisations as would apply to RIPA authorisations.
- 9.4 Magistrates have no role in approval of 'non-RIPA' activities.
- 9.5 Once internally authorised, a signed copy of the authorised form and subsequent review, renewal and cancellation forms must be kept secure with the investigation file and with the central record maintained by the Co-ordinating Officer.

## 10. Forms

- 10.1 The Council has adopted Home Office forms. These are available on the Internet at this [link](#) 10.2. Forms for 'non RIPA' authorisations (e.g. HR investigations) are available on the intranet.

## Essex Procedures and Complying with Codes of Practice.

This part of the document is divided into two sections.

Section A is concerned with directed covert surveillance, including intrusive surveillance, Section B with the use and conduct of covert human intelligence sources.

### Section A - Covert Surveillance

## 11. Surveillance definitions and when RIPA authority can be granted.

**What is meant by 'covert surveillance', 'directed surveillance' and 'intrusive surveillance'?**

- 11.1 **Surveillance** includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications.
- 11.2 **Covert surveillance** is any surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place (section 26(9)(a)).
- 11.3 **Directed surveillance** is surveillance which is covert, but not intrusive, and undertaken for the purposes of a specific investigation or specific operation; in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation) (section 26(2)).

- 11.4 The Council can only use RIPA authorised surveillance for the detection or

prevention of 'serious crime'. This means offences which carry a maximum sentence of at least 6 months imprisonment or relate to the sale of alcohol or tobacco to children.

- 11.5 Surveillance which is an immediate response to events is outside the provisions of RIPA. There is no requirement to follow the RIPA procedures in these circumstances.
- 11.6 **Intrusive surveillance** is surveillance which takes place on residential premises or in private vehicles. The Council **cannot** authorise the use of 'intrusive surveillance'. Where such activity is considered necessary to prevent or detect a crime, the matter should be referred to the Police.
- 11.7 General observations form part of the duties of many law enforcement officers within public bodies. For example, Trading Standards officers may covertly observe and then visit a shop as part of their enforcement function. They may observe goods or services being supplied. Such observation may involve the use of equipment to reinforce normal sensory perception such as binoculars or cameras. Such activity forms part of the everyday function of law enforcement officers within public bodies. This is considered to be low-level activity, which will not usually be regulated under RIPA. Similarly, plain clothes operations, even if targeted at a particular area, are not directed surveillance and are not required to be authorised.
- 11.8 If one or more particular individuals are being targeted as part of an operation, and private information about them is likely to be obtained during the operation, then RIPA authority should be obtained.

### **Use of Public CCTV Systems**

- 11.9 General use of public space CCTV systems is overt and therefore not covered by RIPA. If one or more CCTV cameras are targeted on an individual then this may be directed surveillance which must be authorised under RIPA.

### **Social Media and Internet Based Research**

- 11.10 Reading someone's public postings on social media may not feel like an interference with someone's human rights. However, the compilation of a file information on somebody by the state has been held to be an interference with the human right to respect for privacy.
- 11.11 The law is the same for any collating any information about individuals. Viewing social media postings which are available to the public is the same as cutting an article out of a newspaper or putting other information on a file.
- 11.12 Any such activity needs to be 'in accordance with the law'. Any building up of information on a file about someone needs to be undertaken in accordance with the General Data Protection Regulation and the Data Protection Act 2018.
- 11.13 However, RIPA applies only where the Council undertakes activities which are covert – ie they are intentionally undertaken in such a way that the subject doesn't know it is taking place, and the activity is likely to result in the obtaining of private information. When viewing open postings on social media, you must not do so in a covert way unless it is authorised by RIPA. Repeated viewing of a social media profile could amount to covert surveillance. If undertaken covertly and it is wise to

keep this to a minimum.

- 11.14 It would normally be covert to form a formal online 'friendship' to view closed information (eg follow someone who protects their tweets or view a facebook profile which is not public). Any use of this must be carefully considered as this could amount to directed surveillance or the use of a 'covert human intelligence source' which would need to be authorised under RIPA.
- 11.15 If you are intending to make social media checks then you should consider notifying the subject first. . You do not have to do this if it would prejudice prevention or detection of crime to do so. If you have notified someone that you will be making checks then the viewing of social media is not covert and does not need to be authorized.
- 11.16 As with any personal data held by the Council we need to ensure that we comply with the General Data Protection Regulation and Data Protection Act 2018. That is beyond the remit of this policy but advice is available from Information Governance or Essex Legal Services .
- 11.17 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 include:
- Whether the investigation or research is directed towards an individual or organisation;
  - Whether it is likely to result in obtaining private information (see above for more information about private information) about a person or group of people;
  - Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile as part of a covert operation;
  - 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.

## **12. Obtaining Authority for Directed Surveillance**

- 12.1 An applicant must complete the application and submit it to an authorising officer. The form must be carefully completed and should not use standard wording in the boxes of the form. The authorising officer must consider the application and, if they

grant the authorisation they must use their own words to explain their decision and say what is authorised. They must ensure that the activity is necessary and proportionate and define the parameters of the permitted activity. Even when the authorising officer has approved the authorisation, the authorisation does not take effect unless and until it is approved by a Magistrate.

- 12.2 The proposed surveillance must be planned in connection with an investigation for one of the Council's core statutory functions (eg trading standards).
- 12.3 A written application for authorisation for directed surveillance should describe any conduct to be authorised and the purpose of the investigation or operation. The application should be fair and balanced and include:
- the reasons why the authorisation is necessary in the particular case for the purpose of preventing or detecting a serious crime (or other reason may be possible in relation to a 'non RIPA' authorisation)
  - the reasons why the surveillance is considered proportionate to what it seeks to achieve;
  - the nature of the surveillance, including automated online search engines (the extent and limitations should be considered and detailed);
  - the identities, where known, of those to be the subject of the surveillance;
  - an explanation of the information which it is desired to obtain as a result of the surveillance;
  - an assessment of the risk of collateral intrusion and details of the measures taken to minimize the risk;
  - the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
  - the level of authority required (or recommended where that is different) for the surveillance; and
  - a subsequent record of whether authority was given or refused, by whom and the time and date.
- 12.4 All authorisations must be issued in writing. All reasonable efforts should be made to take account of information which supports or weakens the case for authorisation.
- 12.5 Once an authorisation is approved, the authorisation must be referred to a Magistrate for approval (except for non-RIPA authorisations - which should not be referred to the Magistrate).
- 12.6 An application for approval by a Magistrate will be made:
- (a) by an officer approved by the Trading Standards Manager or
  - (b) by an officer approved by the SRO
- If the Magistrate does not approve the authorisation at the first hearing then, in all cases, the SRO must be informed as a matter of urgency.
- In all cases the SRO must be informed of the date and time of the magistrates' decision and provide details of the hearing for the central record – see paragraph 17.2.
- 12.7 A flowchart explaining the Magistrate Approval process is at this [link](#)
- 12.8 A record of the Magistrate's Decision must be sent to the Co-ordinating Officer.

### **13. Necessity and Proportionality**

- 13.1 The Council can only use RIPA powers if it is necessary and proportionate to do so.
- 13.2 The applicant must explain why they believe the proposed activities are necessary and proportionate. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it, against the need for the activity. It will always involve explaining why this is the least intrusive way possible, and presented in a fair and balanced way.
- 13.3 The activity will not be proportionate if the information which is sought could reasonably be obtained by other less intrusive means or if the intrusion is significant compared to the matter being investigated.

### **14. Collateral Intrusion**

- 14.1 Collateral intrusion refers to activities where information is obtained about people other than those who are directly the subject of the investigation or operation. The risk of collateral intrusion must be assessed as part of proportionality. Wherever practical, measures should be taken to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.
- 14.2 Those carrying out the surveillance should inform the authorising officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. When the original authorisation may not be sufficient, consideration should be given to whether the authorisation needs to be amended and re-authorised or a new authorisation is required.
- 14.3 Before making an application the applicant should consider whether there are particular sensitivities in the local community where the surveillance is taking place which should influence the grant.

### **15. Confidential Information**

- 15.1 The RIPA code of practice suggests that particular care should be taken in cases 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 material. ECC officers are unlikely to come into possession of information of this nature, but need to be alert to the correct procedures should such a situation arise.
- 15.2 If it is likely that confidential information will be acquired, the use of surveillance must be authorised by the Chief Executive or in his absence the Monitoring Officer.
- 15.3 Legally privileged information is confidential information. It is unlikely that surveillance will result in legally privileged information being obtained. Any such information is extremely unlikely ever to be admissible as evidence in criminal proceedings and the Council would not seek to acquire such material.
- 15.4 An application for surveillance likely to result in the acquisition of legally privileged information should only be made in exceptional and compelling circumstances.

## 16. Combined authorisations

- 16.1 The Code of Practice states that a single authorisation may combine two or more different RIPA authorisations. For example, a single authorisation may combine authorisations for directed surveillance and the conduct of a CHIS. In such cases the provisions applicable to each of the authorisations must be considered separately. However as the application forms would need to be separately completed and the criteria involved in both is different, it is recommended that the authorisations are considered separately. Authorisations covering directed surveillance at multiple sites (eg undertaking surveillance of a number of premises as part of test purchasing operations) are appropriate.

## 17. Central Record

- 17.1 In accordance with the codes of practice the Council keeps a centrally retrievable record of all authorisations which is regularly updated whenever an authorisation is refused, granted, renewed or cancelled. These records will be retained for a period of at least three years from the ending of the authorisation.

- 17.2 The following information will be kept on the central record: -

- the type of authorisation
- the time and date the authorisation was given or refused and the date upon which it was notified and approved by a magistrate;
- name and rank/grade of the authorising officer;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- details of the attendances at the Magistrates' court, to include the date of attendance, the determining magistrate, the decision of the court and the time and date of the decision;
- the dates of any reviews;
- dates of any renewals and the name and rank/grade of the authorising officer;
- the result of periodic reviews of the authorisation;
- whether the investigation or operation is likely to result in obtaining confidential information as defined in the code of practice;
- whether the authorisation was granted by an individual directly involved in the investigation;
- the date the authorisation was cancelled;
- a record of all Magistrate decisions, including reasons for any refusals, where applicable and details of any appeal to the Investigatory Powers Commissioner.

- 17.3 The following documents will be kept with the central record:

- a copy of the application and a copy of the authorisation 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 the supporting documentation submitted when the renewal was requested;
- date and time when any instructions were given by the authorising officer

- Magistrate decisions;
- the date and time when any instruction to cease surveillance was given.

17.4 The Co-ordinating Officer maintains records on behalf of the Senior Responsible Officer.

17.5 A central record is also kept of the technical equipment used by the Council for covert surveillance. Any officers or services making use of equipment for covert surveillance should ensure that details are passed to the Co-ordinating officer to be added to the register.

## 18. Duration of Authorisations

18.1 A written authorisation granted by an authorising officer and approved by a Magistrate will cease to have effect (unless renewed) at the end of a period of **three months** beginning with the date of approval by the Magistrate.

18.2 Surveillance must only be undertaken in accordance with the terms of the authorisation. If anyone concerned in the operation is concerned that there may be an error which has resulted in unauthorised directed surveillance taking place

## 19. Reviews

19.1 The authorising officer will specify a frequency of reviews when they complete the authorisation. It is suggested that this is monthly but the frequency will depend on the circumstances. The relevant review form must be completed on each occasion and a copy sent to the Co-ordinating Officer. The review must be signed by an authorising officer but does not need to be approved by a Magistrate. The results of the review must be retained for at least 3 years.

## 20. Renewals

20.1 If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, he may renew it in writing for a further period of **three months**.

20.2 Renewals must be approved by a Magistrate using the same procedure as the original authorisation.

20.3 A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person who is entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

20.4 Applications for the renewal of an authorisation for directed surveillance should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the circumstances or information detailed in the initial application;
- the reasons why it is necessary to continue with the directed surveillance;

- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- whether any privileged material or confidential information was obtained as a result of the activity undertaken under the authorisation;
- the results of regular reviews of the investigation or operation.

20.5 Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations. All renewals must be approved by a Magistrate.

## **21. Cancellations**

- 21.1 The authorisation must be kept under review and be cancelled by an authorising officer (usually the officer who granted or last renewed it) if the criteria upon which it was authorised are no longer met or if the authorisation is no longer required.
- 21.2 As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be recorded in the central record of and the notification of cancellation where relevant.

## **22. Errors**

- 22.1 The Council expects authorising officers to carefully applications before approving them and any application is reviewed by the person presenting the application to a Magistrate, reducing the risk of errors. However, all 'relevant errors' must be reported to the Investigatory Powers Commissioner as soon as reasonably practicable, but no later than 10 working days after it has been established that a relevant error has occurred. The report should include as much detail regarding how the error occurred, the impact of the error and what steps are being taken to prevent any recurrence
- 22.2 A relevant errors is any error by a public authority in complying with any requirements that are imposed on it by any enactment which are subject to review by a Commissioner. These include the following:
- Activity has taken place without lawful authorisation;
  - There has been a failure to adhere to the safeguards regarding the handling of any material gained under a statutory authorisation.
- 22.3 Section 231 of the 2016 Act requires the Investigatory Powers Commissioner to inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious nature and it is in the public interest for the person concerned to be informed of the error.
- 22.4 In deciding whether it is in the public interest for the person concerned to be informed of the error, the Commissioner must consider:
- The seriousness of the error and its effect on the person concerned
  - The extent to which disclosing the error would be contrary to the public interest or prejudicial to:
    - National security
    - The prevention or detection of serious crime
    - The economic well-being of the UK; or
    - The continued discharge of the functions of any of the intelligence services.

- 22.5 If it identified that an error **may** have occurred the Senior Responsible Officer must be informed immediately by email or telephone. The Senior Responsible Officer will ensure that prompt action is taken to establish what has occurred and whether or not this is an error which must be reported to the Commissioner. A record will be made of any decision taken and the reasons for it,

### **23. Retention and destruction of the product**

- 23.1 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained securely. The Criminal Procedure and Investigations Act 1996 requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.
- 23.2 There is nothing in RIPA that prevents material obtained from properly authorised surveillance from being used in other investigations.
- 23.3 Officers must ensure that arrangements are in place for the handling, secure storage and destruction of material obtained through the use of covert surveillance. Authorising officers must ensure compliance with the appropriate data protection requirements.

## **Guidance on Use of Covert Human Intelligence Sources and RIPA**

### **24. What is a Covert Human Intelligence Source?**

- 24.1 A person is a covert human intelligence source ('CHIS') if he or she establishes or maintains a personal or other relationship for the covert purpose of obtaining information or to provide access to any information to any other person or he or she secretly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship. A CHIS may be an informant - or an officer working undercover.
- 24.2 Officers should be aware that there is a risk of someone becoming a CHIS if they give the Council information on more than one occasion if that information comes from a relationship they are maintaining if it can be said that they are partly maintaining the relationship for a covert purpose.
- 24.3 This can happen almost by inadvertence. If someone becomes a CHIS then use of this policy should be considered.

### **25. When may the Council use a CHIS?**

- 25.1 There may be occasions when it is appropriate for an ECC officer to be authorised as a CHIS. However, should the use of a third party, non-ECC officer CHIS become necessary to ensure effective law enforcement, appropriate arrangements must be made with Essex Police to carry out this function on behalf of the Council.
- 25.2 The routine making of simple test-purchases is not usually considered to require a CHIS authorisation. However, if a continuing relationship (whether personal or business) is formed then test purchases may need to be considered for authorisation. Simple test purchases watched by officers involve directed

surveillance and not use of a CHIS.

- 25.3 Forming an online 'friendship' on Social Media in order to view closed postings (eg follow someone who protects their tweets or view a facebook profile which is not public) must be carefully considered. This could amount to directed surveillance or the use of a 'covert human intelligence source' which would need to be authorised under RIPA.

## **26. When is a relationship covert?**

- 26.1 A relationship is used covertly if it is conducted in a manner calculated to ensure that one party is unaware of its purpose.

## **27. What safeguards must the Council observe before using human intelligence sources?**

- 27.1 The Council must be satisfied:-

- That use of a CHIS is in connection with the Council's statutory functions.
- That use of a CHIS is likely to impact on someone's human rights, for example the right to respect for private and family life, home and correspondence, that such interference is proportionate and can be justified.
- That use of a CHIS is properly authorised and lawful.

- 27.2 Only authorised officers listed in Appendix 1 may grant an authorisation.

- 27.3 Following the internal authorisation process the decision must be referred to a Magistrate for approval.

## **28. Authorisation of a CHIS**

- 28.1 An authorisation approved by a Magistrate under Part II of RIPA will provide lawful authority for the County Council to use a CHIS.

- 28.2 Officers involved in the use of CHIS should refer to the statutory Code of Practice.

- 28.3 Local authority staff may only grant authorisations if the activities are necessary for the purpose of preventing and detecting crime or of preventing disorder. Note that the 'serious crime' threshold (as set out in paragraph 11.3) which applies to directed surveillance does not apply to the use of a CHIS.

## **29. Necessity and Proportionality**

- 29.1 RIPA requires that the person granting an authorisation believes that the use of the source is necessary and proportionate.

- 29.2 Use of the source is necessary if the Council needs the information as part of the investigation it is undertaking. It is proportionate if the benefit of the source outweighs the intrusion. To assess this a balancing exercise must be undertaken weighing up the intrusion with the benefit of using the source. This involves considering whether the information which is sought could reasonably be obtained by other less intrusive means.

- 29.3 The use of a source should be carefully managed to meet the objective in question and sources must not be used in an arbitrary or unfair way.

### 30 Collateral Intrusion

- 30.1 An application for an authorisation should include an assessment of the risk of 'collateral intrusion' – ie intrusion into the privacy of anyone who is not directly the subject of the investigation or operation. This includes passers-by or the family of the person who is under investigation. See section 14 for more information.

### 31. Vulnerable Adults

- 31.1 A vulnerable individual should only be authorised to act as a source in the most exceptional circumstances. You should refer to the code and take legal advice before proceeding.
- 31.2 A 'vulnerable individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation.

### 32. Juvenile sources

- 32.1 Special safeguards also apply to the use or conduct of sources under the age of 18. **Authorisations should not be granted to use a source under 16 years of age to give information against a parent.** Authorisations should not be granted with respect to a young person unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (SI 2002/793) are satisfied. The duration of such an authorisation is **four months** instead of twelve months.
- 32.2 The use of young people by ECC Trading Standards to make routine, simple underage test purchases of age-restricted goods is not considered to be the use of a CHIS. However, each case will be considered on its merits and if a proposed operation might involve formation of a relationship with the seller, an application for the appropriate authorisation should be made.

### 33. Authorisation Procedures for CHIS.

- 33.1 Under s29(3) of RIPA an authorisation for the use or conduct of a source may be granted by an authorising officer where he believes that the authorisation is necessary in the circumstances of the particular case for the purpose of preventing and detecting crime or of preventing disorder.
- 33.2 The Council makes very sparing CHIS authorisation powers. Detailed guidance has not been included in these notes. Reference should be made to the procedure for authorising directed surveillance. See also the flow chart relating to Magistrates' Approval in the Home Office Document at this [link](#).
- 33.3 Authorisation for the use of a CHIS will, unless renewed, cease to have effect at the end of a period of **twelve months** beginning with the day on which it was approved by a Magistrate.

- 33.4 Regular reviews of authorisations should be undertaken to assess the need for the use of the source to continue. The results of a review should be recorded on the central record of authorisations. Particular attention is drawn to the need to review authorisations frequently where the use of a source provides access to confidential information or involves collateral intrusion.
- 33.5 Authorisations should be renewed unless there has been a recent review.
- 33.6 A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once, if necessary, provided they continue to meet the criteria for authorisation. The renewal should be kept/recorded as part of the authorisation record.
- 33.7 Any renewal must also be approved by a Magistrate.
- 33.8 All applications for the renewal of an authorisation should record:
- whether this is the first renewal or every occasion on which the
  - authorisation has been renewed previously;
  - any significant changes to the information provided on the original application or any previous reviews;
  - the reasons why it is necessary to continue to use the source;
  - the use made of the source in the period since the grant or, as the case may be, latest renewal of the authorisation;
  - the tasks given to the source during that period and the information obtained from the conduct or use of the source;
  - the results of regular reviews of the use of the source;

## **34. Cancellations**

- 34.1 The authorisation should be cancelled, usually by the officer who granted or renewed the authorisation if he is satisfied that the use or conduct of the source no longer satisfies the criteria for authorisation or that satisfactory arrangements for the source's case no longer exist, or if the use of the CHIS is no longer required.
- 34.2 Where necessary, the safety and welfare of the source should continue to be considered after the authorisation has been cancelled.

## **35. Management of Sources**

- 35.1 The Code of Practice should be followed about management of the source.
- 35.2 In particular you should note the requirement for two senior officers to be involved in the management of the CHIS.

One person must have day to day responsibility for:

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

Another person must have general oversight of the use of the source.

- 35.3 The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the authorising officer.
- 35.4 In cases where the authorisation is for the use or conduct of a source whose activities benefit more than a single public authority, responsibilities for the management and oversight of that source may be taken up by one authority or can be split between the authorities.
- 35.5 ECC will consider safety and welfare when carrying out actions in relation to authorisation or tasking, and to foreseeable consequences to others of that tasking. A risk assessment must be carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known before authorising the use or conduct of a source. The long term security and welfare of the source should also be considered at the outset.

## **36 Combined authorisations**

- 36.1 A single authorisation may combine two or more different authorisations under Part II of RIPA (eg authorising CHIS in connection with test purchases at more than one venue). It is not appropriate to have a single form dealing with applications for surveillance and a CHIS in the same form.

## **37 Central Record of all authorisations**

- 37.1 In accordance with the codes of practice a centrally retrievable record of all authorisations is kept by the County Council and updated whenever an authorisation is granted, renewed or cancelled. Records are retained for three years from the end of the authorisation.
- 37.2 The following information and documents will be kept on the central record:-
- a copy of the authorisation
  - a copy of any decision taken by a magistrate;
  - a copy of any renewal or review of an authorisation;
  - any risk assessment made in relation to the source;
  - the circumstances in which tasks were given to the source;
  - the value of the source to the investigating authority;
  - the reasons, if any, for not renewing an authorisation;
  - the reasons for cancelling an authorisation;
  - the date and time when any instruction was given by the authorising officer to cease using a source.
- 37.3 The SRO is responsible for overseeing compliance with RIPA. The central records are kept under the supervision of the SRO. Copies of each document listed above must be sent to the Co-ordinating Officer immediately.

## **38 Retention and destruction of the product**

- 38.1 Where the product obtained from a source could be relevant to pending or future

criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review. Particular attention is drawn to the requirements of the code of practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the investigation must be recorded and retained.

- 38.2 There is nothing in RIPA which prevents material obtained from properly authorised use of a source from being used in other investigations.
- 38.3 Officers must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. This includes compliance with the data protection principles which require data to be kept securely and to be destroyed when no longer required for the original purpose.

### **39. Errors.**

- 39.1 Section 24 of this document applies to errors in the use of a CHIS in the same way as it applies to directed surveillance.

## APPENDIX 1

### Senior Responsible Officer

Director, Legal and Assurance – Paul Turner

### Authorising Officers

The following officers are authorised to act as authorising officers for the purposes of an application for an authorisation to carry out directed surveillance and for the use or conduct of a covert human intelligence source.

The Head of the Paid Service – Gavin Jones

Service Manager for Trading Standards – Matthew Sanctuary

Head of Assurance – Paula Clowes

Where confidential information is likely to be acquired, authority must be obtained from the Head of the Paid Service or in their absence the Monitoring Officer.

Where there is an allegation of fraud or corruption the Head of Assurance must be notified and agree to any surveillance which is not under his/her direct control.

### Co-ordinating Officer

Karen Bellamy – Counter Fraud Manager, Legal and Assurance

### Advice on RIPA

Advice on the use of RIPA is available from the SRO, the Service Manager for Trading Standards or Essex Legal Services.

### Record Keeping

Information for the Central Record should be sent to the Co-ordinating Officer.

### Version control

Amended policy effective from June 2017.

|                         |   |
|-------------------------|---|
| Title                   | OPERATIONAL POLICY AND PROCEDURAL GUIDANCE ON THE USE OF COVERT SURVEILLANCE AND THE USE OF COVERT HUMAN INTELLIGENCE SOURCES |
| Author/Owner            | Owner: Director – Legal and Assurance   |
| Status                  |   |
| Version                 |   |
| Date                    | June 2017   |
| Review date             | 2018  |
| Security classification | Not protectively marked   |
| Approved by             | Full version approved by Audit, Governance and Standards Committee. Name changed approved by Director, Legal                  |