A meeting of the **CORPORATE GOVERNANCE PANEL** will be held in **ROOM 0.1A CIVIC SUITE, PATHFINDER HOUSE, ST MARY'S STREET, HUNTINGDON, PE29 3TN** on **WEDNESDAY, 24 JULY 2013** at **6:30 PM** and you are requested to attend for the transaction of the following business:-

Contact (01480)

APOLOGIES

1. MINUTES (Pages 1 - 4)

To approve as a correct record the Minutes of the meeting held on 22nd May 2013. **Mrs H J Taylor 388008**

2. MEMBERS' INTERESTS

To receive from Members declarations as to disclosable pecuniary, non-disclosable pecuniary or non pecuniary interests in relation to any Agenda item. See Notes below.

3. CORPORATE GOVERNANCE PANEL - PROGRESS REPORT (Pages 5 - 8)

To receive a report by the Head of Legal and Democratic Services. **Mrs H J Taylor 388008**

4. FILMING AND RECORDING AT COUNCIL MEETINGS (Pages 9 - 14)

To consider a report of the Head of Legal and Democratic Services proposing a variation to the existing constitution relating to photography, broadcasting or recording of meetings. **C Meadowcroft 388021**

5. COMPLAINTS FEEDBACK ANNUAL REPORT (Pages 15 - 24)

To consider a report by the Head of Legal and Democratic Services on the internal complaints determined by the Local Government Ombudsman in 2012/13. **A Roberts 388015**

6. PREPARING THE ANNUAL GOVERNANCE STATEMENT (Pages 25 - 28)

To consider a report by the Assistant Director, Finance and Resources on the action taken to review the Code of Corporate Governance and seeking comments on the Council's draft Annual Governance Statement for 2012/13. **D Harwood 388115**

7. REVIEW OF RIPA POLICIES AND PROCEDURES (Pages 29 -

100)

To receive a joint report by the Heads of Legal and Democratic Services and Customer Services. **N Jennings 388480**

8. INTERNAL AUDIT SERVICE ANNUAL REPORT (Pages 101 - 114)

To receive the annual report of the Internal Audit Manager. **D Harwood 388115**

9. WORK PROGRAMME AND TRAINING (Pages 115 - 116)

To consider a report by the Assistant Director, Finance and Resources. **D Harwood 388115**

10. EXCLUSION OF PRESS AND PUBLIC

To resolve:-

that the public be excluded from the meeting because the business to be transacted contains exempt information relating to the financial or business affairs of any particular person (including the authority holding that information).

11. APPOINTMENT OF PROFESSIONAL ADVISORS (Pages 117 - 118)

To consider a report by the Internal Audit Manager. **D Harwood 388115**

Dated this 16 day of July 2013

Head of Paid Service

Notes

A. Disclosable Pecuniary Interests

(1) Members are required to declare any disclosable pecuniary interests and unless you have obtained dispensation, cannot discuss or vote on the matter at the meeting and must also leave the room whilst the matter is being debated or voted on.

(2) A Member has a disclosable pecuniary interest if it

(a) relates to you, or
(b) is an interest of -

(i) your spouse or civil partner; or
(ii) a person with whom you are living as husband and wife; or
(iii) a person with whom you are living as if you were civil partners

and you are aware that the other person has the interest.

(3) Disclosable pecuniary interests includes -

(a) any employment or profession carried out for profit or gain;
(b) any financial benefit received by the Member in respect of expenses incurred carrying out his or her duties as a Member (except from the Council);
(c) any current contracts with the Council;
(d) any beneficial interest in land/property within the Council's area;
(e) any licence for a month or longer to occupy land in the Council's area;
(f) any tenancy where the Council is landlord and the Member (or person in (2)(b) above) has a beneficial interest; or
(g) a beneficial interest (above the specified level) in the shares of any body which has a place of business or land in the Council's area.

B. Other Interests

(4) If a Member has a non-disclosable pecuniary interest or a non-pecuniary interest then you are required to declare that interest, but may remain to discuss and vote.

(5) A Member has a non-disclosable pecuniary interest or a non-pecuniary interest where -

(a) a decision in relation to the business being considered might reasonably be regarded as affecting the well-being or financial standing of you or a member of your family or a person with whom you have a close association to a greater extent than it would affect the majority of the council tax payers, rate payers or inhabitants of the ward or electoral area for which you have been elected or otherwise of the authority's administrative area, or
(b) it relates to or is likely to affect any of the descriptions referred to above, but in respect of a member of your family (other than specified in (2)(b) above) or a person with whom you have a close association

and that interest is not a disclosable pecuniary interest.

Please contact Mrs H Taylor, Senior Democratic Services Officer, Tel No: 01480 388008 / e-mail: Helen.Taylor@huntingdonshire.gov.uk if you have a general query on any Agenda Item, wish to tender your apologies for absence from the meeting, or would like information on any decision taken by the Panel.

Specific enquiries with regard to items on the Agenda should be directed towards the Contact Officer.

Members of the public are welcome to attend this meeting as observers except during consideration of confidential or exempt items of business.

Agenda and enclosures can be viewed on the District Council's website – www.huntingdonshire.gov.uk *(under Councils and Democracy).*

If you would like a translation of Agenda/Minutes/Reports or would like a large text version or an audio version please contact the Democratic Services Manager and we will try to accommodate your needs.

Emergency Procedure

In the event of the fire alarm being sounded and on the instruction of the Meeting Administrator, all attendees are requested to vacate the building via the closest emergency exit.

This page is intentionally left blank

HUNTINGDONSHIRE DISTRICT COUNCIL

MINUTES of the meeting of the CORPORATE GOVERNANCE PANEL held in the Civic Suite, Pathfinder House, St Mary's Street, Huntingdon, PE29 3TN on Wednesday, 22 May 2013.

PRESENT: Councillor E R Butler – Chairman.

Councillors M G Baker, K J Churchill, G J Harlock, R Harrison, P Kadewere and R J West.

APOLOGY: An apology for absence from the meeting was submitted on behalf of Councillor P G Mitchell.

4. MINUTES

The Minutes of the meetings of the Panel held on 26th March and 15th May 2013 were approved as a correct record and signed by the Chairman.

5. MEMBERS' INTERESTS

Councillor R J West declared an interest in Minute No 13/10 as a Member of the Overview and Scrutiny Panel (Social Well-Being).

6. CORPORATE GOVERNANCE PANEL - PROGRESS REPORT

The Panel received and noted a report by the Head of Legal and Democratic Services (a copy of which is appended in the Minute Book) which contained details of actions taken in response to recent discussions and decisions. In response to concerns that little progress appeared to have been made to introduce a corporate guide to managing projects, the Assistant Director, Finance and Resources reassured the Panel that some work had already been undertaken to prepare a timeframe and establish a Working Group.

Additionally, it was reported that a letter had yet to be sent to the Departments for Communities & Local Government and for Works & Pensions over the cost of auditing benefit claims, as the Assistant Director, Resources was awaiting confirmation as to whom it should be sent.

7. EXCLUSION OF THE PUBLIC

RESOLVED

that the public be excluded from the meeting because the business to be transacted contains exempt information relating to an individual and is likely to reveal the identity of that individual.

8. HOUSING NEEDS COMPLAINT AWARD OF COMPENSATION

Consideration was given to a report by the Head of Customer Services (a copy of which is appended in the Annex to the Minute Book) regarding a complaint that the Council had not responded correctly to a claim of homelessness which had been made to the Local Government Ombudsman.

Members' attention was drawn to the background to the claim and the action taken in response to the findings of the Ombudsman. The Panel expressed some surprise that the Ombudsman had decided, in the first instance, to investigate the matter rather than refer it back to the Council. In response to which, the Head of Legal and Democratic Services explained that the Ombudsman has this discretion when dealing with a complaint about homelessness. In concluding that the matter could have been dealt with through the Council's complaints procedures, the Panel

RESOLVED

(a) that the report be received and a compensation payment of £250 awarded to the complainant to be set against his personal debt to the Council; and

(b) that the Housing Needs and Resources Manager be requested to clarify why the Council had not been given the opportunity to resolve the matter in the first instance.

9. RE-ADMITTANCE OF THE PUBLIC

RESOLVED

that the public be re-admitted to the meeting

10. REVIEW OF THE EFFECTIVENESS OF OVERVIEW & SCRUTINY PANELS

A report by the Internal Audit Manager was submitted which summarised the findings of a review by a Working Group established by the three Overview and Scrutiny Panels to look into the effectiveness of Overview and Scrutiny. A copy of the report is appended in the Minute Book.

The Internal Audit Manager reported that the Panels were generally acting effectively in terms of the discharge of their responsibilities and fulfilling their terms of reference.

In discussing the areas identified by the Working Group as requiring improvement, attention was drawn to the engagement of the public and other stakeholders. In that respect, Members expressed their disappointment that the proposed pilot Local Joint Committee had not yet been organised. As a way forward, Members suggested that the Deputy Executive Leader be requested to update the Panel on the progress being made with the pilot scheme.

Having considered whether there was scope to review other Panels or Committees, the Panel

RESOLVED

(a) that the outcome of the Working Group's review of the effectiveness of the Panels be noted;

(b) that the outcome of the effectiveness review be taken into account when considering the annual governance statement; and

(c) that the effectiveness reviews be continued with a review of the Licensing and Protection Panel/ Licensing Committee.

11. REVIEW OF THE EFFECTIVENESS OF INTERNAL AUDIT SERVICE

Consideration was given to a report by the Internal Audit Manager (a copy of which is appended in the Minute Book) detailing the outcome of a review of the effectiveness of the Internal Audit Service as required by the Accounts and Audit Regulations 2011.

Members were advised that the self-assessment review had been conducted by the Internal Audit Manager against "proper practice" provisions of the Public Sector Internal Audit Standards (PSIAS) and the Local Government Application Note to the PSIAS. Particular attention was drawn to an action plan which had been prepared to address the areas of non-conformance. Having been reassured that these instances were only of a minor nature and were not considered significant enough to warrant inclusion in the Annual Governance Statement, the Panel

RESOLVED

(a) that the outcome of the Internal Audit Manager's self-assessment which shows that the Internal Audit Service generally conforms with the PSIAS be noted;

(b) that the intention of the Action Plan to address the areas of non-conformance identified from the self-assessment be noted; and

(c) that the areas of non-conformance, as outlined in Appendix B of the report now submitted, be confirmed as not being significant enough to be considered in the Annual Governance Statement.

12. WORK PROGRAMME AND TRAINING

By way of a report by the Assistant Director, Finance and Resources (a copy of which is appended in the Minute Book) Members were acquainted with a work programme for the Panel for 2013/14.

The Internal Audit Manager encouraged the Panel to attend a training session for Members with finance, governance, audit and risk management responsibilities being held on 14th June 2013, details of which would be emailed to Members.

Additional, it was reported that Members would be invited to an informal session to discuss the draft annual governance statement prior to it being considered formally by the Panel at their July meeting.

RESOLVED

that the contents of the report now submitted be noted.

13. FRAUD WORKING GROUP

(The Chairman announced that he proposed to admit the following urgent item in accordance with Section 100B (4) (b) of the Local Government Act 1972 given the need to appoint to the Working Group)

RESOLVED

that Councillors E R Butler, K J Churchill, G J Harlock and P G Mitchell be appointed to the Fraud Working Group for the ensuing Municipal Year.

Chairman

CORPORATE GOVERNANCE PANEL PROGRESS REPORT

Panel Date	Decision	Response	Date for Action	Officer Responsible
25/09/12	**Annual report on the Freedom of Information Act, Environmental Information Regulations and Data Protection Act** Agreed that the previous year's statistics on the number of requests received by the Council under the Freedom of Information Act be included in future reports for comparative purposes.		September 2013	Heads of IMD, Legal and Democratic Services
25/09/12	**2010/11 Accounts** The corporate guide to managing projects be reviewed and approved by Chief Officers Management Team and subsequently forwarded on to Managers for their perusal.	A Working Group is being established to undertake this. Timescale will be clarified once they have met.		Assistant Director Finance and Resources
12/12/12	**Corporate Business Continuity Planning** Service Manager, IMD to identify site which would accommodate council services in the event of major incident at Pathfinder House. Details to be included in the 2013 Annual Report to Panel.		December 2013 – Annual Report	Service Manager, IMD
12/12/12	**Fraud Investigation** • Identification of fraud in non welfare work and proposals for the fraud service from April 2015 onwards. • To retain the Fraud Working Group	Fraud Team Business Plan for 2013/2014 outlines areas for non-welfare fraud consideration, including the Cambs Fraud Hub, to identity potential savings to HDC and record outcomes of this work for review by Corp Gov.	September 2014 Ongoing	Head of Customer Services Head of Customer Services

CORPORATE GOVERNANCE PANEL PROGRESS REPORT

Panel Date	Decision	Response	Date for Action	Officer Responsible
		Provisional dates included in the 2013/14 municipal calendar to enable the Working Group to meet quarterly.		
12/12/12	**Providing assurance for the Governance Statement** Draft Annual Governance Statement to May/June Panel Meeting	To allow the development of the assurance mapping process, the draft AGS will be presented to Panel in July.	July 2013	Internal Audit Manager
26/3/13	**Grant Certification** The Assistant Director Finance and Resources to write to the Department of Communities & Local Government, the Department of Works & Pensions and the Audit Commission over the cost of auditing benefit claims and requesting the criteria for taking a second sample be adjusted to require this if the errors are significant.	Letter to be sent	June 2013	Assistant Director Finance & Resources
22/5/13	**Housing needs complaint award of compensation** Compensation payment award of £250 to be offset against debt owed to the Council Housing Needs and Resources Manager to clarify why the Council had not been given the opportunity to resolve the matter in the first instance.	The Ombudsman may not investigate a complaint before a Council has had a reasonable opportunity to investigate and respond to it. There are some circumstances where, exceptionally, the Ombudsman will consider becoming involved sooner these include: • Complaints about education; and • Complaints about homelessness		Housing Needs and Resources Manager Housing Needs and Resources

CORPORATE GOVERNANCE PANEL PROGRESS REPORT

Panel Date	Decision	Response	Date for Action	Officer Responsible
		where the person is currently, or will imminently be, homeless. *(further details available from the Ombudsman's website)*		Manager
22/5/13	**Review of the effectiveness of Overview and Scrutiny Panels** Request to the Deputy Executive Leader to update the Panel on the progress made with the pilot Local Joint Committee. Outcome of effectiveness review to be taken into account when considering the annual governance statement. Effectiveness reviews to be continued with the Licensing and Protection Panel/ Licensing Committee being reviewed next.	Email sent to Councillor Guyatt on 24th May 2013.	July 2013 September 2013 May 2014	Senior Democratic Services Officer Internal Audit Manager Internal Audit Manager
22/5/13	**Fraud Working Group** Councillors E R Butler, K J Churchill, G J Harlock and P G Mitchell appointed to the Fraud Working Group for the 2013/14. First meeting to be arranged.	Meeting on 12th June, papers sent out prior to the meeting.	June 2013	Corporate Fraud Manager

This page is intentionally left blank

CORPORATE GOVERNANCE PANEL **24TH JULY 2013**

COUNCIL PROCEDURE RULES – PROPOSED VARIATION TO PARAGRAPH 17A – PHOTOGRAPHY, BROADCASTING AND RECORDING OF MEETINGS

(Report by the Head of Legal and Democratic Services)

1. INTRODUCTION

1.1 The Panel undertook its biennial review of the Constitution at its meeting in March and recommended to Council the changes required to the Constitution following the publication of the Local Authorities (Executive Arrangements) (Meetings and Access to Information) (England) Regulations 2012. Principally, the Regulations impacted upon the arrangements for executive decision - making and access to information.

1.2 No reference was made in the Regulations to photography, broadcasting or recording of meetings.

1.3 Subsequently in June 2013, the Department for Communities and Local Government published new guidance entitled "Your Council's cabinet – going to its meetings, seeing how it works" – a guide for local people". Essentially this guidance follows the principles of the 2012 Regulations and provides the public with practical information about attending meetings of the Council's Executive and obtaining Council documents. A copy of the full guidance is available by accessing the following link:- www.gov.uk/government/publications/your-council's-cabinet-going-to-its-meetings-seeing-how-it-works

1.4 Within the guidance but not the Regulations is a Section relating to the filming and social media reporting of meetings.

1.5 This report draws attention to the section of the Guidance relating to filming etc. and proposes a consequential variation to the Constitution should Members consider this appropriate.

1.6 Whilst the guidance relates to meetings of the Executive or Cabinet only, it would seem reasonable for any new Council Procedure Rule to be drafted to apply to all meetings held by the Council which are open to the public.

2. EXTRACT FROM GUIDANCE

2.1 Set out below is an extract from the guidance in relation to filming and social media reporting of meetings –

"Can I film the meeting?

Council meetings are public meetings. Elected representatives and council officers acting in the public sphere should expect to be held to account for their comments and votes in such meetings. The rules

require Councils to provide reasonable facilities for any member of the public to report on meetings. Councils should thus allow the filming of councillors and officers at meetings that are open to the public.

The Data Protection Act does not prohibit such overt filming of public meetings. Councils may reasonably ask for the filming to be undertaken in such a way that it is not disruptive or distracting to the good order and conduct of the meeting. As a courtesy, attendees should be informed at the start of the meeting that it is being filmed; we recommend that those wanting to film liaise with Council staff before the start of the meeting.

The Council should consider adopting a policy on the filming of members of the public speaking at a meeting, such as allowing those who actively object to being filmed not to be filmed, without undermining the broad transparency of the meeting.

Will I be able to tweet or blog Council Meetings?

Similarly under the new rules there can be social media reporting of meetings. Thus bloggers, tweeters, Facebook and YouTube users and individuals with their own website should be able to report meetings. You should ask your Council for details of the facilities they are providing for Citizen Journalists."

3. CURRENT CONSTITUTION

3.1 Section 17A of the current Constitution provides

> 'that filming, videoing or audio recording of a meeting or photography at a Council meeting shall be permitted only with the consent of the Chairman of the meeting concerned. The necessary consent shall have been obtained and the Head of Paid Service, or in his/her absence, the Head of Legal and Democratic Services notified by no later than three working days before the meeting'.

3.2 The District Council is committed to being open and transparent in the way it conducts its decision making. Indeed, the requirements of the 2012 Regulations had minimum impact on the Council's decision making process because, in practice, there had been few occasions when it has been necessary for the District Council's Cabinet to consider matters in private and Agenda and reports have been published on the District Council's website for many years.

3.3 Notwithstanding, however, it is opportune to review the Constitution in this respect given the District Council's desire to encourage and maintain interest in its decision making.

3.4 Mindful of the fact that the public attending meetings may not wish to be recorded, it is proposed that the wording in paragraph 17A of the Council Procedure Rules be deleted and replaced with the following:-

"Filming, Photography and Recording at Council Meetings

The Council supports the principles of openness and transparency in its decision making and permits filming, recording and the taking of

photographs at its meetings that are open to the public. It also welcomes the use of social networking and micro-blogging websites (such as Twitter and Facebook) to communicate with people about what is happening at meetings. The Council understands that some members of the public attending its meetings may not wish to be filmed. The Chairman of the meeting will facilitate this preference by ensuring that any such request not to be recorded is respected. These arrangements will operate in accordance with guidelines at Annex (vi). These Guidelines will be published on the Council's website."

4. RECOMMENDATION

4.1 It is proposed that the Panel recommend to Council that the variation to the Constitution described in paragraph 3.4 ante be approved; and

4.2 To avoid any potential difficulty in the interim and should the Panel be minded to support the recommendation in paragraph 4.1 above, it is proposed that the Guidelines should operate informally pending their formal approval by the Council in September.

BACKGROUND DOCUMENTS
Huntingdonshire District Council Constitution.
DCLG Guidance published June 2013 entitled "Your council's cabinet – going to its meetings, seeing How it Works".

Contact Officers:
Christine Deller, Democratic Services Manager☎ 01480 388007.

This page is intentionally left blank

ANNEX (vi)

FILMING, PHOTOGRAPHY AND RECORDING AT COUNCIL MEETINGS

The Council supports the principles of openness and transparency in its decision making and permits filming, recording and the taking of photographs at its meetings open to the public. It also welcomes the use of social networking websites (such as Twitter and Facebook) to communicate with people about what is happening at meetings.

To enable members of the public to be fully informed, anyone proposing to film, record or take photographs of a formal meeting of the Council is requested to advise the Democratic Services Team before the start of the meeting and to provide their name and contact details.

The Chairman of the meeting will have absolute discretion to terminate or suspend any of these activities, if, in their opinion, continuing to do so would prejudice the effective operation of the meeting. The circumstances in which termination or suspension might occur, could include:-

- public disturbance of the meeting;
- when it is necessary to formally exclude the press and public from the meeting due to the confidential nature of the business being discussed;
- where it is considered that continued recording/photography/filming might infringe the rights of any individual; and
- when the Chairman considers that a defamatory statement has been made.

In allowing this, the Council expects those recording proceedings:-

(i) not to edit the film/record/photographs in a way that could lead to a misinterpretation or misrepresentation of the proceedings. This includes refraining from editing an image or views expressed in a way that may ridicule, or show a lack of respect towards those being photographed/filmed/recorded; or

(ii) to comply with the request of any member of the public not to be filmed, recorded or photographed.

If intending to bring large equipment or wishing to discuss any special requirements please contact the Council's Democratic Services Team in advance of the meeting in order, where possible, for any necessary arrangements or adjustments to be made. The Chairman may direct that audio/visual recording or photography must only take place from a specific location in the meeting room.

The use of flash photography or additional lighting will not be allowed unless this has been discussed in advance of the meeting and agreement reached to ensure the meeting will not be unduly disrupted.

At the beginning of the meeting, the Chairman will make an announcement if i that meeting may be filmed, recorded or photographed.

(The Council Procedure Rules (paragraph 19) also provide for the removal of a member of the public from the meeting room should that person, having been warned, continue to interrupt the proceedings. The Chairman of a meeting may also call for any part of the meeting room to be cleared in the event of a general disturbance.)

This page is intentionally left blank

CORPORATE GOVERNANCE PANEL **24TH JULY 2013**

COMPLAINTS
(Report by the Head of Legal and Democratic Services)

1. INTRODUCTION

1.1 This report provides Members with information on internal complaints and complaints referred to the Local Government Ombudsman.

2. COMPLAINTS OUTCOMES AND TRENDS

Internal Complaints

2.1 The Council encourages employees who receive complaints initially to make every effort to resolve the problem straight away. If a complainant remains dissatisfied, or feels that his/her problem has not been looked at properly, or not been fully understood, they have the option to request someone else to investigate it at a more senior level. In this situation, a complaint is referred to the relevant Head of Service. It is at this stage that the matter is deemed to be a formal complaint. The table below shows the total number of formal complaints received over the last four years.

Year	2009/10	2010/11	2011/12	2012/13
Number of Complaints	67	58	40	43

2.2 The table attached as Appendix A lists the formal complaints received in the last year where a lesson has been learned and / or a complaint has been referred to the Ombudsman. The chart at Appendix B shows trends in complaints levels by service.

Complaints to the Call Centre

2.3 The majority of complaints to the Call Centre relate to the Operations Division. For the 2012/13 financial year, 363 (284) complaints were received out of 26,678 (42,630) service requests, which represents a complaint rate of 1.4% (0.7%). The figures in parenthesis are for 2011/12. The significant drop in the number of service requests is the result of payments being transferred to the new automated system. This means the figures should be treated with some caution. It will be possible to make more meaningful comparisons next year.

Complaints to the Local Government Ombudsman

2.4 The Local Government Ombudsman Service has in the past produced an Annual Report on each local authority. The Report contained information on the number of enquires received and how each of those enquiries was treated. The Ombudsman has stopped producing these reports. The Council now will not necessarily know if a complainant has contacted the Ombudsman because it may be decided that a matter does not warrant an investigation. The table in the Appendix identifies those complaints that have been investigated by the Ombudsman and, where a decision has been reached, the Ombudsman's findings. The trend in total complaint numbers is as follows:

Ombudsman Decisions	2009/10	2010/11	2011/12	2012/13
Total	**7**	**18**	**7**	**9**

2.5 Members will recall that one matter dealt with by the Ombudsman was settled locally (Minute No. 8 of the meeting held on 22nd May 2013 refers). The remaining investigations similarly revealed no evidence of maladministration.

3. CONCLUSION

3.1 The decision last year to incorporate lessons learned into the annual report to the Panel on complaints and the withdrawal of the Ombudsman's Annual Report have meant that the format of this report has changed. Members are invited to comment on the new format and consider whether any other information should be included in future reports.

BACKGROUND PAPERS

Complaints Management System

Local Government Ombudsman Decision Notices

Contact Officer: Tony Roberts (01480) 388015

REF NO	REASON	DIVISION	SUBJECT	ACTION	LESSONS LEARNED	OMBUDSMAN DECISION
1098	Council Procedures	Operations	Council waste collection arrangements were causing a nuisance	Staff Instruction		Yes. The Council's refuse collection arrangements for neighbouring properties and its reference to those arrangements in an earlier planning approval did not cause serious injustice so it was decided not to pursue the complaint.
1101	Council Procedures	Development Management	Complainant's residential amenity was adversely affected by grant of planning permission for development on neighbouring land	Planning considerations explained No Action Taken	This case reinforced the need for effective review of subsequent proposals for amendments to schemes	No
1104	Service Delivery	Development Management	Complainant's residential amenity was adversely affected by grant of planning permission for an extension to a neighbouring property	Planning considerations explained No Action Taken		Yes. No maladministration found.
1109	Council Procedures	Development Management	Complainant not notified of planning application and extension not being in keeping and	Planning procedure and considerations explained	This case reiterated the need for appropriate widespread neighbour consultation.	No

			results in overlooking	No Action Taken		
1111	Service Delivery	Development Management	The Council failed properly to consider a planning application, which the complainants felt adversely affected their homes.	Detailed analysis of planning process provided No Action Taken		Yes. No maladministration found.
1112	Action of Employee	Environmental Health	An Enforcement Officer had exceeded her remit.	Officer's role explained No Action Taken	Dog warden investigation procedures reviewed to ensure a dog-owner has understood that where they are the subject of an investigation one outcome may be Court-action (civil or criminal).	No
1114	Council Procedures	Benefits	Benefit stopped whilst under investigation for fraud. Following decision Benefit not reinstated.	Separate benefit appeals procedure used. No Action Taken		No
1116	Action of Employee	Estates	Questioning an 'order' given in letter.	Purpose of letter clarified. Change in Procedures	Future letters to be reviewed prior to their despatch.	No
1119	Service Delivery	Development Management	The Council's approach to development of the complainant's land has been inconsistent and its	Clarification provided of why the Council acted in the way it has how the Development	This case reinforced the need for reasons to be given for the decision made.	No

			decision-making procedures flawed.	Management decisions are reached. No Action Taken		
1123	Service Delivery	Development Management	The Council did not take an objection into account when determining a planning application.	The objection was received but through human error, it was not forwarded on to the case officer. All the matters raised had been taken into account so the decision would not have been affected. Staff Instruction	This case highlighted the need for effective administrative procedures to be in place	No
1124	Service Delivery	Development Management	The Council incorrectly evaluated and considered the potential impacts of a proposed development, upon neighbouring residential amenity during the planning process.	Detailed account of the determination process provided. Case is with the Ombudsman.		Yes – On-going (Ombudsman's provisional view – Council released covenant and granted planning permission without fault)
1129	Service Delivery	Development Management	The Council had failed to enforce a condition of the planning permission for the building of a house as a result of	Apology issued for failure to ensure a condition was discharged.	This case reinforced the need for all proposed conditions to be considered in relation to the applicable statutory tests	Yes – Planning condition does not meet the applicable tests but no substantive injustice for the Council to

			which difficulties with an immediate neighbour had been exacerbated.	Staff instruction.		remedy.
1130	Council Procedures	Benefits	The council's processes, attitudes and behaviour are set up to create hurdles and are not solutions based.	Formal Training. To put this in perspective, the team answer around 2000 p/calls each month with very few complaints.	Need for further training identified on customer care. To be carried out in 2013/14 after latest recruitment exercise.	No
1131	Council Procedures	Council Tax	Complainant unhappy with the way his Council Tax account had been handled and with the fact that a summons and liability order were sent to him.	Detailed analysis of a number of points provided.		Yes. No finding of maladministration.
1132	Service Delivery	Development Management	The Council's decision to grant planning permission for a neighbour's extension failed to take proper account of his amenity.	Responses to various matters relating to the application provided.		Yes - On-going
1133	Council Procedures	Benefits	Concerns about procedural issues in relation to Housing Benefit and bed and breakfast accommodation.	Detailed account of complainant's case provided. Staff Instruction	Joint Housing/Benefits complaint. Reminder to benefit staff about setting up claims where an existing	No

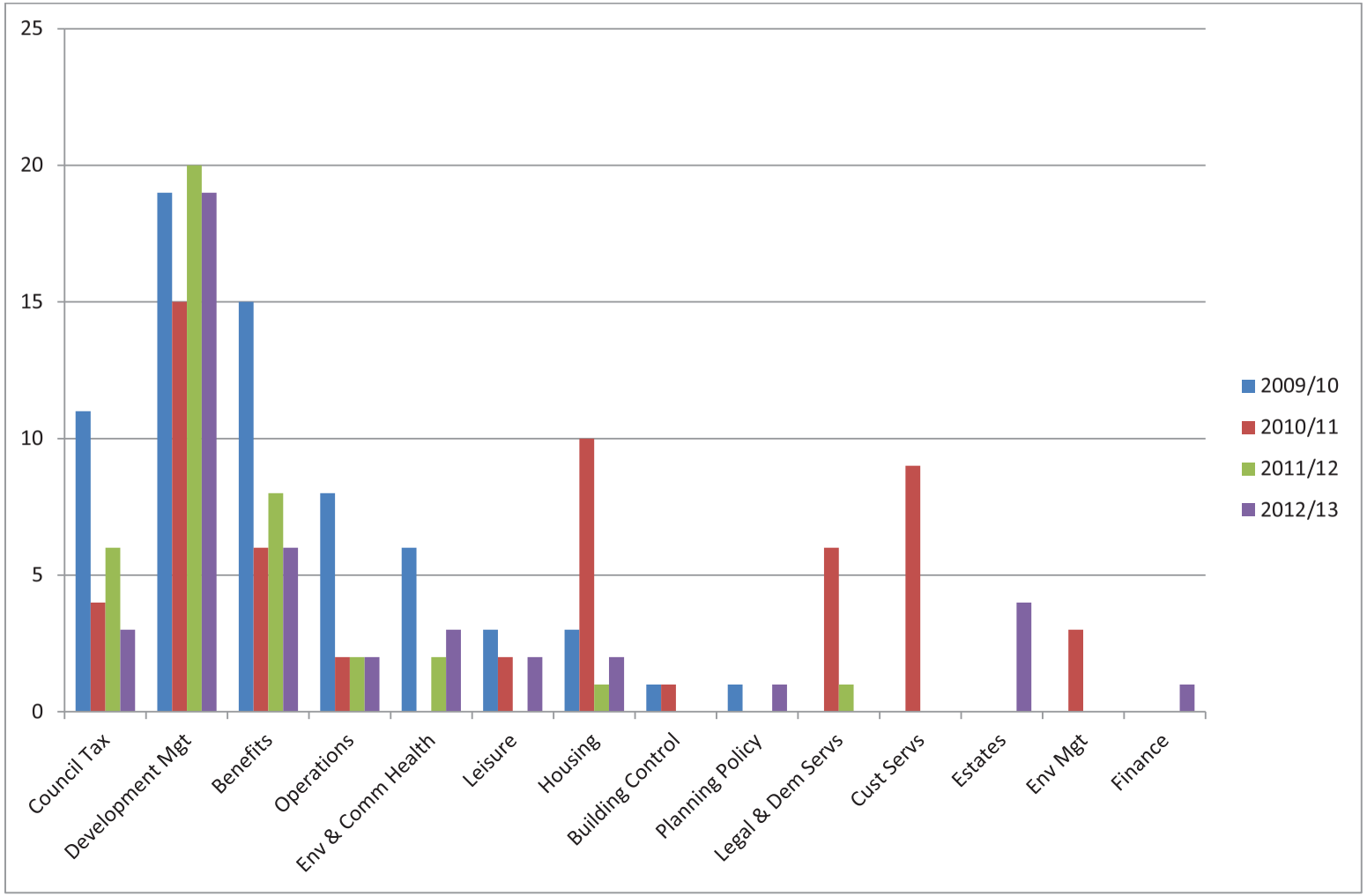
					customer moves - issue now resolved.	
1135	Failure to Respond	Development Management	The Council took too long to write to residents regarding a planning matter	Complaint upheld and apology issued. Staff Instruction	This case reinforced the need for timely communications	No
1137	Council Procedures	Finance	The Council had issued an invoice before it was due.	Invoice generated automatically. Change in Service.	Invoicing system changed.	No.
1141	Failure to Respond	Development Management	The Council failed to take enforcement action against a neighbour carrying out activities for which planning authorisation did not exist.	The results of investigations into the activities provided. Apology issued for delay in communicating the investigation results to the complainant. Staff Instruction	This case also reinforced the need for timely responses to complainants	No
1143	Council Procedures	Council Tax	The Complainant received threatening letters/final notices without having had any previous communication.	Council Tax correspondence sent to property rather than the managing agent's address. Apology sent to complainant. Change in Service	All Local Taxation staff to consider the circumstances when making similar amendments to accounts in the future	No

1144	Service Delivery	Leisure	The Council acted unreasonably by failing to provide alternative arrangements for a club whose facilities were withdrawn.	Decision making process explained. No Action Taken		Yes. No maladministration found.
1146	Council Policy	Environmental Health	Complainant dissatisfied at the Council's arrangements for the prevention of noise nuisance.	Complainant provided with justification for the policy and with explanation of why the investigations undertaken did not establish a nuisance. No Action Taken	The demand and cost/benefit of a 24-hr nuisance investigation service was reviewed- and the present arrangements confirmed appropriate.	No
1147	Service Delivery	Environmental Health	The Council did not take adequate enforcement action against a neighbour's activities which were causing a nuisance.	Breakdown of enforcement actions sent to complainant. No Action Taken	Adherence to our standard investigating procedures was reviewed- the conclusions concur with the Ombudsman's provisional findings (3 June) 'The Council investigated the complaints without fault.	Yes. No maladministration found.
1148	Service Delivery	Benefits	Complainant wanted his Housing Benefit backdated. The Council did not advise him of a time limit and should	Complaint taken to tribunal. No legal power to backdate the claim. Decision confirmed		Yes. Complaint outside Ombudsman' jurisdiction as there was an alternative statutory course of appeal.

			have accepted evidence previously submitted.	through complaints process. No Action Taken		

APPENDIX B

COMPLAINTS TRENDS BY SERVICE



CORPORATE GOVERNANCE PANEL **24 JULY 2013**

PREPARING THE ANNUAL GOVERNANCE STATEMENT
(Report by the Assistant Director (Finance & Resources))

1. Purpose

1.1 To note the action taken to review the Code of Corporate Governance and comment upon the significant issues to be included in the annual governance statement in respect of the year ending 31 March 2013.

2. Code of Corporate Governance

2.1 An informal meeting of the Panel was held on 1 July. It was attended by Councillors Churchill, Harlock, Mitchell and West who considered the Council's current position against the requirements and supporting principles of the Code of Corporate Governance.

2.2 When considering the current position, the following items were noted:

1 The themes and aims of the Leadership Direction were not sufficiently evident in service delivery plans or performance measures or employees performance targets. There was a lack of any meaningful performance measures being reported to Members, other than in respect of financial matters.

2 The Council's Consultation and Engagement Strategy is currently being reviewed by an Overview & Scrutiny Panel working group, and is anticipated to be tabled to Overview & Scrutiny Panels and Cabinet later in the year. It is understood that the Strategy will deal with the 'how to' elements of consultation of engagement, and not the 'when to'. It was considered that the strategy should cover both issues.

3 Customer surveys had been carried out in the previous year in a number of service areas. Concerns were expressed that two of the largest customer facing services – planning and household waste collection – had not undertaken any surveys. How was the quality of service measured in these two areas?

4 The Internal Audit Manager had not undertaken a self-assessment against the CIPFA publication "Role of the Head of Internal Audit". It was agreed that the report the Panel received in May on internal audit effectiveness against the Public Sector Internal Audit Standards was sufficiently challenging. They noted that an independent external review of internal audit was planned during 2013/14.

5 Whilst progress had been made in improving financial competences of budget holders, the financial position of the Council meant that there had to be ever improving accuracy in budgetary control. This would allow financial savings to be identified earlier in the financial year.

6 The Corporate Team Manager was identified as the Lead Officer for a number of the supporting principles. This position was established in 2011, yet the Panel were unclear as to the overall role and responsibilities of the Corporate Team Manager and the impact of the corporate team on the Council's governance arrangements.

The Managing Director intends to review operational structures and the role of the Corporate Team will be included in that review.

7 Prior to finalising any out-sourcing of services, the Corporate Governance Panel to be informed of the governance arrangements that are to be introduced and the procedures for obtaining assurance required to support statements included in the annual governance statement.

8 The Council does not publish one document that contains information relating to its overall governance, performance (delivery against the Leadership Direction, strategic plans or finances), achievements or satisfaction of service users. The public and service users should not be required to have to search the Council's website for this information. Consideration should be given to publishing an annual report.

2.3 Following further discussion of the matters listed above, it was felt that items 1, 5 and 8 were significant enough to be included in the annual governance statement.

2.4 The meeting also felt that the supporting principle to the Code that dealt with the use of resources and excellent value for money could not be supported at the present time. Whilst it was a laudable aim, providing excellent value for money was difficult to achieve when service levels were having to be reduced. The requirement to provide 'excellent' value for money should be deleted from the Code and replaced with 'good'. Good value for money is defined by the National Audit Office as the "optimal use of resources to achieve the intended outcomes".

3. Other Significant issues identified throughout the year

3.1 Issues of concern that had been discussed by the Panel during the year were also considered. It was felt that the following items were significant enough to be included in the annual governance statement.

i. The corporate guide to managing projects be reviewed, approved by Chief Officers Management Team and adopted (Panel meeting 25 September 2012).

ii. The Overview & Scrutiny Panel's effectiveness review highlighted the lack of opportunity to directly engage with the public. (Panel meeting 22 May 2013).

4. Annual Governance Statement

4.1 The basis of the annual governance statement has been discussed at the Chief Officers' Management Team and an initial draft is under preparation. This will be influenced by the annual opinion of the Internal Audit Manager and any other issues arising from this meeting's agenda.

4.2 It is proposed that the draft statement will be circulated to the Panel and the external auditor by the 9 August followed shortly afterwards by an informal meeting of the Panel at which they have the opportunity to review and comment upon the statement. This will allow the final statement to be presented to the Panel in September that reflects their comments.

5. Recommendation

5.1 It is recommended that the Panel:

a. Consider whether the following governance issues should be recorded as being 'significant' in the annual governance statement
   i. Develop the themes and aims in the Leadership Direction through service plans and performance measures
   ii. Improving budgetary control
   iii. Reinvigorate engagement with stakeholders
   iv. Introduce a project management methodology
   v. Prepare an annual report for the 2013/14 financial year

b. Approve the replacement of the word 'excellent' with 'good' in the supporting principle "Ensure that the Council makes best use of resources and that tax payers and service users receive ~~excellent~~ good value for money".

ACCESS TO INFORMATION ACT 1985
Code of Corporate Governance

Contact Officer: David Harwood, Internal Audit Manager ☎ **01480 388115**

This page is intentionally left blank

CORPORATE GOVERNANCE PANEL- 24th July 2013

REVIEW OF RIPA POLICIES & PROCEDURES
(Joint Report by Heads of Legal and Democratic Services and of Customer Services)

1. INTRODUCTION

1.1 Article 8 *(*RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE) of the Human Rights Act 1998 (HRA) states that every person shall have the right to respect for his private and family life, home, and correspondence. The Article states that there shall be no interference with this right by any public body except in accordance with the law. The Article, unlike many of the other Articles, does not give an absolute right to privacy where national legislation, compliant with HRA, states that the right can be suspended

1.2 The Regulation of Investigatory Powers Act 2000 (RIPA) was introduced to provide law enforcement agencies with a legal gateway and strict guidance on when and how the subject of an investigation can have their Article 8 rights suspended. Contrary to much press publicity Local Councils can use the powers conferred by RIPA but only for the purposes of the detection and prevention of crime.

1.3 Local Councils can use RIPA Authorisations to conduct 'Covert Directed Surveillance' or acquire 'Communications Data'. The Legislation, guidance and Code of Practice for both these areas is provided by the Home Office.

1.4 Huntingdonshire District Council (HDC) has had policies in place since 2001 which ensure that officers conducting these activities are fully trained and conversant with both the law and the most recent guidance from the Home Office.

2. Commissioners

2.1 RIPA provided for the creation of two commissioners to oversee the two areas of RIPA which affect HDC. The Office of the Surveillance Commissioner (OSC) and the Interception of Communication Commissioner Office (IOCCO) carry out these two separate functions.

2.2 The Council is required, whether there is a policy in place or not, to provide annual reports to both commissioners on all activity undertaken. The OSC inspect every Local Council affected by RIPA every three years and the IOCCO conduct random inspections.

3. Recent Changes

3.1 In October 2012 the Government introduced a stricter regime for Local Authorities when using the provisions of RIPA. This included the requirement for all applications to be authorised by a Justice of the Peace (JP) and that all RIPA activity, as defined in the Home Office Guidance, only take place where 'serious crime' was being investigated.

3.2 In early 2013 the Home Office produced new guidance and Codes of Practice for the amended requirements that Local Authorities had to meet.

3.3 The Council has now reviewed its own policies in light of these changes and addressed both issues of seriousness and JP authorisation, as well as fully adopting the Home Office guidance on covert surveillance and the acquisition of communications data.

3.4 The changes to Council policies required as a result of the legislative changes outlined in this report are significant. If any future minor changes are required it is proposed that these be dealt with in consultation with the Chairman of Corporate Governance Panel and reported to that Panel to avoid the necessity of a report to full council for every change.

4. Recommendation

that the Panel recommend to Council

(a) the adoption of the RIPA (Surveillance) Policy and Procedure as set out in Annex A.

(b) the adoption of the new RIPA (Communications Data) Policy and Procedure as set out in Annex B.

(c) authorising the Head of Legal and Democratic Services to make any consequential amendments to the Constitution .

(d) authorising the Head of Legal and Democratic Services to make any amendments to the policies in future after consultation with the Chairman of Corporate Governance Panel and subject to the matter being reported to the next meeting of Corporate Governance Panel

ATTACHED.
Annex A. HDC Policy - Covert Surveillance- Regulation of Investigatory Powers Act 2000
Annex B. HDC Policy- Acquisition of Communications Data -Regulation of Investigatory Powers Act 2000

BACKGROUND INFORMATION

Human Rights Act 1998
Regulation of Investigatory Powers Act 2000

Contact Officer: **Nick Jennings -**
☎ 01480 388480

This page is intentionally left blank

HUNTINGDONSHIRE DISTRICT COUNCIL

COVERT SURVEILLANCE

REGULATION OF INVESTIGATORY POWERS ACT 2000

(PART II)

(Directed Surveillance and the use of CHIS)

POLICY & PROCEDURE

CONTENTS

INTRODUCTION AND PURPOSE

Introduction

Since October 2000 when the Human Rights Act 1998 came into force, covert surveillance has become subject to statutory control in the UK. The Regulation of Investigatory Powers Act 2000 (RIPA) provides for the first time a legal framework for covert surveillance activities by public authorities (including local authorities). The Office of Surveillance Commissioners (OSC) has been set up as an independent inspection regime to monitor these activities.

The use of surveillance (both overt and covert) to provide information is a valuable resource for the protection of the public and the maintenance of law and order. To discharge their responsibilities local authorities and law enforcement agencies use unaided surveillance and surveillance devices. RIPA and codes of practice under it provides a legal framework and procedure to authorise the use of covert surveillance. Surveillance is covert if it is carried out in a manner that is calculated to ensure that persons who are subject to it are unaware that it is or may be taking place.

In some circumstances, it may be necessary for Council employees, in the course of their duties, to make observations of a person(s) in a covert manner. By their nature, actions of this sort may constitute an interference with that person's right to privacy. This may give rise to legal challenge as a potential breach of “the right to respect for private and family life, home and correspondence" under Article 8 of the European Convention on Human Rights and the Human Rights Act 1998. RIPA provides a procedure to defend the Council against such challenges

Purpose

This policy statement explains how Huntingdonshire District Council will meet legal requirements in relation to the use of covert surveillance. It also seeks to encourage and promote a professional approach in undertaking surveillance so that those affected may have confidence that the Council will act effectively and in a fair and lawful manner. It should be read in conjunction with the Regulation of Investigatory Powers Act 2000 and the current version of the Code of Practice on the use of Covert Human Intelligence sources and the Code of Practice on Covert Surveillance on the Home Office website www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice

STATEMENT OF INTENT

This policy statement applies only to the use of covert surveillance, although it is expected that usually any surveillance activity undertaken by or on behalf the Council will be **overt**.

The Council intends to fulfil its lawful obligations and use directed surveillance and covert human intelligence sources within the terms of the Regulation of Investigatory Powers Act 2000, the relevant Codes of Practice and the directions of the Office of Surveillance Commissioners in accordance with its lawful requirements.

The Council will keep its policy and procedures under review and update them as necessary and in accordance with any changes in the Law.

The Council will take necessary steps to ensure that employees whose duties involve investigations or supervision of them are informed of all relevant policy standards, procedures, and legislation.

Employees have a duty to follow this policy and its procedures and any employees knowingly acting outside this policy may be be subject to the Council's disciplinary procedures.

Evidence gathered by surveillance should be treated as confidential and only disclosed to persons (internal and external) whose authority has been explicitly established. Employees will be held responsible for any misuse, security breach or unauthorised disclosure while it is in their control.

Evidence gathered by covert surveillance will be held in accordance with the Council's Document Retention Policy. Documents created as part of surveillance applications including authorisations, reviews and cancellations will be held on the councils Central Register which will be maintained by the RIPA Central Monitoring Officer will be held for three years, as required by the Act.

The Council will keep in place appropriate security measures as required.

A reporting structure will be established headed by the RIPA Central Monitoring Officer with a liaison officer for each service division so:

- that authorisation, Judicial application/order form, review, renewal and cancellation forms and procedures are co-ordinated and consistent across the Council and comply with legislation
- All activity is available for inspection by the Office of Surveillance Commissioners
- All problems can be investigated thoroughly

Regular meetings are held, at least once every six months, with the liaison officers to review and update service divisions on changes in the law or Home Office guidance.

Subjects of covert surveillance carried out by or on behalf of the Council therefore can be assured that evidence collected (including personal data) will be processed with care and strictly in accordance with the law.

Council employees **will not carry out intrusive surveillance** within the meaning of the Regulation of Investigatory Powers Act 2000. This is covert surveillance carried out in relation to anything taking place on any residential premises or in any private vehicle; and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device capable of providing information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle.

The Council will seek to adhere to the authorisation, review, renewal and cancellation procedure provided for by the RIPA legislation and the codes of practice thereon before conducting any covert surveillance.

The Council will not intentionally gather evidence by covert surveillance from individuals where it is disproportionate or unnecessary in relation to the purposes of the investigation.

Surveillance carried out by a third party on behalf of the Council shall be subject to a contract which stipulates compliance with the law and this policy. Any service that intends to instruct a third party are required to liaise with the Central Monitoring Officer so that an Authorising Officer can take into account the capability of an agent acting for the Council before any contracts are agreed.

To assist with oversight of the Council's RIPA processes, it has appointed Colin Meadowcroft (Head of Law, Property and Governance) as the Senior Responsible Officer

(SRO) who will be responsible for the integrity of the process. However it must be stressed that all staff involved in the process must take their responsibilities seriously which will assist with the integrity of the Councils processes and procedures.

PRINCIPLES OF SURVEILLANCE

In planning and carrying out covert surveillance Huntingdonshire District Council employees shall comply with the following principles :

Lawful purposes

On 1 November 2012 two significant changes came into force that effects how local authorities use RIPA.

- **Approval of Local Authority Authorisations under RIPA by a Justice of the Peace**: The amendments in the Protection of Freedoms Act 2012 mean that local authority authorisations under RIPA for the use of Directed Surveillance or use of Covert Human Intelligence sources (CHIS) can only be given effect once an order approving the authorisation has been granted by a Justice of the Peace (JP). **This applies to applications and renewals only, not reviews and cancellations.**

- **Directed surveillance crime threshold**: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of **Directed Surveillance** where the local authority is investigating criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

The crime threshold, as mentioned is only for Directed Surveillance.

Therefore the only lawful reason is **prevention and detection of crime** in respect of its Core Functions. As from 1 November 2012 there is no provision for a Local Authority to use RIPA to conduct covert activities for disorder such as anti-social behaviour unless there are criminal offences involved which attract a maximum custodial sentence of six months.

Employees carrying out covert surveillance as far as practicable shall not interfere with any property or harass any person.

Confidential material

Applications where a significant risk of acquiring confidential material has been identified shall always require the approval of the Head of Paid Service.

Confidential material consists of :

- matters subject to legal privilege (e.g. between professional legal advisor and client)
- confidential personal information (e.g. relating to a person's spiritual, physical or mental health) or
- confidential journalistic material

DEFINITIONS

Unless the context otherwise requires, in this document the expressions in the first column shall have the meaning in the second column and any reference to a statute or statutory instrument or code of practice within the document shall include amendments to it.

Authorising Officer	means a person entitled to give an authorisation for directed surveillance or for the use of a covert human intelligence source in accordance with Section 30 of the Regulation of Investigatory Powers Act 2000 and the Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) Order 2000 SI No. 2417 as adapted to the organisational structure of the Council and who is included in the list of officers designated by the Council for such purposes.
Council	means Huntingdonshire District Council
Covert Human Intelligence Source	means a person who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within Section 26(8)(b) or (c) Regulation of Investigatory Powers Act 2000 namely :

b) to covertly use such a relationship to obtain information or to provide access to any information to another person; or

c) to covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship

a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

Covert Surveillance means surveillance carried out in a manner that is calculated to ensure that persons who are subject to this surveillance are unaware that it is or may be taking place

Directed Surveillance means covert surveillance which is not intrusive and is undertaken :

a) for the purpose of a specific investigation or a specific operation;

b) 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); and

c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of RIPA to be sought for the carrying out of surveillance

Private Information Private information includes any information relating to a person's private or family life. Private information

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

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of *private information*. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a *public authority* of that person's activities for future consideration or analysis.

Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute *private information* even if individual records do not. Where such conduct includes surveillance, a directed surveillance *authorisation* may be considered appropriate.

Private Vehicle means any vehicle that is used primarily for the private purpose of the person who owns it or of a person otherwise having the right to use it (except where the right to use the vehicle derives only from his having to pay, or undertake to pay for the use of the vehicle and its driver for a particular journey)

Residential Premises means so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as

	living accommodation (including hotel or prison accommodation that is so occupied or used)
Surveillance Device	means any apparatus designed or adapted for use in surveillance
Surveillance*	is defined in Section 48 of the Regulation of Investigatory Powers Act 2000 and includes : a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications; b) recording anything monitored, observed or listened to in the course of surveillance; and c) surveillance by or with the assistance of a surveillance device * surveillance does not include references to : a) any conduct of a covert human intelligence source for obtaining or recording (whether or not using a surveillance device) any information which is disclosed in the presence of the source; b) the use of a covert human intelligence source for so obtaining or recording information; or c) any such entry on or interference with property or with wireless telegraphy as would be unlawful unless authorised under Section 5 of the Intelligence Services Act 1994 (warrants for the intelligence services) or Part III of the Police Act 1997 (powers of the police and of customs officers)

SCOPE OF PROCEDURE

The RIPA procedure **does not** apply to :

- Covert observations where private information will not be obtained
- Observations that are not carried out covertly, or
- Ad-hoc covert observations that do not involve the systematic surveillance of a specific person(s)
- Unplanned observations made as an immediate response to events.

However staff should always remember that any actions taken must be justified and recorded.
In cases of doubt, the authorisation procedure described below should be followed.

Surveillance outside of RIPA

Due to the changes of the Serious Crime Criteria which commenced on the 1 November 2012 , there may be a necessity for the Council to undertake surveillance which does not meet the RIPA criteria such as, in cases of anti-social behavior involving disorder, or serious disciplinary investigations. The Council still must meet its obligations under the Human Rights Act and therefore any surveillance outside of RIPA must still be necessary and proportionate having taken account of the intrusion issues. The decision making process and the management of such surveillance must be well documented.

There is a requirement for the Councils Senior Responsible Officer (SRO) to regularly monitor surveillance outside of RIPA. Therefore before any such surveillance takes place, advice must be sought from the Head of Legal Services or the Senior Solicitor.

AUTHORISATION PROCEDURE

General

As mentioned earlier on 1 November 2012 two significant changes came into force that effects how local authorities use RIPA.

- **Approval of Local Authority Authorisations under RIPA by a Justice of the Peace**: The amendments in the Protection of Freedoms Act 2012 mean that local authority authorisations under RIPA for the use of Directed Surveillance or use of Covert Human Intelligence sources (CHIS) can only be given effect once an order approving the authorisation has been granted by a Justice of the Peace (JP). **This applies to applications and renewals only, not reviews and cancellations.**

- **Directed surveillance crime threshold**: Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of Directed Surveillance where the local authority is investigating criminal offences which attract a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

This crime threshold, as mentioned, is only for Directed Surveillance.

Application, Review, Renewal and Cancellation procedure

No covert activity covered by RIPA or the use of a CHIS should be undertaken at any time unless it meets the legal criteria (see above) and has been authorised by an Authorising Officer and approved by a JP/Magistrate as mentioned above. The activity conducted must be in strict accordance with the terms of the authorisation.

All the forms will be the Home Office Model approved forms downloaded from the Home Office Website and approved by the Council's RIPA Central Monitoring Officer. (See the List in the Annex).

Home Office forms, codes of practice and supplementary material will be available through the Council Intranet, the RIPA Central Monitoring Officer and the Home Office Website.

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-covert

The effect of the above legislation means that all applications and renewals for covert RIPA activity will have to have a JP's approval. It does not apply to Reviews and Cancellations which will still be carried out internally.

The procedure is as follows;

All applications and renewals for Directed Surveillance and use of a CHIS will be required to have a JP's approval.

The applicant will complete the relevant application form ensuring compliance with the statutory provisions shown above. The application form will be submitted to an Authorising Officer for consideration. If authorised, the applicant will also complete the required section of the judicial application/order form. Although this form requires the applicant to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

It will then be necessary within Office hours to arrange with Her Majesty's Courts & Tribunals Service (HMCTS) administration at the magistrates' court to arrange a hearing. The hearing will be in private and heard by a single JP

Officers presenting the application at these proceedings will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or provide information as required by the JP.

Upon attending the hearing, the officer must present to the JP the partially completed judicial application/order form, a copy of the RIPA authorisation form, together with any supporting documents setting out the case, and the original authorisation form.

The original RIPA authorisation should be shown to the JP but will be retained by the local authority so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT).

The JP will read and consider the RIPA authorisation and the judicial application/order form. They may have questions to clarify points or require additional reassurance on particular

matters. These questions are supplementary to the content of the application form**. However the forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided**.

The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. They will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

The JP may decide to

Approve the Grant or renewal of an authorisation
The grant or renewal of the RIPA authorisation will then take effect and the local authority may proceed to use the technique in that particular case.

Refuse to approve the grant or renewal of an authorisation
The RIPA authorisation will not take effect and the local authority may **not** use the technique in that case.

Where an application has been refused the applicant may wish to consider the reasons for that refusal. If more information was required by the JP to determine whether the authorisation has met the tests, and this is the reason for refusal the officer should consider whether they can reapply, for example, if there was information to support the application which was available to the local authority, but not included in the papers provided at the hearing.

For, a technical error, the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.

Refuse to approve the grant or renewal and quash the authorisation
This applies where the JP refuses to approve the authorisation or renew the authorisation and decides to quash the original authorisation. However, the court must not exercise its power to quash the authorisation unless the applicant has had at least 2 business days from

the date of the refusal in which to make representations. If this is the case the officer will inform the Legal section who will consider whether to make any representations.

Whatever the decision the JP will record their decision on the order section of the judicial application/order form. The court administration will retain a copy of the local authority RIPA authorisation form and the judicial application/order form. The officer will retain the original authorisation and a copy of the judicial application/order form.

If approved by the JP, the date of the approval becomes the commencement date and the three months duration will commence on this date. The officers are now allowed to undertake the activity.

The original RIPA authorisation form and the copy of the judicial application/order form should be forwarded to the Central Register and a copy retained by the applicant and by the AO. This will enable the AO to check what was authorised and monitor any reviews and cancellation to determine if any errors occurred and if the objectives were met.

There is no complaint route for a judicial decision unless it was made in bad faith. If the applicant has any issues they must contact the Legal Department for advice. A local authority may only appeal a JP decision on a point of law by Judicial Review. If such a concern arises, the Legal team will decide what action if any should be taken.

Responsibilities and Completion of the Relevant Forms

Applications

All applications for directed surveillance authorisation will be made on **Form 1** (reference ***RIPA 1 DS authorising*** form). All the relevant sections on an application form must be completed with sufficient information for the Authorising Officer to consider Necessity, Proportionality and the Collateral Intrusion issues. Risk assessments should take place prior to the completion of the application form. Each application should be completed on its own merits of the case. **Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.**

All applications will be submitted to the Authorising Officer via the Line Manager of the appropriate enforcement team, in order that they are aware of the activities being undertaken by the staff. The Line Manager will perform an initial quality check of the application. However they should not be involved in the sanctioning of the authorisation.

Applications whether authorised or refused will be issued with a unique number by The Councils RIPA Central Monitoring Officer (Corporate Fraud Manager).

If authorised the applicant will then complete the relevant section of the judicial application/order form and follow the procedure above by arranging and attending the Magistrates Court to seek a JP's approval. (see procedure above RIPA application and authorisation process)

Reviews

The reviews are dealt with internally by submitting the review form to the authorising officer. There is no requirement for a review form to be submitted to a JP.

All applications for review of directed surveillance authorisation will be made on **Form 2** (reference ***RIPA 2 DS review*** form**)**.

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

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

Applicants should submit a review form by the review date set by the Authorising Officer. They should also use a review form for changes in circumstances to the original application so that the need to continue the activity can be reassessed. However if the circumstances or the objectives have changed considerably or the techniques to be used are now different, a new application form should be submitted and will be required to follow the process again and be approved by a JP. If in doubt seek advice... The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

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

Renewal

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. Should it be necessary to renew a Directed Surveillance or CHIS authorisation this must be approved by a JP

All applications for directed surveillance renewals will be made on **Form 3** (reference ***RIPA 3 DS* renewal** form).

Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant authorising officer and a JP to consider the application).

The applicant should complete all the sections within the renewal form and submit the form to the authorising officer.

Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

If the authorising officer refuses to renew the application the cancellation process should be completed. If the AO authorises the renewal of the activity the same process is to be followed as mentioned earlier for the initial application.

A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

Cancellation

Where authorisation ceases to be either necessary or proportionate the Authorising Officer or appropriate deputy will cancel an authorisation using **Form 4** (reference ***RIPA 4 DS cancellation*** form).

The cancellation form is to be submitted by the applicant or another investigator in their absence. The Authorising Officer who granted or last renewed the authorisation must cancel it if they are satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the Authorising Officer is no longer available, this duty will fall on the

person who has taken over the role of Authorising Officer or the person who is acting as Authorising Officer

As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation should inform the Authorising Officer. The Authorising Officer will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given should also be recorded in the central record of authorisations (see paragraphs 5.18 in the Codes of Practice). **It will also be necessary to detail the amount of time spent on the surveillance .**

The officer submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and what if any images were obtained and any images containing third parties. The Authorising Officer should then take this into account and issue instructions regarding the management and disposal of the images etc.

The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight.

Applications for directed surveillance will be made only to an Authorising Officer. The names and posts of such officers may be found recorded in a list held for that purpose by the RIPA Central Monitoring Officer (see the List in the Annex). Authorising Officers will be, as a minimum, Heads of Service. Any nomination of such an officer in that list empowers those officers in line above them to act in their place. Officers responsible for management of an investigation will normally be no lower than Activity Manager.

Authorising officers shall ensure they are fully aware of their responsibilities and comply with the requirements of the law including the relevant codes of practice and the Council's policies and procedures in respect to the authorisation, review, renewal and cancellation of authorisations for covert surveillance. They shall ensure a satisfactory risk assessment, including the Health and Safety of staff is completed in respect of each authorisation.

Where an application for authorisation is refused the Authorising Officer shall record the refusal on the application and the reasons for it on the case file and supply a copy of it to the RIPA Central Monitoring Officer as with other authorisations. The Authorising Officer shall

also ensure that any supplementary information and supporting documents submitted with any application for authorisation, review, renewal or cancellation are recorded and retained on the case file as required by the codes of practice or other legal requirement.

Immediate response to events

There may be occasions when officers come across events unfolding which were not pre planned which then requires them to carry out some form of observation. This will not amount to Directed Surveillance. Officers must not abuse the process and be prepared to explain their decisions in court should it be necessary. Therefore they should document their decisions, what took place, what evidence or information was obtained.

Joint Agency Surveillance

In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the police. If it is a joint operation involving both agencies the lead agency should seek authorisation.

Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the application to carry out the activity. When staff are operating on another organisation's authorisation they are to ensure they see what activity they are authorised to carry out and make a written record. They should also inform the RIPA Central Monitoring Officer of the unique reference number, the agencies involved and the name of the officer in charge of the surveillance. This will assist with oversight of the use of Council staff carrying out these types of operations.

Documentation and Central Record

Authorising Officers or Managers of relevant enforcement departments may keep whatever records they see fit to administer and manage the RIPA application process. However this will not replace the requirements under the Codes of Practice for the Council to hold a centrally held and retrievable record.

A centrally retrievable record of all authorisations will be held by the RIPA Central Monitoring Officer and updated whenever an authorisation is refused, granted, renewed or cancelled. The record will be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners, upon request. These records should be retained for at least three years from the ending of the authorisation or for the period stipulated by the Council's document retention policy, whichever is greater.

Use of CCTV

The use of the CCTV systems operated by the Council do not normally fall under the RIPA regulations. However it does fall under the Data Protection Act 1998 and the Council's CCTV policy**.** However should there be a requirement for the CCTV cameras to be used for a specific purpose to conduct surveillance it is likely that the activity will fall under Directed Surveillance and therefore require an authorisation.

On the occasions when the CCTV cameras are to be used in a Directed Surveillance situation either by enforcement officers from relevant departments within the Council or outside Law Enforcement Agencies such as the Police, either the CCTV staff are to have a copy of the application form in a redacted format, or a copy of the authorisation page. If it is an urgent oral authority, a copy of the applicant's notes are to be retained or at least some other document in writing which confirms the authorisation and exactly what has been authorised. It is important that the staff check the authority and only carry out what is authorised. A copy of the application or notes is also to be forwarded to the Central Monitoring Officer for filing. This will assist the Council to evaluate the authorisations and assist with oversight.

Operators of the Councils CCTV system need to be aware of the RIPA issues associated with using CCTV and that continued, prolonged systematic surveillance of an individual may require an authorisation.

The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what they stated was necessary in the application form. This check will form part of the oversight function. Where issues are identified they will be brought to the attention of the line manager and the Senior Responsible Officer (SRO). This will assist with future audits and oversight.

Any person granting an authorisation for the use of directed surveillance must record on the appropriate form the matters they took into account in reaching their decision and they must be satisfied that :

- **no overt means** are suitable for the purpose
- the authorisation is for a prescribed lawful purpose (see above)
- account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated/targeted in the operation or investigation (**collateral intrusion**)

- measures are be taken, where ever practical, to avoid unnecessary intrusion into the lives of those affected by collateral intrusion.
- the authorisation is necessary.
- the authorised surveillance proposed is proportionate;
- any equipment to be used and its technical capabilities is specified

Necessity

Surveillance operations shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s).

Effectiveness

Surveillance operations shall be undertaken only by suitably trained or experienced employees (or under their direct supervision).

Proportionality

The use of surveillance shall not be excessive but shall be in proportion to the significance/harm of the matter being investigated. (i.e. don't use a sledge hammer to crack a nut).

Authorisation

All directed surveillance shall be authorised in accordance with this procedure.

Use of a Covert Human Intelligence Source (CHIS)

The use of CHIS should only be considered in exceptional cases and after consulting the Legal Section to ensure it is appropriate and all safeguards needed are in place.

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

a) the identity of the source;

b) the identity, where known, used by the source;

c) any relevant investigating authority other than the authority maintaining the records;

d) the means by which the source is referred to within each relevant investigating authority;

e) any other significant information connected with the security and welfare of the source;

f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (e) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

g) the date when, and the circumstances in which, the source was recruited;

h) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);

i) the periods during which those persons have discharged those responsibilities;

j) the tasks given to the source and the demands made of him in relation to his activities as a source;

k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

l) the information obtained by each relevant investigating authority by the conduct or use of the source;

m) any dissemination by that authority of information obtained in that way; and

n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect or the source's activities for the benefit of that or any other relevant investigating authority.

In addition the Code of Practice requires records to be kept of:

- a copy of the authorisation together with the supporting documentation and notification of the approval given by the authorising officer;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorisation considered it necessary to do so;
- any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- any risk assessment made in relation to the source;
- the circumstances in which tasks were given to the source;
- the value of the source to the investigating authority;
- a record of the results of any reviews of the authorisation;
- the reasons, if any, for not renewing an authorisation;

- the reasons for cancelling an authorisation;
- the date and time when any instruction was given by the authorising officer to cease using a source.

Authorising Officers must not grant an authorisation for a CHIS unless they believe that there are arrangements in place to ensure there is at all times a person responsible for maintaining a record of the use of that source.

All applications for authorisation for the use or conduct of a CHIS will be made on **Form 5** (reference ***RIPA 5 CHIS authorising*** form). The applicant in all cases should complete this.

The application process is the same as described earlier with the authorisation (if authorised) requiring the approval of a Justice of the Peace.

All applications for review of authorisation for the use or conduct of a CHIS will be made on **Form 6** (reference ***RIPA 6 CHIS review*** form). The applicant in all cases should complete this where the investigation/operation is to be continued.

All applications for authorisation for the use or conduct of a CHIS renewal will be made on **Form 7** (reference ***RIPA 7 CHIS renewal*** form). The applicant in all cases should complete this where the surveillance requires to continue beyond the previously authorised period (including previous renewal). The renewal will require approval of a Justice of the Peace.

Where authorisation ceases to be either necessary or appropriate the Authorising Officer or appropriate deputy will cancel an authorisation using **Form 8** (reference ***RIPA 8 CHIS cancellation*** form).

Any person giving an authorisation for the use of CHIS must record on the appropriate form matters taken into account in reaching their decision and must be satisfied that :

- **no overt means** are suitable for the purpose
- the authorisation is for a prescribed lawful purpose (see above)
- account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated/targeted in the operation or investigation (**collateral intrusion**)
- measures must be taken, where ever practical, to avoid unnecessary intrusion into the lives of those affected by collateral intrusion.
- the authorisation is necessary.

- the authorised surveillance proposed is proportionate;
- any equipment to be used is specified

Necessity

Surveillance operations shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s).

Effectiveness

Surveillance operations shall be undertaken only by suitably trained or experienced employees (or under their direct supervision).

Proportionality

The use of surveillance shall not be excessive but shall be in proportion to the significance/harm of the matter being investigated. (i.e. don't use a sledge hammer to crack a nut).

Authorisation

All directed surveillance shall be authorised in accordance with this procedure.

Persons who repeatedly provide information

It is possible that members of the public repeatedly supply information to Council staff on either one particular subject or investigation or a number of investigations. It is important that Council staff make the necessary enquiries with the person reporting the information to ascertain how the information is being obtained. This will not only assist with evaluating the information but will determine if the person is establishing or maintaining a relationship with a third person to obtain the information, and then provide it to the Council staff. If this is the case, the person is likely to be acting as a CHIS and there is a potential duty of care to the individual which a duly authorised CHIS would take account of. Therefore Council staff should ensure that they are aware of when a person is potentially a CHIS by reading the below sections.

DURATION TIME OF AUTHORISATIONS

Directed Surveillance	3 Months
Renewal	3 Months
Covert Human Intelligence Source	12 Months
Renewal	12 months
Juvenile Sources	1 Month

All authorisations commence from the date approved by the Justice of the PEACE.

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

RECORD KEEPING, TRAINING AND MONITORING

Security and Retention of Records

Each service division or discrete location within a division, must maintain a record of all applications for authorisations (including refusals), Judicial application/order form, renewals, reviews and cancellations on the appropriate form. Each individual form must be given a unique reference number issued by the RIPA Central Monitoring Officer. Such unique reference numbers should follow on in sequential order from that used for previous forms. The most Authorising Officer in that service division or that location may maintain records for directed surveillance and covert human intelligence sources for their own records.

The Authorising Officer shall retain together the original authorisation, copy of the Judicial application/order form, review and renewal forms, copies being provided to the Central Monitoring Officer, until cancelled. On cancellation, the original application, review, renewal and cancellation forms and any associated documents shall be sent to the Central Monitoring Officer and retained in a file in a secure place for three years after cancellation, as required by the Act.

The codes do not affect any other statutory obligations placed the Council to keep records under any other enactment such as the Criminal Procedure and Investigations Act 1996 (CPIA) This requires that material which is obtained in the course of an investigation and which may be relevant to the investigation must be recorded, retained and revealed to the prosecutor.

Training

The Senior Responsible Officer will have responsibility for ensuring appropriate training for staff mentioned within this policy and for retaining a record of that training. They must supply a copy of the record to the RIPA Central Monitoring Officer at regular intervals.

Central Register

The RIPA Central Monitoring Officer will maintain the Central Register of Authorisations. Authorising Officers shall notify the RIPA Central Monitoring Officer within 48 hours of the grant, renewal or cancellation of any authorisation and the name of the applicant officer to ensure the accuracy of the central register.

Oversight

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

Errors

There is now a requirement as set out in the OSC procedures and Guidance 2011 to report all covert activity that was not properly authorised to the OSC in writing as soon as the error is recognised. This includes activity which should have been authorised but wasn't or which was conducted beyond the directions provided by the authorising officer. It is therefore important that when an error has been identified it is brought to the attention of the SRO in order to comply with this guidance. The Council has a responsibility to report to the Inspector at the commencement of an inspection all activity which should have been authorised but wasn't. This is to confirm that any direction provided by the Chief Surveillance Commissioner has been followed. This will also assist with the oversight provisions of the Councils' RIPA activity.

This does not apply to covert activity which is deliberately not authorised because an authorising officer considers that it does not meet the legislative criteria, but allows it to continue. This would be surveillance outside of RIPA. (See oversight section below)

Senior Responsible Officer

Overall oversight within the Council will fall within the responsibilities of the Senior Responsible Officer (SRO) for the Council. The SRO is responsible for:

- the integrity of the process in place within the *public authority* to authorise directed surveillance
- compliance with Part II of the 2000 Act, Part III of the 1997 Act and with this code;
- engagement with the Commissioners and inspectors when they conduct their inspections, and
- where necessary, overseeing the implementation of any post inspection action plans recommended or approved by a Commissioner

Reporting to Members

Annual returns of all surveillance activity undertaken by Council staff including joint surveillance and Directed Surveillance using the CCTV system will be compiled by the RIPA Central Monitoring Officer and provided to the Corporate Governance Panel annually in line with the current advice in the Codes of Practice. Members will review on a yearly basis the policy to assess whether the activity undertaken is in line with this policy.

The Office of Surveillance Commissioners

The Office of Surveillance Commissioners provides an independent overview of the use of powers contained within the Regulation of Investigatory Powers Act 2000. This scrutiny includes inspection visits to local authorities by inspectors appointed by the OSC and the provision of annual reports by the Council to the OSC on all relevant surveillance activity undertaken as part of this policy.

It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information he requires for the purpose of enabling him to carry out his functions.

The Office of Surveillance Commissioners may be contacted at :

Office of Surveillance Commissioners
PO Box 29105
London SW1V 1ZU
Telephone : 020 7828 3421
www.surveillancecommisoners.gov.uk

The Regulation of Investigatory Powers Act 2000 also establishes an independent tribunal, the **Investigatory Powers Tribunal**. This has full powers to investigate and decide any cases within its jurisdiction.

ADVICE

If you require further advice about covert surveillance, please contact the RIPA Central Monitoring Officer. In particular advice should be sought before considering the use of a covert human intelligence source where considerations of risk assessment, insurance, managing tasking the source and ensuring confidentiality require specific consideration.

POLICY UPDATING PROCEDURE

Proposed amendments to this Policy must be forwarded to the Head of Legal and Democratic Services where they will be considered in consultation with the RIPA Central Monitoring Officer before submission to Chief Officers Management Team and Cabinet.

The Policy shall be reviewed as required by legislation, upon advice from the Home Office or following a bi-annual inspection by the OSC.

FURTHER INFORMATION ENQUIRIES AND COMPLAINTS

The RIPA Central Monitoring Officer is the first point of contact on any of the matters raised in this policy statement. Enquiries should be addressed to:

The RIPA Central Monitoring Officer
Fraud Section
Huntingdonshire District Council
Pathfinder House
St Mary's Street
Huntingdon
Cambridgeshire
PE29 3TN
Tel : (01480) 388388 or direct dial (01480) 388022

The RIPA Central Monitoring Officer is the Council's Fraud Manager and will be responsible for dealing with all internal and external enquiries and complaints. All complaints should be in writing, dated and include details of the complaint and also an account of the nature of the problem.

The Council will attempt to complete internal investigations within 20 working days. An acknowledgement of the complaint should be despatched to the complainant as soon as possible after its receipt.

Nick Jennings
Corporate Fraud Manager
31.5.2013

ANNEX A

HOME OFFICE MODEL FORMS

RIPA 1DS Authorising Form

RIPA 2DS Review Form

RIPA 3DS Renewal Form

RIPA 4DS Cancellation Form

RIPA 5CHIS Authorising Form

RIPA 6CHIS Review Form

RIPA 7CHIS Renewal Form

RIPA 8CHIS Cancellation Form

Note:
DS : Directed Surveillance
CHIS : Covert Human Intelligence Source

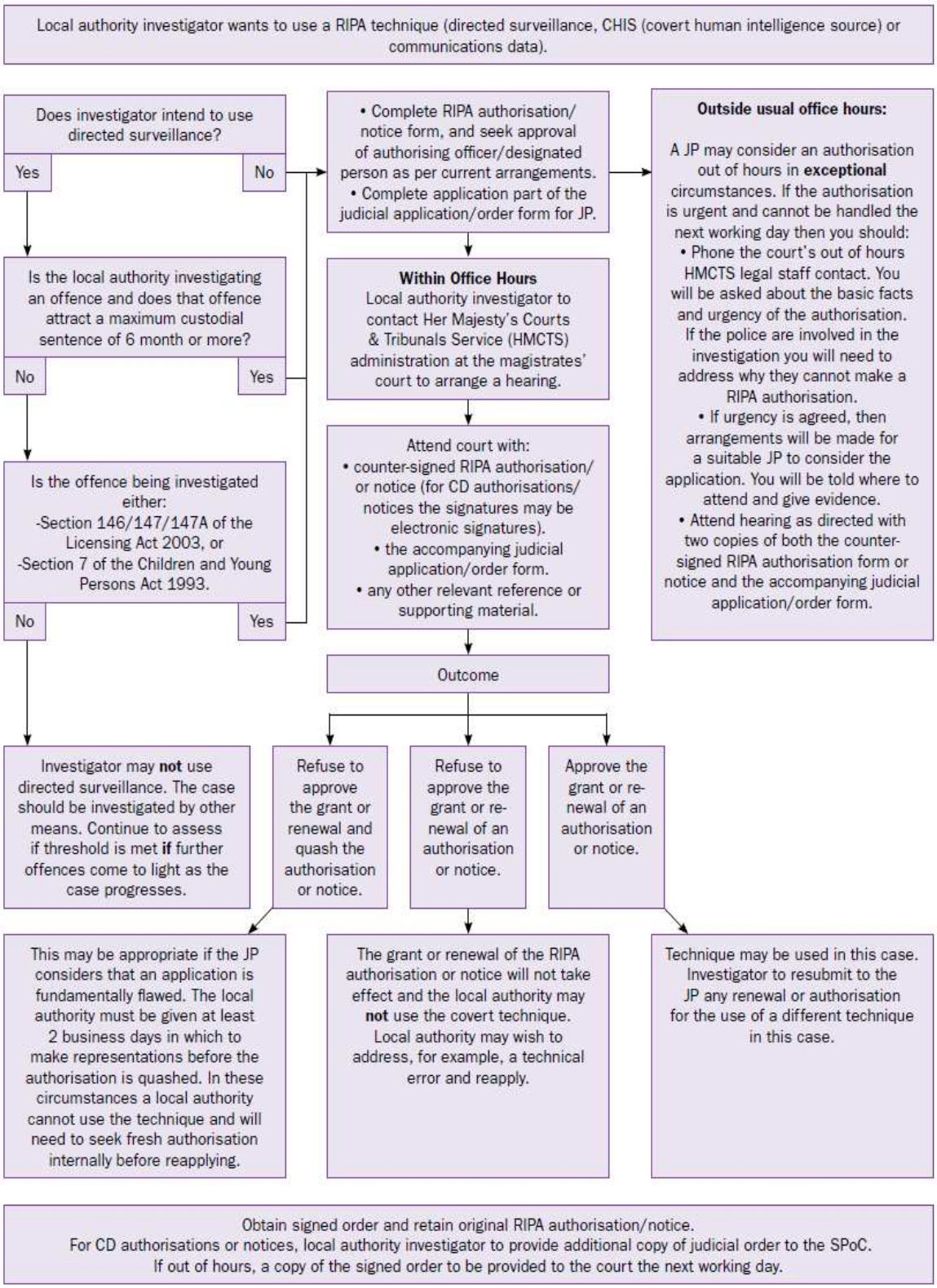
ANNEX B

LIST OF OFFICERS ROLES

ROLE	SERVICE	POST	POST HOLDER
Central Monitoring Officer	Council-wide	Fraud Manager	Nick Jennings
Senior Responsible Officer	Council-Wide	Head of Legal and Democratic Services	Colin Meadowcroft
Senior Authorising Officer	Council-Wide	Head of Paid Service	Malcolm Sharp
Authorising Officer	Customer Services	Head of Customer Service	Julia Barber
Authorising Officer	Environmental Health and Community Services	Head of Environmental Health Services	Sue Lammin
Authorising Officer	Planning Services	Head of Planning Services	Steve Ingram
Authorising Officer	Head of Operations Division	Head of Service-Operations Division	Eric Kendall

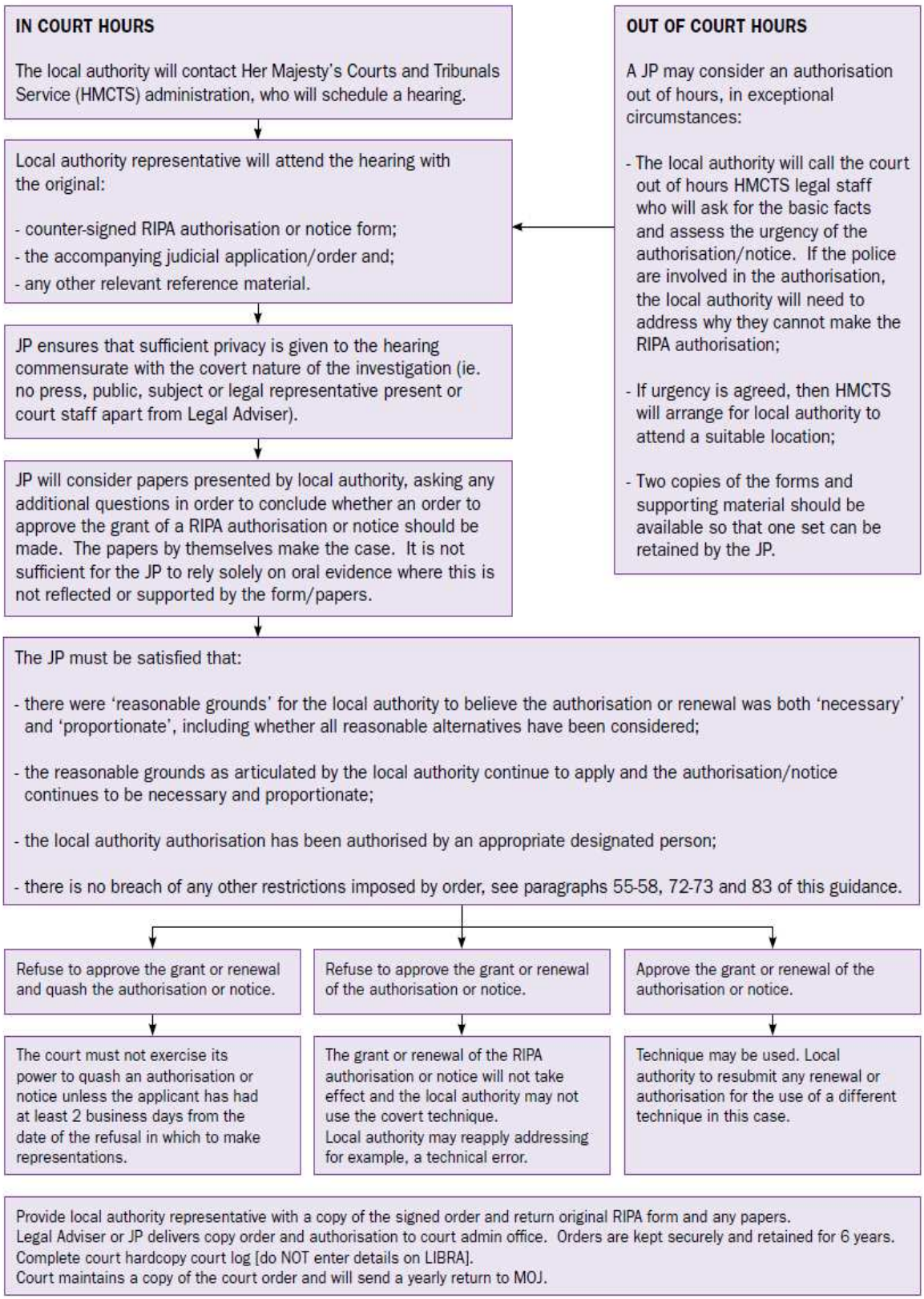
Annex C

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



Annex D

PROCEDURE: LOCAL AUTHORITY APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



Annex E

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local thority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....

.....

.....

.....

.....

.....

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

Order made on an application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Magistrates' court:.....

Having considered the application, I (tick one):

☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

HUNTINGDONSHIRE DISTRICT COUNCIL

ACQUISITION OF COMMUNICATIONS DATA

REGULATION OF INVESTIGATORY POWERS ACT 2000
(PART I, CHAPTER II)

POLICY & PROCEDURE

CONTENTS

INTRODUCTION

The powers provided by the Regulation of Investigatory Powers Act 2000 (RIPA) allow the Council to obtain Communications Data to progress Criminal Investigations from Communications Service Providers (CSP's). It is not to be confused with the Councils Monitoring at Work Policy and Practices under the Lawful Business Practices Legislation. This latter legislation relates to the monitoring of the Council's own communication and computer systems.

Part 1 of RIPA introduces a statutory framework to regulate the access to communications data by public authorities consistent with the Human Rights Act 1998. All applications for Communications Data will be made through one of the Council's Accredited Officers known as Single Point of Contacts (SPoC's) who have passed a Home Office approved course. These Officers are based in the Councils Fraud Team located at Pathfinder House. One centrally held record will be maintained by the SPoC's to prevent duplication of acquiring communications data. This will also assist with the councils responsibilities with regard to record keeping.

This Policy sets out the Councils procedures and approach to obtaining and handling Communications Data for the purposes of preventing or detecting crime or of preventing disorder. It should be read in conjunction with the Home Office Interception of Communications Data Code of Practice (the codes) which explains the duties and responsibilities placed upon each party involved in these processes and creates a system of safeguards, consistent with the requirements of article 8 of the ECHR http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/interception-comms-code-practice . This policy will be reviewed periodically.

The Codes can be obtained from the Home Office Website and are available to all Council staff involved in the acquisition of Communications Data.

Both this policy and the Codes of Practice will be followed at all times and under no circumstances should unauthorised access to obtain Communications Data be sought outside of this guidance or by requiring, or inviting, any postal or telecommunications

operator to disclose communications data by exercising any exemption to the principle of non-disclosure of communications data under the Data Protection Act 1998 ('the DPA').

The Codes of Practice are admissible in evidence in criminal and civil proceedings.

A Communications Service Provider (CSP's) is an operator who provides a postal or telecommunications service such as Royal Mail and the usual Telephone Service providers as well as Internet Service Providers.

What is Communications Data

Communications Data does not include the contents of any communication. It is not lawfully possible for Council employees under any circumstances to obtain the contents of communications. SPoC/Accredited officers will ensure they are aware and remain up to date with the less obvious communications data which would constitute contents such as email headers.

The term 'communications data' embraces the 'who', 'when' and 'where' of a communication but not the content, not what was said or written. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within a communication including text, audio and video (with the exception of traffic data to establish another communication such as that created from the use of calling cards, redirection services, or in the commission of 'dial through' fraud and other crimes where data is passed on to activate communications equipment in order to obtain communications services fraudulently).

Consultation with the Council's Single Point of Contact (SPoC) will determine the most appropriate plan for acquiring data where the provision of a communication service engages a number of providers. It may be advisable that applicants seek advice and guidance when where enquiries regarding communications data are being considered within an investigation.

Types of Communications Data

There are three types of Communications Data which may be obtained dependant upon what the legislation allows the Public Authority to lawfully acquire. They are:

(a) Traffic Data

(b) Service Use Information

(c) Subscriber/ Account information

Huntingdonshire District Council has no lawful authority to obtain Traffic Data. However it can lawfully obtain Service Use data and Subscriber/Account information if the application meets the test of Necessity and Proportionality which will be decided by the Designated Person (Authorising Officer).

Traffic Data

The Act defines certain communications data as 'traffic data' in sections 21(4)(a) and 21(6) of the Act. This is data that is or has been comprised in or attached to a communication for the purpose of transmitting the communication and which 'in relation to any communication':

Examples of traffic data, within the definition in section 21(6), include:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);

- information identifying the location of equipment when a communication is, has been or may be made or received (such as the location of a mobile phone);

- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or

attached to the communication;

- routing information identifying equipment through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed);

- web browsing information to the extent that only a host machine, server, domain name or IP address is disclosed;

- anything, such as addresses or markings, written on the outside of a postal item (such as a letter, packet or parcel) that is in transmission and which shows the item's postal routing;

- record of correspondence checks comprising details of traffic data from postal items in transmission to a specific address, and

- online tracking of communications (including postal items and parcels).

Any message written on the outside of a postal item, which is in transmission, may be content (depending on the author of the message) and fall within the scope of the provisions for interception of communications for which Council has no Authority to obtain. For example, a message written by the sender will be content but a message written by a postal worker concerning the delivery of the postal item will not. All information on the outside of a postal item concerning its postal routing, for example the address of the recipient, the sender and the post-mark, is traffic data within section 21(4)(a) of the Act.

Huntingdonshire District Council has no lawful authority to obtain Traffic Data.

Service Use Information

Data relating to the use made by any person of a postal or telecommunications service, or any part of it, is widely known as 'service use information' and falls within section 21(4)(b) of the Act and the Council can lawfully obtain this data..

Examples of data within the definition at section 21(4)(b) include:

- itemised telephone call records (numbers called);
- itemised records of connections to internet services;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded;
- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about the use of forwarding/redirection services;
- information about selection of preferential numbers or discount calls;
- records of postal items, such as records of registered post, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

Subscriber Information

The third type of communication data, widely known as 'subscriber information', is set out in section 21(4)(c) of the Act. This relates to information held or obtained by a CSP about persons to whom the CSP provides or has provided a communications service. Those persons will include people who are subscribers to a communications service without necessarily using that service and persons who use a communications service without necessarily subscribing to it, and the Council can lawfully obtain this data

Person includes any organisation and any association or combination of persons.

Examples of data within the definition at section 21(4) (c) include:

- 'subscriber checks' (also known as 'reverse look ups') such as "who is the subscriber of phone number 012 345 6789?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space *www.example.co.uk*?";

- information about the subscriber to a PO Box number or a Postage Paid Impression used on bulk mailings;

- information about the provision to a subscriber or account holder of forwarding/redirection services, including delivery and forwarding addresses;

- subscribers or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;

- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed to (or may have subscribed to) including

conference calling, call messaging, call waiting and call barring telecommunications services;

- information about apparatus used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes;

- information provided by a subscriber or account holder to a CSP, such as demographic information or sign-up data (to the extent that information, such as a password, giving access to the content of any stored communications is not disclosed.

The SPoC will provide advice and assistance with regard to the types of Communications Data which can be lawfully obtained and how that data may assist with an investigation.

Who Can We Obtain the Data From and For What reason?

Communications data can be obtained from a Communications Service Provider (CSP's) A CSP is an operator who provides a postal or telecommunications service such as Royal Mail and the usual Telephone Service providers. However there may be less obvious companies which may be classed as a CSP and advice should be sought from the SPoC.

Council can only process and consider applications to access Communications Data from within this Authority. Under no circumstances will applications be accepted for outside authorities/agencies. However, it may be necessary during joint investigations to obtain Communications Data. If this becomes necessary it is important that we are not bending the rules and applying or using the data where we would not normally be allowed to either access the data or that the other organisation has no lawful power to obtain Communications Data.

Lawful Reason to Access Communications Data

The Council's only lawful reason to access Communications Data is for

- the purpose of preventing or detecting crime or of preventing disorder;

Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed.

Using Other Powers

The codes state where a public authority seeks to obtain communications data using provisions providing explicitly for the obtaining of communications data (other than Chapter II of Part I of the Act) or using statutory powers conferred by a warrant or order issued by a person holding judicial office, the SPoC should be engaged in the process of obtaining the data to ensure effective co-operation between the public authority and the CSP.

Although there is some limited provision for obtaining some low grade Communications Data by other Statutory means such as The Social Security Administration Act the position of this Council is that the RIPA legislation will be used.

Should it be necessary to obtain Communications Data via other means such as a court order or should data be required from a CSP which falls outside of the definition of Communications Data the application should be handled by a SPoC.

The Two Ways of Obtaining Communications Data

The legislation provides two different methods of acquiring communications data (see below). The SPoC will provide advice regarding the method to be used and complete the relevant form.

The two methods

- an Authorisation under section 22(3), or
- a Notice under section 22(4).

An Authorisation (see Authorisation Form) should be used to obtain all section 21(4)(c) data (see page 8) unless it is being requested from the same provider as the inextricably linked service use data under section 21(4)(b) such as itemised billing. Both would normally be requested using a Notice in these circumstances. It will be the role of the SPoC to determine which method should be used. Unless using an automated system the Authorisation will be forwarded to the CSP by the SPoC.

Note
Although this is the advice of the Home Office, some CSPs state that they require a notice for data which is not obtained from their automated system. The SPoC will determine the correct method to be used.

Notices and Authorisations
A Notice and Authorisation are documents which when authorised and approved by a Justice of the Peace are forwarded to the CSP by the SPoC. Both are virtually identical documents requesting the CSP to provide the data which would usually be returned to the SPoC. However, a Notice is a Legal document which the CSP has to comply with. The decision of a designated person whether to give a Notice or Authorisation shall be based upon information presented to them in an application form.

Ordinarily the CSP should disclose, in writing or electronically, the communications data to which a Notice or an authorisation relates not later than the end of the period of ten working days from the date the Notice is served upon the CSP. Should the data not be returned within this period they should only be contacted by the SPoC.

The original Authorisation or Notice will be retained by the SPoC within the public authority

Duration of Authorisations and Notices

As from 1 November 2012 there is a requirement for authorisations and notices to be approved by a Justice of the Peace (JP). From the date that the authorisation or notice is approved by the JP, (which follows its authorisation by the DP), it has a validity of a maximum of one month. This means the conduct authorised should have been commenced or the notice served within that month.

Realistically there should be no significant delay between the application being approved by the JP and the request to obtain the data.

A month means a period of time extending from a date in one calendar month to the date one day before the corresponding or nearest date in the following month. For example, a month beginning on 7 June ends on 6 July, a month beginning on 30 January ends on 28 February or 29 February in a leap year.

Internal Investigations

The Codes state where an investigation relates to an allegation of criminal conduct by a member of a public authority, that public authority (or another public authority appointed to investigate the complaint) may use their powers under Part 1 Chapter II to obtain communications data for the purpose of preventing and detecting the alleged or suspected crime where the investigating officer intends the matter to be subject of a prosecution within a criminal court. Should it be determined there are insufficient grounds to continue the investigation or insufficient evidence to initiate a prosecution within a criminal court, it will, with immediate effect, no longer be appropriate to obtain communications data under the Act.

If Communications Data is sought in connection with internal staff committing crimes against the Council it is important that the enquiry is a genuine Criminal Investigation with a view to proceeding Criminally as opposed to just a Disciplinary matter.

Advice may be required from the Councils Legal section if this arises.

Roles of Staff Involved in the Process

Acquisition of communications data under the Act involves four roles within a relevant public authority. A list of the Officers who have authority to act for Huntingdonshire District Council in these matters is attached in **ANNEX A**.

The Applicant

The applicant is a person involved in conducting an investigation or operation who makes an application in writing for the acquisition of communications data. The applicant completes an application form, setting out for consideration by the designated person, the necessity and proportionality of a specific requirement for acquiring communications data. Prior to the completion of the relevant paperwork it may be advisable to consult with the SPoC.

The Designated Person

The Designated Person (DP) is a person holding a prescribed office in a relevant public authority and who considers the application for Authorisation much the same as a Surveillance RIPA application.

Individuals who undertake the role of a designated person must have current working knowledge of human rights principles, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data.

The Designated person must hold a position within the Council that meets the level specified in the Act and in particular noted in *SI 2010 No.480 Investigatory Powers, The Regulation of Investigation Powers (Communications Data) Order 2010.*

The designated person shall assess the necessity for any conduct to acquire or obtain communications data taking account of any advice provided by the SPoC. They will also assess the issue of proportionality taking into account any meaningful collateral intrusion issues. These responsibilities take place prior to seeking approval by a JP.

Designated persons should not be responsible for granting Authorisations or giving Notices in relation to investigations or operations in which they are directly involved,

The Single Point of Contact

The single point of contact (SPoC) is either an accredited individual (Home Office Course) or a group of accredited individuals trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and CSPs. They will have been issued a SPoC Personal Identification Number (PIN). Details of all accredited individuals are available to CSP's for authentication purposes.

Under no circumstances will a SPoC allow anyone to use their PIN number.

An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for communications data are undertaken. The SPoC provides objective judgement and advice to both the applicant and the designated person. In this way the SPoC provides a "guardian and gatekeeper" function ensuring that public authorities act in an informed and lawful manner.

SPoC's should be conversant with their role and all the relevant contents within the codes of practice.

The SPoC should be in a position to:

- engage proactively with applicants to develop strategies to obtain communications data and use it effectively in support of operations or investigations;

- assess whether the acquisition of specific communications data from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data

- advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of CSPs;

- advise applicants and designated persons on the interpretation of the Act, particularly whether an Authorisation or Notice is appropriate;

- provide assurance to designated persons that Authorisations and Notices are lawful under the Act and free from errors;

- provide assurance to CSPs that Authorisations and Notices are authentic and lawful;

- assess whether communications data disclosed by a CSP in response to a Notice fulfils the requirement of the Notice;

- assess whether communications data obtained by means of an Authorisation fulfils the requirement of the Authorisation;

- assess any cost and resource implications to both the public authority and the CSP of data requirements.

The SPoC will retain the original of all the documents involved in the process. Copies of the documents may be retained by the applicant, Designated Person or within the relevant department for audit and filing purposes.

For the purposes of Huntingdonshire District Council, to demonstrate fairness, all three roles will be performed within the application process by separate officers.

The Senior Responsible Officer

The senior responsible office will be responsible for:

- the integrity of the process in place within the public authority to acquire communications data;

- compliance with Chapter II of Part I of the Act and with this code;

- oversight of the reporting of errors to Interception of Communications Commissioners Office (IOCCO) and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;

- engagement with the IOCCO inspectors when they conduct their inspections, and

- where necessary, oversee the implementation of post-inspection action plans approved by the Commissioner.

The SRO will liaise with the Council's SPoC's and DP's to ensure that the relevant systems and knowledge are of a required standard to comply with their role.

The Application Process

On 1 November 2012 a significant change came into force that effects how local authorities use RIPA to access Communications Data. There is now a requirement under the amendments in the Protection of Freedoms Act 2012, following the acquisition of the Communications Data being authorised by the DP to seek the approval of Local Authority Authorisations and Notices under RIPA by a Justice of the Peace(JP). A Judicial Application/Order form will be completed by either the SPoC or the applicant will be required to attend court and seek the approval of the Justice of the Peace. The original application and a copy will have to be produced to the JP who will either approve or refuse it. The original application will then be retained together with a copy of the Judicial Application/Authorisation form. A copy of the original application form will be retained by the JP.

Prior to an applicant applying for communications data the applicant should contact a SPoC who will be in a position to advise them regarding the obtaining and use of communications data within their investigation. This will reduce the risk of the applicant applying for data which we are not able to obtain and it will also assist the applicant to determine their objectives and apply for the most suitable data for those particular circumstances.

Necessity and Proportionality

The acquisition of communications data under the Act will be a justifiable interference with an individual's human rights under Article 8 of the European Convention on Human Rights only if the conduct being authorised or required to take place is both necessary and proportionate and in accordance with law. Designated Persons who can authorise applications on behalf of this Council will need to have some training with regard to the Human Rights Act and in particular necessity, proportionality and the collateral intrusion issues which may arise with regard to obtaining Communications Data.

The designated person must believe that the conduct required by any Authorisation or Notice is necessary. They must also believe that the conduct to be proportionate to what is sought to be achieved by obtaining the specified communication data – that the conduct is no more than is required in the circumstances. This involves balancing the

extent of the intrusiveness of the interference with an individual's right of respect for their private life against a specific benefit to the investigation or operation being undertaken.

Consideration must also be given to any actual or potential infringement of the privacy of individuals who are not the subject of the investigation or operation. They should consider any meaningful degree of collateral intrusion.

Designated Persons should give particular consideration to any periods of days or shorter periods of time for which they may approve for the acquisition of data. They should specify the shortest period in which the objective for which the data is sought can be achieved. To do otherwise will impact on the proportionality of the Authorisation or Notice and impose unnecessary burden upon a CSP given such Notice.

What Forms Will be Used

Below is a list of forms which will be used for the process of obtaining Communications Data. The SPoC's complete most of the forms once the application has been submitted. The SPoC's will therefore ensure that they have the necessary knowledge in how to complete the required paperwork.

- Application Form (to be completed by applicant)
- SPoC Officers Rejection Form (to be completed by the SPoC if necessary)
- SPoC Officers Log Sheet (to be completed by the SPoC)
- SPoC Officers section of the application form
- Draft Notice (to be completed by the SPoC)
- Authorisation form (to be completed by the SPoC if necessary)
- Schedule form (to be completed by the applicant for consequential data)

- Applicants Cancellation Form (to be completed by applicant when necessary and forwarded to the SPoC)

- Notice Cancellation Form (to be completed by the SPoC and forwarded to relevant CSP)

- Authorisation Cancellation Form (to be completed by the SPoC when necessary)

- Error Reporting Letter (to be completed by the SPoC and forwarded to Interception of Communications Commissioners Office (IOCCO)

Up to date version of some these forms can be obtained from the Home office Website http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms other forms can be obtained from the intranet page a HDC.

Application

All applications will be submitted by the applicant in writing using the application forms which can be obtained from the Home Office website to ensure they are relevant and up to date. All the relevant sections should be completed fully as the DP can only consider authorization based on the content of the application form. The details contained within the application form must take account of the objectives, necessity, proportionality and any meaningful degree of collateral intrusion. Should it be determined from advice from the SPoC that consequential data such as telephone subscriber information is likely to be required when applying for an itemized bill; this should be explained on the application form. The SPoC will provide advice regarding these issues and completion of the form.

Schedule

The purpose of this form is to obtain consequential data (additional data) from the data obtained in the initial application form. For example, an application form is submitted for itemised billing on a particular number with a view to analysing the data within it, and then apply for relevant subscriber checks from that itemised bill. The additional

subscriber checks will be regarded as consequential data. However, the fact that the applicant is likely to require the data needs to be explained within the initial application form and authorised by the DP.

The applicant would decide which subscriber checks were required and detail them within the schedule form, which will then be submitted to the SPoC. As the data is subscriber information, it would be possible for the SPoC to obtain this data in circumstances where the CSP will agree to provide the data by way of an authorisation, without the need for fresh applications and Judicial Approval. However, if the CSP requires a notice to be served on them prior to providing the data, there will be a requirement to complete an additional application form and seek approval from a JP, following the normal application process. The time limit of one month applies as mentioned earlier. The SPoC will advise the applicant regarding this process.

Within a schedule form, there is the requirement for the applicant to carry out open source enquiries prior to applying for the consequential data. Many telephone numbers and the businesses or persons connected to the numbers, are detailed on the internet. This information can subsequently eliminate the telephone number from the enquiry, or provide valuable intelligence material for the investigator. The test of necessity and proportionality are required when applying for consequential data. It is unlikely to be necessary to obtain a subscriber check on a telephone number, which if checked via the internet would have revealed that it was a bank or something similar. Applicants are required to sign the schedule form to say that they have carried out these types of enquiries. The inspectors, upon carrying out an inspection are likely to check whether the open source enquiries have been carried out. Under no circumstances should data be applied for using the schedule without the open source enquiries being completed. A record of the enquiries undertaken should be maintained. This is also a requirement under the Criminal Procedures Investigations Act (CPIA).

Renewal of Authorisations and Notices

Renewals would normally be used when obtaining future data such a cell site analysis which this Council is not allowed to obtain. However, in the rare event the SPoC believes it necessary and appropriate to renew an application for whatever reason, they will

advise the applicant on the appropriate process to be followed and Judicial Approval will be required.

The original application, Notice/ Authorisation (or copy if original has been served on CSP) will be retained by the SPoC within a central records held by the Fraud Team.

Cancellation of Notices and Withdrawal of Authorisations

A cancellation will be appropriate when an Authorisation or Notice has been authorised and prior to receiving or obtaining the Data from the C.S.P. it becomes apparent that the data requested is no longer required, or no longer proportionate to what was sought to be achieved.

In these situations it is the responsibility of the applicant or other officers conducting the investigation to ensure that they notify the SPoC as soon as it becomes apparent that the data is no longer required. The notification to the SPOC should be done in such a way as to produce a written record such as by email. An Application Cancellation form, which can be obtained from the Home Office Website or HDC intranet/SPOC, should be submitted by the applicant and a cancellation of the Authorisation or Notice form should be signed by the originating DP (or another DP in their absence) which will then be served on the CSP by the SPoC

It will be at the discretion of the SPoC to decide whether they feel it necessary to inform the CSP prior to serving a cancellation Notice.

Urgent Oral Authorisation

There is no provision within the legislation for the Council to orally provide authority to obtain Communications Data. All requests will be made in writing on the appropriate application forms.

Costs

There may be costs incurred when obtaining Communications Data from CSP's. It will be the responsibility of the SPoC to assess the costs involved and advise the DP prior to Authorisation. The SPoC will also provide advice to applicants to ensure that no unnecessary costs are incurred.

Records

Security of Records and Data

All the records and any data obtained as a result of the process under this legislation must be kept secure and confidential.

Applications, Authorisations, Judicial application/approval forms, copies of Notices, and records of the withdrawal of Authorisations and the cancellation of Notices, must be retained by the Council in written or electronic form, and physically attached or cross-referenced where they are associated with each other. The Council will also keep a record of the date and, when appropriate to do so, the time when each Notice or Authorisation is given or granted or cancelled. Errors should they occur (see below) will also be recorded by the SPoC and notified to the Senior Responsible Officer. These records will be held centrally by the SPoC.

These records must be available for inspection by the Commissioner and retained to allow the Investigatory Powers Tribunal to carry out its functions

Record of Activity

To meet its requirements the Council must also keep a record of the following items:

- number of applications submitted to a designated person for a decision to obtain communications data which were rejected after due consideration;

- number of Notices requiring disclosure of communications data within the meaning of each subsection of section 21(4) of the Act or any combinations of data;

- number of Authorisations for conduct to acquire communications data within the meaning of each subsection of section 21(4) of the Act or any combinations of data;

This record will be maintained by the SPoC and must be sent in written or electronic form to the Commissioner when requested by him.

Errors

The thorough checking of applications and this Council's operating procedures, including the careful preparation and checking of applications, Notices/Authorisations, should reduce the scope for making errors. Attention to detail will be required by all persons involved in the process.

Reporting and recording of errors will draw attention to those aspects of the process of acquisition and disclosure of communications data that require further improvement to eliminate errors and the risk of undue interference with any individual's rights. Therefore the SPoC will bring to the immediate attention of the SRO of either a recordable error or a reportable error and the necessary action can then be taken in line with the Codes of Practice.

Where material is disclosed by a CSP in error which has no connection or relevance to any investigation or operation undertaken by the public authority receiving it, that material and any copy of it should be destroyed as soon as the report to the Commissioner has been made.

An error can only occur after a designated person:

- has granted an Authorisation and the acquisition of data has been initiated, or
- has given Notice and the Notice has been served on a CSP in writing, electronically or orally.

It is important to apply the procedures correctly to reduce the risk of an error occurring.

Where any error occurs, a record should be kept.

There are two types of errors:

- Reportable

- Recordable

Reportable

Where communications data is acquired or disclosed wrongly a report must be made to the Commissioner **("reportable error")**. Such errors can have very significant consequences on an affected individual's rights with details of their private communications being disclosed to a public authority and, in extreme circumstances, being wrongly detained or wrongly accused of a crime as a result of that error. (see below for some examples of reportable errors).

Recordable

In cases where an error has occurred but is identified by the public authority or the CSP without data being acquired or disclosed wrongly, a record will be maintained by the public authority of such occurrences **("recordable error").** These records must be available for inspection by the Commissioner. (see below for some examples of recordable errors).

The staff involved in the process of acquiring Communications Data must adhere and report errors once they have been identified. It will not be acceptable for the error to be ignored. It will be the responsibility of SPoC's and the Senior Responsible Officer to be aware of the different ways in which errors can occur and the relevant procedure to be followed. Some examples are detailed below. They will also be responsible for informing applicants to report any errors that they are aware of to the SPoC.

Examples can include:

Reportable Errors

- an Authorisation or Notice made for a purpose, or for a type of data, which the relevant public authority cannot call upon, or seek, under the Act;

- human error, such as incorrect transposition of information from an application to an Authorisation or Notice

- disclosure of the wrong data by a CSP when complying with a Notice;

- acquisition of the wrong data by a public authority when engaging in conduct specified in an Authorisation;

Recordable errors

- a Notice given which is impossible for a CSP to comply with and an attempt to impose the requirement has been undertaken by the public authority;

- failure to review information already held, for example unnecessarily seeking the acquisition or disclosure of data already acquired or obtained for the same investigation or operation, or data for which the requirement to acquire or obtain it is known to be no longer valid;

Excess Data

Where an application by this Authority results in the acquisition of excess data, or its disclosure by a CSP in order to comply with the requirement of a Notice, all the data acquired or disclosed will be retained by the public authority.

As the material will have been obtained in connection with a criminal investigation it is bound by the Criminal Procedures Investigations Act (CPIA) and its code of practice and therefore there will be a requirement to record and retain data which is relevant to the criminal investigation, even if that data was disclosed or acquired beyond the scope of a valid Notice or Authorisation. If the criminal investigation results in proceedings being instituted all material that may be relevant must be retained at least until the accused is acquitted or convicted or the prosecutor decides not to proceed.

If having reviewed the excess data it is intended to make use of the excess data in the course of the investigation or operation, the applicant must set out the reason(s) for needing to use that material in a report which will be an addendum to the application upon which the Authorisation or Notice was originally granted or given. This will be submitted via the SPoC who will forward the relevant documentation to the Designated Person who will then consider the reason(s) and review all the data and consider

whether it is necessary and proportionate for the excess data to be used in the investigation or operation.

Criminal Procedures and Investigations Act (CPIA) and the Data Protection Act (DPA)

The codes do not affect any other statutory obligations placed the Council to keep records under any other enactment such as the Criminal Procedure and Investigations Act 1996 (CPIA) This requires that material which is obtained in the course of an investigation and which may be relevant to the investigation must be recorded, retained and revealed to the prosecutor.

Data Protection Safeguards

Communications data acquired or obtained under the provisions of the Act, and all copies, extracts and summaries of it, must be handled and stored securely. In addition, the requirements of the Data Protection Act 1998 and its data protection principles must be adhered to.

There is no provision in the Act preventing CSPs from informing individuals about whom they have been required by Notice to disclose communications data in response to a Subject Access Request made under section 7 of the DPA. However, a CSP may exercise certain exemptions to the right of subject access under Part IV of the DPA.

Section 29 provides that personal data processed for the purposes of the prevention and detection of crime; the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or other imposition of a similar nature are exempt from section 7 to the extent to which the application of the provisions for rights of data subjects would be likely to prejudice any of those matters. However this is not an automatic right. In the event that a CSP receives a subject access request where the fact of a disclosure under the Act might itself be disclosed the CSP concerned must carefully consider whether in the particular case disclosure of the fact of the Notice would be likely to prejudice the prevention or detection of crime.

Should a request for advice be made from a CSP regarding a disclosure the SPoC will consult with the Data Protection Officer of the Council and Head of Legal Services if necessary before a decision is made. Each case should be examined on its own merits.

Equally these rules will apply should a subject access request be made from an individual where material under this legislation is held by the Council.

A record will be made of the steps taken in determining whether disclosure of the material would prejudice the apprehension or detection of offenders. This might be useful in the event of the data controller having to respond to enquiries made

subsequently by the Information Commissioner, the courts and, in the event of prejudice, the police.

Should the Council have a request to obtain or disclose Communications Data to an overseas authority this request will be notified to the SPoC. All parties involved should refer to the section covering this area within the Codes of Practice and they should also take advice from the Council's Data Protection Officer.

It will be the responsibility of the SPoC to ensure that they are aware of how acquiring Communications Data impacts on the Data Protection Act.

Training

The Senior Responsible Officer will have responsibility for ensuring appropriate training for staff mentioned within this policy and for retaining a record of that training.

Reporting to Members

Annual returns of all activity undertaken by Council staff will be compiled by the Senior Responsible Officer and provided to the Corporate Governance Panel annually in line with the current advice in the Codes of Practice. Members will review on a yearly basis the policy to assess whether the activity undertaken is in line with this policy.

Oversight

The Act provides for an Interception of Communications Commissioner ('the Commissioner') whose remit is to provide independent oversight.

It is important to note that should the Commissioner establish that an individual has been adversely affected by any willful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under the Act in relation to the acquisition or disclosure of communications data, he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable him or her to effectively engage the Tribunal.

Complaints

The Act established an independent Tribunal

Details of the relevant complaints procedure can be obtained from the following address:

The Investigatory Powers Tribunal
PO Box 33220
London
SW 1H 9ZQ
020 7035 3711

ADVICE

If you require further advice about covert surveillance, please contact the Fraud Team (SPoC Officers) based at Pathfinder House.

POLICY UPDATING PROCEDURE

Proposed amendments to this Policy must be forwarded to the Senior Responsible Officer where they will be considered in consultation with Fraud Team (SPoC Officers) before submission to Chief Officers Management Team and Cabinet.

The Policy shall be reviewed as required by legislation, upon advice from the Home Office or following an inspection by the IOCCO.

FURTHER INFORMATION ENQUIRIES AND COMPLAINTS

The Senior Responsible Officer is the first point of contact on any of the matters raised in this policy statement. Enquiries should be addressed to :

The Head of Legal & Democratic Services
Pathfinder House
Huntingdonshire District Council
Pathfinder House
St Mary's Street
Huntingdon
Cambridgeshire
PE29 3TN
Tel : (01480) 388388

Nick Jennings
Fraud Manager

1.5.2013

ANNEX A

LIST OF OFFICERS ROLES

ROLE	SERVICE	POST	POST HOLDER
Senior Responsible Officer	Council-Wide	Head of Legal and Democratic Services	Colin Meadowcroft
(Senior) Designated Person	Council-Wide	Head of Paid Service	Malcolm Sharp
Designated Person	Customer Services	Head of Customer Service	Julia Barber
Designated Person	Environmental Health and Community Services	Head of Environmental Health Services	Sue Lammin
Designated Person	Planning Services	Head of Planning Services	Steve Ingram
Designated Person	Head of Operations Division	Head of Service-Operations Division	Eric Kendall
SPoC Officers	Fraud Team		Nick Jennings Loraine Southworth Cindy Dickson

CORPORATE GOVERNANCE PANEL **24 JULY 2013**

INTERNAL AUDIT SERVICE ANNUAL REPORT (Report by the Internal Audit Manager)

1. INTRODUCTION

1.1 This is the annual report of the Internal Audit Manager as required by the Public Sector Internal Audit Standards (PSIAS). It covers the period 1 August 2012 to 30 June 2013.

1.2 The report includes the Internal Audit Manager's annual opinion on the overall adequacy and effectiveness of the Council's internal control and governance processes.

The opinion is based upon

- the work carried out by Internal Audit during the year; and
- the assurances made available by external assessors and similar providers.

1.3 The report also provides information on:

- the delivery of the annual audit plan;
- audit reports issued and issues of concern;
- implementation of agreed actions; and
- Internal Audit's performance.

2. OVERALL OPINION

Audit Opinion
Based upon work undertaken and statements from external assurance providers, it is my opinion that the Council's internal control environment and systems of internal control as at 30 June 2013 provide limited assurance over key business processes and financial systems.

David Harwood
Internal Audit Manager July 2013

Definition of Limited *: There are weaknesses in the level of internal control for managing the material inherent risks within the internal control environment. The control failings identified from the evaluation and testing of individual systems show that the internal control environment is clearly at risk of not being able to meet its objectives and significant improvements are required to improve the adequacy and effectiveness of control.*

2.1 The audit opinion has been given as at 30 June 2013 to reflect the current state of the internal control environment and systems of internal control (definition in Annex C) across the Council and provide the Panel with a timely opinion for inclusion in the draft annual governance statement. If significant changes occur to the internal control

environment prior to the Panel approving the annual governance statement in September, the Panel will be informed.

2.2 During the reporting period it should be noted that:

- One 'no' assurance and seven 'limited' assurance opinions were issued.
- Significant failings in procurement practices have been identified.
- Key financial systems have 'adequate' assurance.
- The overall number of internal audit actions suggested and accepted by Managers for the period ending 30 June 2013 has reduced from 75 in 2012 to 58 in 2013.
- The implementation rate of agreed actions has increased.

2.3 The report also provides information on:

- the delivery of the annual audit plan;
- audit reports issued and issues of concern;
- implementation of agreed actions; and
- Internal Audit's performance.

2.4 Assurance from external sources that impacts upon the internal control environment and systems of internal control is detailed at Annex A. No serious control weaknesses have been identified in those reports.

2.5 The Internal Audit Manager reports functionally to the Corporate Governance Panel and maintains organisational independence. He has had no constraints placed upon him in respect of determining overall audit coverage, audit methodology, the delivery of the audit plan or proposing actions for improvement or forming opinions on individual audit reports issued.

3. DELIVERY OF AUDIT PLAN

3.1 The Internal Audit Plan was approved by Management Team and the Corporate Governance Panel in June 2012 in respect of the year ending July 2013.

Due to the introduction of the Public Sector Internal Audit Standards and Panel's wish to consider a draft annual governance statement at their July meeting, the decision was taken to revert the internal audit plan back to the financial year. Consequently the audit plan agreed in June 2012 has not been delivered in full but has been reviewed and recast. This approach was agreed by the Corporate Governance Panel in March 2013 when they also approved the internal audit plan and quarterly planning process for 2013/14.

Internal Audit Reports issued

3.2 The audit reports issued (draft/final or closed) during the period 1 August 2012 to 30 June 2013, the assurance opinion and number of agreed (or proposed) actions are listed in the table below. All the reports can be accessed via the Internal Audit intranet pages.

Audit area	Level of assurance				Agreed action status		
	Substantial	Adequate	Limited	Little	Red	Amber	The risk identified has been accepted by the Manager[1]
Housing benefits: Verifying information	✓✓				0	0	
Major incident planning	✓✓				0	0	
Legal debt collection & recovery	✓✓				0	0	
Provision of legal advice	✓✓				0	0	
Housing: Choice-based lettings	✓✓				0	3	
Payroll: Payments & reconciliations	✓✓				0	3	
Facilities management		✓			1	3	
New homes bonus grant		✓			0	3	
Payroll: Variations to Pay		✓			0	3	
Housing benefits: e-forms		✓			0	3	
Payroll: Variations to pay		✓			0	1	
Voluntary redundancy		✓			0	0	
Registration of interests		✓			0	0	
Call Centre (draft)		✓			0	0	
One Leisure: Café Zest (draft)			✗		3	5	
Robustness of budget savings			✗		2	3	
Post-implementation reviews			✗		2	0	
Contract management			✗		1	4	
E-marketplace			✗		0	4	
External funding/grants (draft)			✗		0	4	
Mobile & office telephone use			✗		0	3	
One Leisure: Pure spa				✗✗	7	6	

[1] There are occasions when a risk identified during an audit is acknowledged and accepted by a Manager and they decide that no further action is required. The right hand column of this table records any such instances.

3.3 In addition to the reports listed above, a substantial amount of work has been undertaken in the following areas:

- 2011/12 final accounts process
- Re-development of One Leisure St. Ives
- Licensing & Community Safety
- Penetration Testing

No assurance opinions were given on these pieces of work as they were either reported to Panel separately, subsumed into other work areas or developed into consultancy type reviews.

3.4 The Licensing and Community Safety review examined the arrangements operating between Licensing, Community Safety and the Police that allowed for anti-social behaviour and crime and disorder to be addressed. Two actions were agreed that have resulted in the greater sharing of information/intelligence and an inspection programme being introduced.

3.5 Penetration testing of internet facing systems was undertaken to provide an assessment of the logical security controls supporting the network infrastructure. Whilst a number of weaknesses were identified, these are not considered business critical.

3.6 A review of the software developed by the Information Management Division to manage the community infrastructure levy was also undertaken and a draft report issued. Subsequently, a decision was taken to purchase commercial software. The audit was closed as it was no longer appropriate.

3.7 The continuous auditing of key controls within main financial systems has been introduced. Summary details are shown in the table below.

Audit area	Level of assurance				Agreed action status		
	Substantial	Adequate	Limited	Little	Red	Amber	The risk identified has been accepted by the Manager[1]
Council Tax		✓			0	0	
Main Accounting System		✓			0	2	
Accounts Payable (Creditors)		✓			0	0	
Accounts Receivable (Debtors)		✓			0	4	

[1] There are occasions when a risk identified during an audit is acknowledged and accepted by a Manager and they decide that no further action is required. The right hand column of this table records any such instances.

3.8 Internal audit have also undertaken work in a number of other areas. These include:

- Review of the Council Tax support scheme
- Management of the commercial estate
- Contract review of the Planning Services Framework
- Two employee investigations
- Responding to whistleblowing allegations
- Consideration of the national fraud initiative data received in February 2013
- Payment procedure for the 2nd green bin initiative
- Payments hub system replacement

3.9 Guidance has also been provided on an ad-hoc basis on a wide variety of control issues.

4. ISSUES OF CONCERN CONTRIBUTING TO THE LIMITED ASSURANCE OPINION

One Leisure – Pure and Café Zest

4.1 The reviews of the management of the Pure spa and therapy facilities and Café Zest identified similar types of control failings. These included inconsistent operations across the Centres, the lack of formal business plans, strategies and targets. Little management review or monitoring is performed. Stock controls are weak and inconsistent. Pricing and discount arrangements are not sufficiently controlled.

Post Implementation Reviews

4.2 There is infrequent, formal challenge or consideration of the value for money aspects of completed projects. The prime emphasis has tended to be on project budget approval with less concern on demonstrating improved service outcomes.

Code of Procurement

4.3 Compliance with the Code of Procurement remains an issue. Failings have been identified in contract management procedures, the lack of expertise available within the Council in certain areas and the need to use contractors to provide guidance which has resulted in close professional relationships developing, over familiarity and conflicts of interest.

Limited amount of IT audit coverage

4.4 Computer audit coverage for the period ending March 2014 was considered by the Panel in December 2012.

4.5 The number of computer audit reviews completed during the period is of concern. My annual report for 2012 only listed two reviews, this year only one audit (penetration testing) has been completed. Staff within the Information Management Division are managing a large number of projects and have been unable to meet with the auditors to allow the reviews to commence. Whilst this has been accepted, it has meant that no assurance can be given on the application of controls within this key area.

5. ISSUES OF CONCERN FROM PREVIOUS REPORTS

Data Protection

5.1 Reference was made in the 2012 report to County Council employees (LGSS) transferring via email, confidential information to the County Council computer system in order to improve their workflow/efficiency. The risks associated with this were accepted by the former Managing Director (Resources). Changes have recently been made to workflow arrangements with the result that LGSS staff now access data securely.

Establishment Control

5.2 Ensuring the accuracy of the payroll to reduce the opportunity for fraud is a key control. Reports have not been sent every six months to Heads of Service listing employees within their services and requesting positive confirmation that the reports were correct. At the time of writing this report, the information is respect of the period ending June 2013 was due to be issued.

Issues outstanding from previous years

5.3 Audit reviews that have had either an assurance opinion of 'limited' or 'little' in previous years are listed in the table below together with a summary of the progress made towards implementing the agreed actions.

The right hand column of the table shows a revised assurance opinion, based upon the action that has been taken by the manager and evidence from the follow-up work that has been completed. The revised opinion is only a guide to the potential improvement that would be expected, if the audit was repeated and all other system controls remained effective.

Original level assurance	Agreed Action Status		Audit area and follow-up findings	'Potential' level of assurance
	Red	Amber		
2011-12				
Limited	2	0	**Business Continuity Planning** Both actions have been introduced.	Adequate
2010-11				
Little	4	4	**Supermarket car park income agreements** 3 of the 4 actions have been introduced. It has been agreed that the action relating to contractual agreements will not be pursed.	Adequate

Assurance definitions are included in Annex C.

6. IMPLEMENTATION OF AGREED ACTIONS

6.1 Management Team have set a target of 60% of agreed actions being implemented on time, based on a rolling 12 month timeframe. The figures for the year ending 30 June 2013 are shown below. The 60% target has been exceed since January 2013.

Status of Action							
	Introduced on time		Introduced Late		Not introduced		**TOTAL**
Red Action	10		0		0		10
Amber Action	27		2		7		36
Total	**37**		**2**		**7**		**46**
% age	**80%**		**5%**		**15%**		
Head of Service	*Red*	*Amber*	*Red*	*Amber*	*Red*	*Amber*	
Financial Services		2		0		0	**2**
Law & Democratic Services		3		0		0	**3**
Operations		3		0		0	**3**
Corporate Team		0		0		5	**5**
Information Management	2	5		0		0	**7**
General Mgr, One Leisure	7	8		2		0	**17**
Environmental Management	1	3		0		2	**6**
Environmental Health		0		0		0	**0**
Customer Services		3		0		0	**3**
Total	10	27	0	2	0	7	**46**

6.2 A sample of actions that Managers report as being completed have been checked throughout the year to see that the action introduced sufficiently deals with the risk that has been identified. The table below summarises the work done during the year ending 31 March 2013.

		Red	Amber	Total
Follow up status	Accepted and closed	3	19	22
	Disputed, partially met	3	2	5

6.3 If during the review of actions introduced it is found that the action taken by a manager does not fully deliver against the agreed action, the matter

is discussed with the manager and if necessary, changes to the database are made to reflect the actual position. There are five disputed actions that fall into this category.

7. INTERNAL AUDIT PERFORMANCE

7.1 Internal Audit have undertaken a self-assessment review against the Public Sector Internal Audit Standards. The outcomes of the review were reported to the Corporate Governance Panel in May 2013. The internal audit service does not fully conform to the Standards and the Panel considered that the areas of non-conformance were not significant enough to be included in the annual governance statement.

7.2 A quality assurance and improvement programme has not yet been formally developed as required by the Standards. Details of this and other developments planned during 2013/14 are listed in Annex B together with information regarding the performance of internal audit during 2012/13 and service developments that have taken place.

8. RECOMMENDATION

It is recommended that the Panel note the report and take into account the Internal Audit Manager's opinion when considering the Corporate Governance statement.

ACCESS TO INFORMATION ACT 1985
Internal Audit Reports
Internal Audit Performance Management Information

Contact Officer: David Harwood, Internal Audit Manager
☎ **01480 388115**

ANNEX A

EXTERNAL ASSURANCE RECEIVED

Date	Report from	Area covered	Assessment
March 2012	Interception of Communications Commissioner's Office	Compliance with the requirements of the Regulation of Investigatory Powers Act 2000.	The Council has a satisfactory level of compliance with the Act and Code of Practice.
June 2012	Local Government Ombudsman	Complaints made to the Ombudsman for 2011/12.	"I am pleased to say that I have no concerns about your authority's response times and there are no issues arising from the complaints that I want to bring to your attention".
December 2012	External Auditor (PricewaterhouseCoopers)	Final Accounts 2011/12	Unqualified accounts.
March 2013		Grant Certification Report	2 grants certified: Housing and Council Tax benefits subsidy grant qualified. National Non Domestic Rates return not qualified.
March 2013	EMQC (on behalf of the Dept for Business Innovation & Skills)	Customer Service Excellence – (previously Charter Marks) Customer Service and Call Centre.	Fully meets the requirements to allow maintenance of the Customer Service Excellence Standard Certification.
March 2013	Electoral Commission	Review of performance standards for Electoral registration Officers	The standards have been met.

ANNEX B

INTERNAL AUDIT PERFORMANCE

Customer Satisfaction

Target: 85% or more of customers rating service quality as good or better.
Achieved: 12 months to June 2013 – 100% (from 12 responses)

At the conclusion of all audits, managers are requested to complete an end of audit survey form and give an opinion on the value of the audit. The options available are – very good, good, acceptable, requires improvements or unacceptable. Target information is calculated on a rolling twelve month basis rather than by financial year.

The Head of Financial Services has also undertaken his annual customer satisfaction survey with senior managers. The April 2013 figure showed 85% (78% previous year) of managers felt audit provided a good or very good service. No respondent considered the service required improvement or was unacceptable.

Service delivery targets

Target: The service delivery targets are achieved.

There are four elements to this target which all relate to the progress of individual audits and the reporting process.

Since all three auditors have become part-time it has become clear that they do not have the same degree of flexibility to manage meeting dates as they did when working full-time. It is the intention to keep the same targets. They are challenging but should be seen as aspirational. Keeping them does provide a target and benchmark of trends.

		Achieved	
	Target	@ August 2012	@ June 2013
a) Complete audit fieldwork by the date stated on the audit brief	75%	75%	71%
b) Issue draft audit reports within 15 working days of completing fieldwork	90%	45%	75%
c) Meet with customer and receive response allowing draft report to progress to final within 15 working days of issuing draft report	75%	75%	64%
d) Issue final audit report within 5 working days of receiving full response	90%	92%	92%

INTERNAL AUDIT PERFORMANCE

Target (c) shows the lowest level of achievement. Non-achievement is due to the time taken to obtain a formal response to the draft report from a manager. A separate target, for internal use only, records the length of time an auditor takes to meet with the manager to discuss the draft report. This shows that 89% of meetings were held in 15 days. It is the expectation that managers will respond formally to the draft report during the meeting, but they are now wanting to reply more formally, which means the 15 day target is not met.

Service Developments

The following service developments have taken place:

- The continuous audit process has been successfully introduced.
- A self-assessment review of the Internal Audit Service against "proper practice" provisions of the Public Sector Internal Audit Standards showed that the service generally conforms with those Standards and an action plan has been prepared to address the non-compliance (confirmed as only minor in nature).
- The internal audit strategy and terms of reference (audit charter) has been revised to take account of the Public Sector Internal Audit Standards.

A number of developments are expected during the next year. These include:

- Formally introducing a quality assurance and improvement programme.
- Introducing business rates into the continuous audit process and examining the opportunities from the use of automated software.
- Reviewing the wider role of the Internal Audit Manager across the Council against the Cipfa publication "The role of the head of internal audit in public sector service organisations".
- The Head of Welland Internal Audit Consortium undertaking a peer review of the service, the results of which will be reported to the Panel.

ANNEX C

DEFINITIONS USED IN THE REPORT

Assurance definitions: for information

Substantial Assurance	✓✓	*There are no weaknesses in the level of internal control for managing the material inherent risks within the system. Testing shows that controls are being applied consistently and system objectives are being achieved efficiently, effectively and economically apart from any excessive controls which are identified in the report.*
Adequate Assurance	✓	*There are minor weaknesses in the level of control for managing the material inherent risks within the system. Some control failings have been identified from the systems evaluation and testing which need to be corrected. The control failings do not put at risk achievement of the system's objectives.*
Limited Assurance	✗	*There are weaknesses in the level of internal control for managing the material inherent risks within the system. Too many control failings have been identified from the systems evaluation and testing. These failings show that the system is clearly at risk of not being able to meet its objectives and significant improvements are required to improve the adequacy and effectiveness of control.*
Little Assurance	✗✗	*There are major, fundamental weaknesses in the level of control for managing the material inherent risks within the system. The weaknesses identified from the systems evaluation and testing are such that the system is open to substantial and significant error or abuse and is not capable of meetings its objectives.*

Internal control environment:
The control environment comprises the systems of governance, risk management and internal control. The key elements of the control environment include:

- establishing and monitoring the achievement of the organisation's objectives
- the facilitation of policy and decision-making ensuring compliance with established policies, procedures, laws and regulations – including how risk management is embedded in the activity of the organisation, how leadership is given to the risk management process, and how staff are trained or equipped to manage risk in a way appropriate to their authority and duties
- ensuring the economical, effective and efficient use of resources and for securing continuous improvement in the way in which its

DEFINITIONS USED IN THE REPORT

functions are exercised, having regard to a combination of economy, efficiency and effectiveness

- the financial management of the organisation and the reporting of financial management
- the performance management of the organisation and the reporting of performance management

System of internal control
A term to describe the totality of the way an organisation designs, implements, tests and modifies controls in specific systems, to provide assurance at the corporate level that the organisation is operating efficiently and effectively.

This page is intentionally left blank

CORPORATE GOVERNANCE PANEL **24 JULY 2013**

WORK PROGRAMME & TRAINING
(Report by the Assistant Director Finance & Resources)

1. WORK PROGRAMME

1.1 The anticipated work programme for the Panel for the next year is shown at Annex A

1.2 Panel are asked to consider the work programme and decide what training they would like in preparation for the next or future agendas. Normally this training would be for 30-45 minutes immediately prior to the formal meeting but there may be occasions when a separate longer session would be more appropriate.

1.3 Training can be provided by appropriate officers, external audit or external trainers (subject to budgetary constraints).

1.4 An informal meeting of the Panel will be held in August to discuss the annual governance statement before it is finalised and presented to the September meeting.

2. RECOMMENDATION

2.1 It is recommended that Panel consider what training is to be provided prior to the September meeting.

BACKGROUND INFORMATION
None

Contact Officer: David Harwood, Internal Audit Manager ☎ **01480 388115**

Annex A

Anticipated Work Programme

26 September 2013

- Approval of the statement of accounts
- Approval of the Annual Governance Statement
- External audit – ISA 260 report
- Effectiveness of the Panel
- Assurance mapping

27 November 2013

- Internal Audit interim progress report
- Housing Benefit fraud investigation activity
- Whistleblowing : policy review & investigations
- National Fraud Initiative
- Assurance mapping

29 January 2014

- Progress on issues raised in the Annual Governance Statement
- Review of the risk management strategy
- Review of the anti-fraud & corruption strategy
- Assurance mapping

26 March 2014

- Review of Council constitution
  - Code of financial management
  - Code of procurement
- Internal Audit Plan
- External Audit
  - Audit plan
  - Grant claims
- Assurance mapping

May 2014

- Review of the internal audit service
- Internal audit annual report & opinion
- Assurance mapping

July 2014

- Feedback – annual report
- Draft Annual Governance Statement
- Assurance mapping

In addition to the items listed above, reports may be submitted on an ad-hoc basis on

- Awards of compensation
- Employee's code of conduct
- Ombudsman reviews
- Money laundering and bribery
- Accounting policies

By virtue of paragraph(s) 3 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank