Public Document Pack

Ethics Committee Agenda

To: Councillor Oliver Lewis (Chair)
Councillor Joy Prince (Vice-Chair)
Councillors Pat Clouder, Mario Creatura, Maggie Mansell, Donald Speakman and Wayne Trakas-Lawlor
Anne Smith and Ashok Kumar (Independent Co-opted Members)

Reserve Members: Patricia Hay-Justice, Steve Hollands, Karen Jewitt, Dudley Mead and Andrew Rendle

A meeting of the **Ethics Committee** which you are hereby summoned to attend, will be held on **Wednesday, 28 February 2018** at **6.30 pm** in **F10, Town Hall, Katharine Street, Croydon CR0 1NX**

JACQUELINE HARRIS-BAKER
Director of Law and Monitoring Officer
London Borough of Croydon
Bernard Weatherill House
8 Mint Walk, Croydon CR0 1EA

Stephen Rowan
020 8726 6000 x62529
stephen.rowan@croydon.gov.uk
www.croydon.gov.uk/meetings
Tuesday, 20 February 2018

Members of the public are welcome to attend this meeting.
If you require any assistance, please contact the person detailed above, on the righthand side.

N.B This meeting will be paperless. The agenda can be accessed online at www.croydon.gov.uk/meetings

AGENDA – PART A

1. Apologies for Absence

To receive any apologies for absence from any members of the Committee.

2. Minutes of the Previous Meeting (Pages 5 - 8)

To approve the minutes of the meeting held on 6 September 2017 as an accurate record.

3. Disclosure of Interests

In accordance with the Council's Code of Conduct and the statutory provisions of the Localism Act, Members and co-opted Members of the Council are reminded that it is a requirement to register disclosable pecuniary interests (DPIs) and gifts and hospitality to the value of which exceeds £50 or multiple gifts and/or instances of hospitality with a cumulative value of £50 or more when received from a single donor within a rolling twelve month period. In addition, Members and co-opted Members are reminded that unless their disclosable pecuniary interest is registered on the register of interests or is the subject of a pending notification to the Monitoring Officer, they are required to disclose those disclosable pecuniary interests at the meeting. This should be done by completing the Disclosure of Interest form and handing it to the Democratic Services representative at the start of the meeting. The Chair will then invite Members to make their disclosure orally at the commencement of Agenda item 3. Completed disclosure forms will be provided to the Monitoring Officer for inclusion on the Register of Members' Interests.

4. Urgent Business (if any)

To receive notice of any business not on the agenda which in the opinion of the Chair, by reason of special circumstances, be considered as a matter of urgency.

5. Corporate RIPA (Regulation of Investigatory Powers Act 2000) Policy Revisions (Pages 9 - 38)

The Committee is asked to note the findings and recommendations made by the Office of the Surveillance Commissioner's inspection and the subsequent revisions to the corporate policy and procedures.

6. Use of the Powers Available Under the Regulation of Investigatory Powers Act 2000 Year Ending 31 December 2017 (Pages 39 - 42)

The Committee is asked to note how the powers available to the Council under RIPA have been used over the last calendar year.

7. Recent Development on the Regulation of Councillor Conduct (Pages 43 - 50)

The Committee is asked to note the recent Government consultation on disqualification criteria for Councillors and Mayors; to consider the current consultation on local government ethical standards; and to note the outcome of a recent case in relation to the regulation of Councillor conduct.

8. Annual Update on Ethics Complaints Received Year Ending 31 December 2017 (Pages 51 - 52)

The Committee is asked to note the content of this update report.

9. Annual Whistleblowing Report for Year Ending 31 December 2017 (Pages 53 - 54)

The Committee is asked to note the use of the Council's whistleblowing procedure during the past calendar year.

10. Member Learning and Development 2017-18 (Pages 55 - 58)

The Committee is asked to note Member Learning and Development activity in the 2017-18 Municipal Year.

11. Dispensation Applications for Members (Pages 59 - 64)

To receive the report of the Director of Law on Members' dispensations for consideration, if any are received.

12. Exclusion of the Press and Public

The following motion is to be moved and seconded where it is proposed to exclude the press and public from the remainder of a meeting:

"That, under Section 100A(4) of the Local Government Act, 1972, the press and public be excluded from the meeting for the following items of business on the grounds that it involves the likely disclosure of exempt information falling within those paragraphs indicated in Part 1 of Schedule 12A of the Local Government Act 1972, as amended."

PART B AGENDA

13. Dispensation Applications for Members

To receive the report of the Director of Law on Members' dispensations for consideration, if any are received.

This page is intentionally left blank

Ethics Committee

Meeting held on Wednesday 6 September 2017 at 6:30pm in Room F5, the Town Hall, Katharine Street, Croydon CR0 1NX

DRAFT
MINUTES - PART A

Present: Councillor Oliver Lewis (Chair)
Councillors Steve Hollands, Karen Jewitt, Andrew Rendle and Donald Speakman

Mr Ashok Kumar, Independent Person (non-voting) and Mrs Anne Smith, Independent Person (non-voting)

Apologies: Councillors Pat Clouder, Mario Creatura, Maggie Mansell and Joy Prince

MINUTES - PART A

A1 Minutes

The minutes of the meeting held on 1 February 2017 were agreed as an accurate record.

A2 Disclosure of Interest

There were none.

A3 Urgent Business (if any)

There were no items of urgent business.

A4 Exempt Items

The allocation of business between Part A and Part B was agreed.

A5 Regulation of Investigatory Powers Act 2000 – April 2017 Inspection of the Council by the Office of Surveillance Commissioners

The Information Management Co-ordinator informed the Committee that the Office of the Surveillance Commissioner (OSC) undertook inspections of authorities on a two and a half year to year cycle, and that the last inspection of Croydon Council took place in April 2017.

During the inspection representatives of the OSC met with officers who undertook RIPA activities; including those who worked Council's CCTV room with whom they discussed the general use of CCTV and the processes followed when outside bodies, such as the Police and Department for Work and Pensions, requested the use of the Council's CCTV for surveillance.

It was noted by the Information Management Co-ordinator that the findings of the OSC were fairly limited in regards to actions the Council was required to undertake. The need for all staff to be appropriately trained when undertaking investigations was identified, and whilst it was noted that training had been undertaken changes in personnel meant that a review was required. Furthermore, training around the use of social media had been identified and Members were informed that the RIPA policy was to be redrafted to include a section on the effective use of social media and would be brought to a future meeting of the Committee for consideration. The OSC finally reviewed the authorisation documentation and recommended that a standard electronic record was used which had been actioned by the Council.

In response to Member questions the Information Management Co-ordinator informed the Committee that as part of the RIPA policy review there would be a review of those who had the power to authorise the use of investigations. Furthermore, a review of training would be undertaken to ensure the right people were trained especially in light of staff turnover.

The Information Management Co-ordinator informed the Committee that social media was used occasionally by officers to aid investigations but those being investigated were not being actively engaged via social media; it was being used as an investigative tool rather than surveillance.

RESOLVED: To note the findings of the recent Office of the Surveillance Commissioner (OSC) Inspection, which documents the Council's use of the powers available under Regulation of Investigatory Powers Act 2000 (RIPA) since the last inspection.

A6 **Recent Case Law Update**

The Director of Law stated that having updates on recent case law was a useful way to learn from other authorities on how to deal with possible future cases which involved ethics. The case outlined within the report had been reported on earlier in the year and was in relation to an allegation of Member bullying and wrongdoing. Due to the Member being unhappy with how the investigation was undertaken and that the details had been released into the public domain it was heard at the High Court.

The Director of Law stated that the case had provided clarification around the powers within the Localism Act to undertake investigations and also that the wider powers of an authority could be used, such as the general powers to ensure the financial affairs of the local authority were in order. The ruling of the High Court had endorsed the process taken and the publication of the investigation material due to the high public interest of the case. Furthermore, the case clarified that the actions taken before the Localism Act came into power could be taken into consideration.

In response to Member questions the Director of Law informed the Committee that there was not one area where all reports on recent case law had been saved, however this could be reviewed and the reports could be stored on the Members' Portal for reference. The Director of Law informed the Committee that a quarterly update on recent case law was circulated to departments to ensure officers were kept informed.

The Committee noted that paragraph 3.3 of the report should read; "Documents also refer to members bullying employed officials and officers who were *not* compliant in carrying out the members wishes."

RESOLVED: To note the outcome of recent case law.

A7 Members' Dispensations

The Committee received the report of Director of Law and noted that no applications for dispensation had been received from Members of the Council.

RESOLVED: To note the report.

A8 Draft Work Programme for 2017/18

The Committee considered the draft work programme for the 2017/18 municipal year and made no amendments.

RESOLVED: To note the draft work programme for the 2017/18 municipal year.

A9 Exclusion of the Press & Public

The following motion was moved by Councillor Lewis and seconded by Councillor Jewitt to exclude the press and public:

“That, under Section 100A(4) of the Local Government Act, 1972, the press and public be excluded from the meeting for the following

items of business on the grounds that it involves the likely disclosure of exempt information falling within those paragraphs indicated in Part 1 of Schedule 12A of the Local Government Act 1972, as amended."

The motion was put and it was agreed by the Committee to exclude the press and public for the remainder of the meeting.

MINUTES - PART B

B10 Minutes

The minutes of the meeting held on 1 February 2017 were agreed as an accurate record.

B11 Members' Dispensations

There were no applications for Members' dispensations to conisder.

The meeting ended at 6.52pm

REPORT TO:	**ETHICS COMMITTEE** **28 February 2018**
SUBJECT:	**CORPORATE RIPA (REGULATION OF INVESTIGATORY POWERS ACT 2000) POLICY REVISIONS**
LEAD OFFICER:	**DIRECTOR OF LAW AND MONITORING OFFICER**
WARDS:	**ALL**
CABINET MEMBER:	**Councillor Hamida Ali - Communities, Safety and Justice**
CORPORATE PRIORITY/POLICY CONTEXT: Monitoring compliance with the Regulation of Investigatory Powers Act supports the Council's approach to corporate governance.	
FINANCIAL IMPACT The recommendation contained in this report has no financial implications.	
KEY DECISION REFERENCE NO: This is not a key decision.	

1. RECOMMENDATION

The Committee is asked to:

1.1 Note the revisions to the corporate policy and procedures managing the use of Covert Surveillance authorised under the Regulation of Investigatory Powers Act (RIPA) 2000 by the Council arising from the Office of Surveillance Commissioner's recommendations following a Council inspection in 2017.

2. EXECUTIVE SUMMARY

2.1 The Committee were informed of the results of an Office of the Surveillance Commissioner's inspection of the Council's use of RIPA at their meeting held on 6 September 2017. This report provided details of the inspectors finding and recommendations made.

2.2 The inspection report concluded that there was a clear commitment on the part of those officers involved in both operational and supervisory roles, to maintain proper standards.

3.0 KEY FINDINGS

3.1 As part of the inspection, the Inspector considered and commented on the Council's Policy document. The Inspector commented that the Council's current Policy document did not include the use of social media. Therefore, a recommendation was made that this should be included. This can now be found at Section 17 of the attached policy. The opportunity has also been taken to revise other parts of the Policy, to include guidance on particular issues that had been previously provided to investigators in Sections 15, 16 and 18.

3.2 The Inspector further commented that Policy and Procedure was of high quality and was balanced and easy to follow. Members may wish to note that in addition to the Council's RIPA Policy document, an Aide-memoir had been issued to the Council officers who undertake RIPA activities, which included the use of Social Media in investigations in addition to specific pieces of advice provided separately in respect of individual investigations. This now forms part of the of the revised policy document.

3.3 The Committee may also wish to note that during the coming year training events will take place for officers whose role requires the potential use of surveillance. It is hoped to host a training event facilitated by the National Anti-Fraud Network in April, with a further training event later in the year.

4.0 FINANCIAL AND RISK ASSESSMENT CONSIDERATIONS

4.1 There are no direct financial implications arising from this report.

5.0 LEGAL IMPLICATIONS

5.1 There are no direct legal consequences arising from the contents of this report beyond those set out in the body of the report.

CONTACT OFFICER: Jacqueline Harris-Baker, Director of Law and Monitoring Officer (ext 62328)

BACKGROUND PAPERS: None

Appendices: Appendix 1 – Corporate Policy & Procedures

London Borough of Croydon

Corporate Policy & Procedures managing the use of Covert Surveillance Authorised under the Regulation of Investigatory Powers Act & Unregulated Activities

Index

22.0 Security of Documentation & Communications

23.0 Consequential Amendments

Annex A

1.0 Introduction

1.2 RIPA and the Human Rights Act

The Regulation of Investigatory Powers Act (RIPA) legislates for the use by local authorities of covert methods of surveillance and information gathering to assist the detection and prevention of crime in relation to an authorities core functions. **Evidence obtained by any covert surveillance or use covert human intelligence sources could be subject to challenges under Articles 6 (right to a fair trail) and 8 (right to a private and family life) of the European Convention on Human Rights (ECHR) - the right to respect for private and family life. However, properly authorised covert surveillance under RIPA makes lawful what might otherwise be a breach of Articles 6 and 8 of the ECHR and protects the Council from any civil liability.**

1.3 Using these powers, the Council is able to:

- Acquire data relating to communications (subscriber information);
- Carry out surveillance;
- Use covert human intelligence sources (CHIS).

1.4 While some members of the community may consider RIPA to be intrusive, it is a vital tool for this Council's work to undertake a number of its core functions for example (and not exclusively) counter fraud, trading standards investigations and managing environmental issues (i.e. fly tipping). The 'core functions' were referred to by the Investigatory Powers Tribunal (*C v The Police and the Secretary of State for the Home Office - IPT/03/32/H dated 14 November 2006*) as the 'specific public functions', undertaken by a particular authority, in contrast to the 'ordinary functions' which are those undertaken by all authorities (e.g. employment issues, contractual arrangements etc.). A public authority may only engage RIPA when in performance of its 'core functions'. For example, the disciplining of an employee is not a 'core function'.

1.5 Some of the Council's enforcement functions will require the use of covert surveillance or CHIS but the community must be confident that this is undertaken in accordance with the law is necessary, proportionate, and undertaken with the minimum of intrusion into an individual's private life.

1.6 The Council is fully committed to complying with the Human Rights Act 1998 (HRA) and the Regulation of Investigatory Powers Act 2000 (as amended by the Protection of Freedoms Act 2012) (RIPA). To ensure compliance all covert directed surveillance, and use of covert human intelligence source (CHIS), falling within the scope of the Act, carried out by officers of the

Council or contractors acting on the Council's behalf, must be properly authorised by a Designated Authorising Officer.

2.0 Purpose of the Policy & Procedures

2.1 To comply with RIPA, it is vital that officers carrying out activities under its powers must have full regard to the codes of practice and guidance issued by the Home Office, Office of the Surveillance Commissioner and the Interception of Communications Commissioner.

2.2 Investigations which fall within the scope of the RIPA, but which are not correctly authorised could leave the Council open to legal challenge by individuals who consider that there has been an intrusion into their private lives or infringement of their right to a fair trial.

2.3 The purpose of the Council's policy and procedure on RIPA**,** is to reinforce the requirements of the RIPA, and relevant Codes of Practice, provide guidance to officers to minimise the risk of legal challenge to the Council and protect the rights of individuals. This policy covers those activities, which are authorised conduct under RIPA.

2.4 Any failure to comply with the policy and procedures set out in this document may be considered a disciplinary offence.

3.0 Implementation

3.1 This policy and procedure replaces any previous policies and procedures, and applies to all Council staff. The Council's standard contract terms and conditions require contractors to comply with all relevant policies of the Council as have been notified to it as part of the Contract. Accordingly, where any contractor may be involved in surveillance activities, this Policy and Procedure should be notified to them as part of the contracting process.

4.0 Basic Requirements

4.1 Under RIPA, directed covert surveillance, use of CHIS and access to communications data should only be authorised if the Designated Authorising Officer is satisfied that:

- **SURVEILLANCE** is likely to obtain *private information*;
- The action is **NECESSARY** for the prevention or detection of a crime (see 1.7 below); and

- Is **PROPORTIONATE** - in that it to the least extent possible the rights and freedoms (of the individual concerned and of innocent third parties), is carefully designed to meet the objectives in question and is not arbitrary, unfair or based on irrational considerations.

4.2 This requires:

- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime;
- Explaining how the methods adopted will cause the least possible intrusion on the subject of the surveillance and/or others;
- Considering whether the activity is appropriate use of the legislation and a reasonable way having considered all reasonable alternatives of obtaining the necessary result;
- Evidencing as far a reasonably practicable what other methods have been considered and why they were not implemented.

4.3 The proposed activity will not be proportionate if the information sought could be obtained by less intrusive means.

5.0 Judicial Approval

5.1 The Council is required to seek **Judicial Approval before** an authorisation can take effect. This is in addition to getting authorisation from one of the Council's Designated Authorising Officers. For communications, data requests the application for Judicial Approval is provided by National Anti-Fraud Network (NAFN) as part of the Single Point of Contact (SPOC) process and sent directly to the Investigating Officer. For directed surveillance and CHIS operations, the application will be prepared and submitted by the Director of Law and Monitoring Officer (Director of Law) whose representative will attend Court with the Investigating Officer when the request for Judicial Approval to proceed is sought. **See Annex A**

5.2 Criminal Threshold - The use of directed surveillance under RIPA is limited to the investigation of crimes, which attract a 6 month or custodial sentence, with the exception of offences relating to the underage sale of alcohol and tobacco - See Annex A

6.0 Types of Surveillance (*includes monitoring, observing or listening to persons; their movements, conversations or other activities and communications*)

6.1 Covert Surveillance is surveillance that is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

6.2 Where those who are going to be targets of surveillance have been informed that surveillance will take place between a clearly specified time periods e.g. test purchases to be made for X weeks after training has been provided by the Council to retailers in respect of their responsibilities in trading in age related products. Overt use of CCTV, does not require an authorisation, and will not be considered to be covert and consequently fall outside of the RIPA regime.

6.3 **Local Authorities are NOT able to authorise to intrusive surveillance, or to interfere with the property of others whilst conducting directed surveillance.** Surveillance is intrusive if it is carried out in relation to anything taking place on any residential premises or in any private vehicle **and** involves the presence of an individual on the premises or in the vehicle **or** is carried out by means of a surveillance device (visual or audio). However a surveillance device **not** on or in the premises/vehicle will only be intrusive if it consistently provides information of the same quality and detail as might be expected to be obtained for a device actually on/in the premises/vehicle.

6.4 For example the placing of a camera in such a manner, which provides images of the activities within residential premises, or the use of a 'tracker', attached to a private vehicle, would constitute intrusive surveillance.

6.5 **Directed Surveillance** - is **covert, but not 'intrusive'** and is undertaken for the purposes of a specific investigation or operation and involving the observation of a person or persons in order to gather **private** information about them (which can include information about persons at work). Where surveillance is covert and is directed at individual(s) to obtain information about them, RIPA is likely to apply and prior authorisation must be obtained.

6.6 Directed surveillance must be authorised in accordance with this policy and procedure.

7.0 Authorisation and Duration

7.1 All requests to conduct, extend or renew a directed surveillance exercise must be made in writing on the appropriate application forms (available from the Director of Law). All requests must be submitted to a Designated Authorising Officer of the Council for their consideration and agreement before seeking a **Judicial Approval** to proceed.

7.2 The power to grant, extend and renew authorisations is limited to Designated Authorising officers, subject to **Judicial Approval**. Extensions should only be

granted where directed surveillance is believed by the Designated Authorising Officer to be **necessary** and **proportionate**. Written authorisations for directed surveillance will be valid for 3 months from the date of the authorisation or extension has been **Judicial Approved.** Designated Authorising Officers are responsible for ensuring that every authorisation is cancelled as soon as it is no longer required, with reviews as to whether, there is a continuing need for the surveillance being undertaken on a regular basis.

8.0 Urgent Authorisations

The Council has no powers to grant urgent oral authorisations to conduct surveillance.

9.0 Equipment

9.1 Surveillance equipment will only be installed once the necessary authorisation of the Council's Designated Authorising Officers has **Judicial Approval**. Permission to locate surveillance equipment in occupied residential premises, to undertake non-intrusive surveillance must be obtained in writing from the householder or tenant. Designated Authorising Officers shall maintain an inventory of the Council's surveillance equipment and all equipment shall be stored securely in Council premises**.**

10. Health & Safety

In addition to a **Judicial Approval**, a covert surveillance operation must not be commenced without detailed consideration of any insurance or health and safety applications and the necessary precautions and insurance having been put in place. Whenever practicable a site visit should always be undertaken prior to the installation of any surveillance equipment.

11. Evidence

11.1 During a covert surveillance operation, recorded material or information collected must be stored and transported securely. It will be reviewed regularly and access to it will be restricted to Designated Authorising Officers, the Director of Law, and the investigation officers concerned in the case.

11.2 The Designated Authorising Officers are responsible for deciding whether requests for access to evidence by third parties, including council officers, should be allowed and having taken legal advice where necessary. Access should generally only be allowed to limited and prescribed parties including law enforcement agencies, prosecution agencies and/or legal

representatives (unless disclosure would prejudice any criminal enquiries or proceedings and/or an individual's right under the Data Protection Act). Designated Authorising Officers will maintain a record of all reviews of material recorded and collected covertly.

11.3 A register will be kept (by the senior investigating officer) of all recorded material, or information collected through the covert surveillance activities. In cases where an Interview under Caution has taken place, the material or information should be retained for at least three years from:

(a) The date the Investigating Officer decides that criminal proceedings are inappropriate;
(b) Director of Law decides the case is not suitable for prosecution;
(c) A court dismisses a prosecution;
(d) The defense or the prosecution withdraws its case;
(e) A court case does not proceed for any other reason.

11.4 Designated Authorising Officers must retain a record of the material shared with any third parties and the reasons for doing this.

12. Covert Human Intelligence Sources (CHIS)

12.1 Definition

A person is a CHIS if:

- They establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything;
- if they covertly uses such a relationship to obtain information or to provide access to any information to another person; and/or
- they covertly disclose information obtained by the use of such a relationship or because of the existence of such a relationship.

12.2 A CHIS may be needed to establish or maintain a personal or other relationship for the purpose of an investigation, i.e. the person with whom the relationship is established is unaware of. A CHIS is "**tasked**" to obtain information, provide access to information or the investigation to otherwise act, incidentally, for the benefit of the relevant public authority.

12.3 Where members of the public volunteer information as part of their *normal civic duties*, e.g. an Anti-Fraud Hotline, they would not generally be regarded as a CHIS. **Similarly, a routine test purchase is unlikely to be considered a CHIS activity where the engagement of the test purchaser with those at the premises from which the test purchase is made is that of a normal transaction and does not entail establishing or maintaining a personal or other relationship**.

12.4 Consequently, the need for the use of CHIS by the Council is likely to be infrequent, however there may be **limited and exceptional circumstances** in which it is necessary to use a CHIS, and the procedures set out below must be followed if such circumstances arise.

12.5 Any designated Authorising Officer seeking guidance in CHIS related matter should contact the Director of Law.

12.6 CHIS Authorisation

12.7 As well as applying the same principles and procedures as for directed surveillance, and seeking necessary approvals there are additional considerations relating to the security, welfare and management of the source, and records relating to them which must be taken into account before the use of a CHIS can be authorised. If followed, material or information obtained from a CHIS may be used as evidence in criminal

proceedings and the proper authorisation of a CHIS should ensure the legality of such evidence.

12.8 Use of a CHIS may only be authorised if it is necessary for the prevention or detection of crime.

12.9 The Designated Authorising Officers listed in Section 20, may authorise the use of a CHIS, provided that they are satisfied that it is necessary and proportionate to do so, and that there are arrangements in place (as set out below) for managing a CHIS.

13.0 An authorisation for a CHIS may be in broad terms and highlight the nature of the CHIS's task**.** However, where it is intended to task a source in a new or significantly greater way, the handler or controller (see below) must refer the proposed tasking to the Designated Authorising Officer, who should consider whether a separate authorisation is required.

13.1 Applications to use, extend or discontinue the use of a CHIS must be made in writing on the appropriate authorisation forms. Written authorisations for CHIS will be valid for a maximum of 12 months from the date of authorisation or extension. As with directed surveillance, Designated Authorising Officers are responsible for ensuring that authorisation is cancelled as soon as it is no longer required, and that reviews of authorisations are carried out on at least a monthly basis.

13.2 Management of the Source

13.3 A Designated Authorising Officer must not seek an authorisation for the use or conduct of a CHIS unless they have appointed a person with day to day responsibility (a 'Handler') who will deal with the CHIS on behalf of the Council, direct the day to day activities of the CHIS, record the information supplied by them and monitor the security and welfare of the CHIS. A Controller with responsibility for the general oversight of them should also be appointed.

13.4 Meetings that take place between the Handler, Controller and/or the CHIS must be recorded, along with details of meeting between the CHIS and the subject of the investigation. Where there are unforeseen occurrences, these should be recorded as soon as practicable after the event, and the authority checked to ensure that it covers the circumstances that have arisen.

13.5 **Record Keeping**

13.6 Proper records must be kept of the authorisation and use of a CHIS, the following records must be kept when a CHIS is authorised:

- The identity of the CHIS;
- The identity, where known, used by the CHIS;
- Any relevant investigating authority other than the authority maintaining the records;
- The means by which the CHIS is referred to within each relevant investigating authority;
- Any other significant information connected with the security and welfare of the CHIS;
- Any confirmation made by a person granting or renewing an authorisation for the conduct or use of a CHIS that relevant information has been considered and that any identified risks to the security and welfare of the CHIS have where appropriate been properly explained to and understood by the CHIS;
- The date when, and the circumstances in which, the CHIS was recruited;
- The identifies of the persons who will act as handler, controller and person responsible for maintaining records of the use of the CHIS;
- The periods during which those persons have discharged those responsibilities;
- The tasks given to the CHIS and the demands made of them in relation to their activities as a CHIS;
- All contacts or communications between the CHIS and the Council's handler;
- The information obtained by the Council by the conduct or use of the CHIS;
- Any dissemination by that authority of information obtained in that way.

13.7 The Home Office Code of Practice on the use of CHIS also contains additional advice on records to be kept in relation to a CHIS. In addition to the authorisation forms, risk assessment, and the above information, a record should be kept of the circumstances in which tasks were given to the CHIS and the value of the CHIS's information in relation to the Council's investigation.

13.8 The records must be kept in a way that preserves the confidentiality of the CHIS and the information provided by them. The Designated Authorising Officer must not authorise the use of a CHIS until a Controller has been designated as the person with responsibility for maintaining a record of the use made of the CHIS, and arrangements are in place for ensuring that the records will be kept securely.

13.9 **Safety & Security**

13.10 Prior to authorising the use of a CHIS, the Designated Authorising Officer

shall have regard to the safety and welfare of the CHIS and shall continue to have such regard, throughout the use of the CHIS. At the outset, the safety and welfare of the CHIS after the authorisation has been cancelled or where the investigation has been closed must also be taken into account. When seeking authorisation to use a CHIS a risk assessment must be completed, to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known and provide it to the Designated Authorising Officer for consideration. This should include the nature and magnitude of any risk to the CHIS; and risks on a personal, operational and ethical basis must be considered. The risk assessment must be taken into account by the Designated Authorising Officer in deciding whether it is appropriate for authorisation to be granted for the use of the CHIS, along with the usual considerations of proportionality, necessity etc. The Designated Authorising Officer must satisfy themselves that any risks identified are justified in relation to the investigation, and that any identified risks have been properly explained and understood by the source.

13.11 The handler of the CHIS will be responsible for bringing any concerns about the personal circumstances of the CHIS to the attention of the controller, in so far as they may affect the validity of the risk assessment, the conduct of the source and the safety and welfare of the source. Where appropriate such concerns should be brought to the attention of the Designated Authorising Officer and a decision taken on whether or not to allow the authorisation to continue.

13.12 The use as a CHIS of vulnerable individuals, such as the mentally impaired, can only be authorised by the Chief Executive (or in his/her absence a Deputy Chief Executive), and **only in the most exceptional cases**. In relation to the use of juveniles as a CHIS, Designated Authorising Officers should also abide by the related Home Office Code of Practice. On no account should the use or conduct of a CHIS under 16 years of age be authorised to provide information where the relationship to which the use of the source relates is between the source and their parents (or any person who has parental responsibility) In other cases authorisation should not be granted unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (SI2000/2793) are satisfied. These requirements relate to the presence of an appropriate adult (e.g. a parent) at meetings with the source and consideration of risk assessments. Authorisation of juvenile CHIS may only be granted by the Chief Executive (or in his/her absence a Chief Officer) and the duration of such an authorisation will be only one month, rather than twelve months.

14.0 Test Purchasing

14.1 This Council's need to undertake test purchasing of age restricted goods such as knives, alcohol, solvents etc, sometimes requires the use of test

purchasers who are juveniles i.e. under the age 18. Test purchasing will be conducted in accordance to the Department for Business Innovation & Skills, Better Regulation Delivery Office, and Code of Practice on Age Related Products.

14.2 When considering the nature of the relationship the young person, undertaking the test purchase on behalf of the Council is unlikely to be construed as a CHIS on a single transaction but this would change if the juvenile revisits the same establishment in a way that encourages familiarity. If the test purchaser wears covert recording equipment, or an adult is observing the test purchase*,* it will be desirable to obtain an authorisation for directed surveillance because the ECHR has construed the manner in which a business is run as private information and such an authorisation must identify the premises involved. In all cases a prior risk assessment is essential in relation to a young person. If conducting covert test purchase operations at more than one establishment, it is not necessary to create an authorisation for each premise to be visited but the intelligence must be sufficient to prevent 'fishing trips'. Premises may be combined within a single authorisation provided that each is identified at the outset. Necessity, proportionality, and collateral intrusion must be carefully addressed in relation to each of the premises.

14.3 It does not follow that there must be a CHIS authorisation because designated public authorities are empowered but not obliged to authorise a CHIS. Therefore, the Designated Authorising Officer must be satisfied that they have fully considered all the relevant issues and decide whether in their opinion that a CHIS has been 'created'. If the purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to granting a directed surveillance authorisation.

14.4 Therefore, when a test purchase is considered to be necessary, it should be based on supporting intelligence that provides a weight of evidence to support it being undertaken and so that the tests of necessity, proportionality, and collateral intrusion must be carefully considered and that a demonstration that overt methods have been attempted.

14.5 If covert technical equipment is worn by the test purchaser, an authorisation for Directed Surveillance is required and such authorisation must identify the premises involved. If an adult is observing the test purchase and no covert technical equipment is used then the decision whether a Directed Surveillance authorisation is required will be based on a careful consideration of the circumstances of the individual case, as this is likely to be considered part of the part of the legislative functions of Council (as per the example above), as opposed to the pre-planned surveillance of a specific individuals. **Any use of** persons to undertake test purchases must be subject to risk assessment which must take account of the safety and

welfare of the test purchaser.

15.0 Requests to undertake Covert Surveillance using the Council's CCTV

15.1 The CCTV Control Room staff from time to time, may be requested to undertake covert surveillance on behalf of other enforcement authorities such as the Police. ALL requests must be supported by an appropriate RIPA Authorisation, from the enforcement authority and a copy of this should be provided to the CCTV Intelligence Manager before the surveillance is commenced.

15.2 The CCTV Intelligence Manager may refuse to provide surveillance facilities, where it is believed that information provided within the RIPA Authorisation, does not enable the requested surveillance to be conducted in accordance, with the relevant codes of practice.

15.3 CCTV Control Room staff will only undertake the surveillance as described within the RIPA Authorisation, and they will remain in control of the cameras and ancillary equipment at all times.

15.4 The CCTV Intelligence Manager shall have operational control of the surveillance being undertaken, and may choose to cease the surveillance at any time in the light of operational considerations.

15.6 However, surveillance request that is unforeseen and undertaken as an immediate response to a situation when it is not reasonably practicable to obtain authorisation, which falls outside the definition of Directed Surveillance will be facilitated at the discretion of the CCTV Intelligence Manage in the light of operational considerations.

16.0 Noise Nuisance Investigations

Where covert recording of noise where the recording is decibels only or constitutes non-verbal noise (such as music, machinery or an alarm) and/or the recording of verbal content is made at a level which does not exceed that which could be heard from the street outside or an adjoining property with the naked ear. The perpetrator would normally be regarded as having forfeited any claim to privacy. In either circumstance, an authorisation is unlikely to be required.

17.0 Social Media

17.1 The use of the internet may be required to gather information prior to and/or during an operation, which *may* amount to directed surveillance. Whenever use of social media is considered as part of an investigation, a consideration must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific investigation. Where it is considered that private information is likely to be obtained, consideration to the whether or not an authorisation is required.

17.2 Where an investigator may need to communicate covertly online, for example contacting individuals using social media websites, a CHIS authorisation should be considered.

17.3 If Social Media Sites are being accessed this should be done only by using a Council operated open account and generally to visit open source material only.

17.4 Where privacy settings are available but not applied the data may be considered open source. Even if open source sites are being reviewed, while reviewing an open source site does not require authorisation, if this is being undertaken regularly a directed surveillance authorisation may be required. Repeat viewing of open source sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

17.5 If it becomes necessary to breach the privacy controls and become, for example "a friend" on a social media site, with the investigating officer utilising a false account concealing their identity for the purpose of gleaning intelligence, this is a covert operation intended to obtain private information and an directed surveillance authorisation should be obtained. If the investigator engages in any form of relationship with the account operator/holder then this will require a CHIS authorisation.

17.6 Therefore investigators when using social media to assist an investigation:

- must not 'friend' individuals on social networks, without seeking an appropriate authorisation for ether Directed Surveillance, CHIS and/or both;
- must not use their own private accounts to view the social networking accounts of other individuals;
- investigators reviewing an individual's profile on a social networking

site should do so only once in order to obtain evidence to support or refute their investigation. Such viewing can take a backward look at the individual's profile;

- further reviewing of open profiles on social networking sites to monitor an individual's status, must only take place once an appropriate authorisation for ether Directed Surveillance, CHIS and/or both has been granted;

- Investigators should be aware that it may not be possible to verify the accuracy of information on social networking sites and, if such information is to be used as evidence, steps must be taken to ensure its validity;

- Investigators who wish to use a false identity to assist in investigation using social media can only do so once an appropriate authorisation ether Directed Surveillance, CHIS and/or both has been granted;

- Investigators are forbidden from using photographs of other persons without their explicit consent to support the use of a false identity (explicit consent being an agreement in writing of how the photograph is to be used to support the investigation). Further, the safety of the person whose identity is used must be fully considered and adequate steps taken to ensure that they are not placed at risk.

18.0 Surveillance in respect of 'Non-Core' Activities or those not meeting the Criminal Threshold and Staff surveillance

18.1 It must be remembered that the Council is only able to seek an authorisation when using the investigation to support its 'core functions'. The 'core functions' were referred to by the Investigatory Powers Tribunal (C v The Police and the Secretary of State for the Home Office - IPT/03/32/H dated 14 November 2006) are the 'specific public functions', undertaken by a particular authority, in contrast to the 'ordinary functions' which are those undertaken by all authorities (e.g. employment issues, contractual arrangements etc). For example:

- A member of staff is suspected by the Council of undertaking additional employment in breach of their contract. The Council wishes to conduct covert surveillance to confirm or refute the allegation. While such activity, even if it is likely to result in the obtaining of private information, would not constitute directed surveillance for the purposes of RIPA as it does not relate to the discharge of the Council's core functions. Rather it relates instead to the carrying out of ordinary functions, such as employment,

which are common to all public authorities. Activities of this nature are covered by the Data Protection Act 1998 and the ICO employment practices codes.

- A member of staff is claiming compensation for injuries allegedly sustained at work is suspected by the Council of fraudulently exaggerating the nature of those injuries. The Council wishes to conduct covert surveillance of the member of staff outside the work environment. Again such activity does not relate to the discharge of the Council's core functions, and therefore would not constitute directed surveillance for the purposes of RIPA as it does not relate to the discharge of the Council's core functions. Rather it relates instead to the carrying out of ordinary functions, such as employment, which are common to all public authorities. Activities of this nature are covered by the Data Protection Act 1998 and employment practices codes.

- A member of staff is suspected of fraudulently claiming a means tested benefit, which the Council administers. The Council wishes to conduct covert surveillance of the member of staff outside the work environment. As the administration of the means tested benefit is a core function of the Council; the proposed surveillance is likely to result in the obtaining of private information and, as the alleged misconduct amounts to the criminal offence of fraud, a directed surveillance authorisation may be appropriate.

18.2 Where any such surveillance is being considered, this should be dealt with in a manner similar to that of a formal authorization being sought under RIPA. A full record as to the reasoning behind the surveillance, who the surveillance was undertaken and the evidence obtained should be recorded. The Director of Law's advice must be sought prior to any such activities taking place. **Under no circumstances, whatsoever must communications data be accessed without a judicial authority, as it is only permitted to undertake directed surveillance in this manner.**

18.3 RIPA and the Data Protection Act (DPA) (which will be replaced by the General Data Protection Regulations from May 2018) do not prevent an employer from undertaking the surveillance of their staff, but such activities must be done in a way which is consistent with the with the requirements of the RIPA, DPA and the General Data Protection Regulations (GDPR).

18.4 However, the must be a clear understanding of whether or not the use of surveillance relates to an allegation in respect of the core function of the Council or if the allegation is connected to the employment of the officer. In the former, it will generally be possible to consider an authorisation under RIPA, in the case of the latter that will not be possible.

18.5 Whenever, surveillance of employees is being considered advice should be

sought from the Director of Law in the first instance and the Information Commissioners Office "Employment Practices Code", should be consulted. This Code provides useful guidance on the monitoring of staff and how this relates to their rights under DPA and GDPR.

19.0 Access to Communications Data

19.1 The Council has the power to gain access to communications data - that is, information held by telecommunication or postal service providers about the use of their services by persons who are the subject of criminal investigations.

19.2 In using such powers, officers must have full regard to the Code of Practice on Accessing Communications Data, issued by the Home Office. As with covert surveillance, access to communications data must be authorised by a designated 'Designated Person' and obtained via the Council's 'Single Point of Contact' (SPOC) who are National Anti-Fraud Network (NAFN). Access to the NAFN website will be required for this. The Order permits access to communications data, by local authorities only where it is necessary for the prevention or detection of crime or the prevention of disorder. As with surveillance, access to communications data should only be authorised where it is proportionate to the objectives the Council is seeking to achieve - it should not be authorised where less intrusive means can be used to further an investigation.

19.3 The Council is only able to gain access to:

- Service Data - this is information held by a telecom or postal service provider about the use made of a service by a person under investigation.

- Subscriber Data - any other information or account details that a telecom/postal service provider holds on a person under investigation.

- Internet Service Provider Information - Service and Subscriber Data.

19.4 Local Authorities are NOT authorised to obtain access to "traffic data" - information about when communications were made, who from and who to. Further, these powers do not permit access to the contents of the communication itself.

19.5 All requests to obtain communications data must be made using the NAFN website and will require a registered NAFN account and may only be granted

where access to communications data is to be necessary and proportionate.

19.6 **Designated Persons**

19.7 The posts listed in Section 20 below, detail those persons authorised by the Council to act as the Designated Person.

19.8 **Single Point of Contact (SPOC) NAFN**

The role of the SPOC is to:

- assess whether it is reasonably practicable to obtain the communications data requested;
- to advise applicants/Designated Authorising Officers on the types of communications data that can be obtained and associated costs;
- to check that the Form is properly completed and authorised; and
- to liaise with the service providers on obtaining the communications data requested.

19.9 NAFN manages communications data requests on behalf of the Council; with NAFN acting as the SPOC for the Council. To make a communications request applicants must first register with NAFN (www.nafn.gov.uk).

19.10 **Procedure**

19.11 Designated Authorising Officer will grant an Authorisation for NAFN to engage in any conduct to acquire the data. The applicant must submit the request completed on the appropriate Form to NAFN, the Council's SPOC. On receipt of the Form, the NAFN will allocate to it a unique reference number.

19.12 If NAFN is satisfied that the application has been made properly, and that the required communications data can reasonably be obtained, the application form will then be forwarded to the Council's Designated Officer for consideration. The Designated Person will then either accept or reject the request and may refuse the application (giving reasons) if they consider that the application has not been properly made.

19.13 If accepted the NAFN will fill in an Assurance of an Authorisation, this Notice must also be authorised by a Designated Officer Person before it can be served on the service provider. Once this has been done, the NAFN will serve the Notice on the Service Provider. When data is provided, the NAFN will then feed it back to the applicant or the designated person.

19.14 The NAFN has one month from the Authorisation being granted by the Designated Officer to request the information sought. If necessary the Authorisation can easily be renewed for a further month - it is important to note that a renewal must be granted prior to the original authorisation expiring.

19.15 The NAFN will record the outcome of the application on the Form and will retain as a record, the application form and notice. The NAFN will also record any cancellations of authorisations made by the Designated Person. Such records must be retained by the NAFN until such time as they have been audited by the Office of Interception Commissioners.

Oral applications for communications data are not permitted

19.16 Errors

19.17 The NAFN will record any errors that occur during acquisition of communications data. Such errors will be reported to the Interception of Communications Commissioner. The Director of Law is the 'Senior Responsible Officer' to oversee the reporting of errors to the Commissioner and to take steps to ensure that such errors do not reoccur.

19.18 There are two types of error:

- **Reportable Errors** - where an error in the application, information/communications data requested and/or information/communications supplied has resulted in the NAFN obtaining information/communications data. This error **MUST** both be recorded and reported to the Interception of Communications Commissioner; or

- **Recordable Errors** - where were an error in the application or information/communications requested results in no information/communications data has been obtained by the NAFN. This error must be recorded and provided to the Interception of Communications Commissioner on request.

20.0 Requesting Authorisation to Undertake Directed Surveillance or Use of CHIS

20.1 Authorisation Procedure

20.2 All authorisation requests for directed surveillance or use of a CHIS, must be made by the Investigating officer using use the appropriate Home Office template forms (available from the Director of Law) (including for a CHIS a

copy of the risk assessment). The Designated Authorising Officer must then consider whether the proposed surveillance is **justified**, **necessary** and **proportionate.**

20.3 Once the Designated Authorising Officer has completed their part of the authorisation form but before it is signed and the authorisation given:

- A hard or electronic copy of the signed authorisation form must be supplied to the Director of Law.

- The Director of Law will review the requested authorisation and in particular advise on whether the issues of proportionality, necessity and collateral intrusion have been thoroughly considered and that the authorisation addresses the requirements of the legalisation and the Office of the Surveillance Commissioner's Code of Practice.

- Once that advice is received, the Designated Authorising Officer must decide whether or not to grant the authorisation and seek Judicial Approval for the conduct to take place (taking into account any revisions to the authorisation as required in response to the advice from the Director of Law).

- The Director of Law will then seek Judicial Approval – see also Annex 1.

- If approved, the authorisation will be entered in the Central Register.

20.4 **Reviews & Cancellations**

- **Reviews** - Designated Authorising Officers should review on a regular basis the Directed Surveillance activity they have approved; if following a review of an active authorisation the Designated Authorising Officer believes that the Authorisation needs to be continued for a further period following the initial end date, then this will also require further Judicial Approval. A copy of the Review form as well as a Renewal Form must be supplied to the Director of Law as soon as practicable. The Director of Law will then seek Judicial Approval - see Annex 1. **This process must be completed before the expiry date of the active authorisation otherwise a new application will be required**.

- **Cancellations** - Designated Authorising Officers retain the authority to cancel an application. A copy of the cancellation form must be supplied to the Director of Law as soon as practicable.

20.5 **Confidential Information**

The Chief Executive (or in their absence the Director of Law) is required to authorise any activity when knowledge of confidential information (confidential personal information, legally privileged information ***and*** confidential journalistic material) is likely to be acquired.

20.6 **Use of Contractors to Undertake Directed Surveillance on Behalf of the Council**

The use of specialist contactors is permitted. When carrying out directed surveillance activities on behalf of the Council, they are only able to carry out such activities that have been authorised and use such equipment that has been stated within the authorisation. The Council's standard contract terms and conditions require contractors to comply with all relevant policies of the Council, accordingly, where any contractor may be involved in surveillance activities, this Policy and Procedure should be notified to them as part of the contracting process.

20.7 Central Record

The Director of Law will maintain a register of all requests and authorisations for covert surveillance together with reasons for any request being denied. The records in this central register will be kept for 3 years, on a rolling basis. A copy of each RIPA form is kept along with a register of the details for each authorisation (date, type of authorisation, subject of surveillance, identity of Designated Authorising Officer and dates of reviews, cancellations and renewals). The Director of Law will be responsible for monitoring authorisations and carrying out an annual review of applications, authorisations, refusals, extensions and cancellations, based on the information contained in the Central Record. RIPA forms will be checked for quality on receipt of forms for the Central Record.

20.8 **Unique Reference Number Procedure**

20.9 Each RIPA authorisation requires a Unique Reference Number (URN). The URN is used as a single reference for the life of an authorization and the Designated Authorising Officer must contact the Director of Law for a URN for each RIPA authorisation.

20.10 When requesting a URN the Designated Authorising Officer will be asked to provide the following information:

- Name/description of the case.

- Confirm whether it is a directed surveillance or CHIS authorisation.

- The Designated Authorising Officer will be provided with a URN which must be used on the authorisation, review and cancellation forms relating to that authorisation.

20.11 The URN is not transferable i.e. if authorisation for which it has been obtained is not proceeded with then the Director of Law must be informed and the Central Register will be updated accordingly.

21.0 Authorising Officers

21.2 Local authority Designated Authorising Officers/designated persons are required to be, Director, Head of Service, Service Manager or equivalent levels.

21.3 The authorisation of directed surveillance or use of a CHIS likely to obtain confidential information or the deployment of a juvenile or vulnerable person (by virtue of mental or other condition) as a CHIS requires authorisation by the most senior local authority officer - Head of Paid Service or, in his/her absence the acting Head of Paid Service. The Council's Designated Authorising Officers are detailed below:

Designated Authorising Officer / Designated Persons			**Area of Activity**
David Hogan	Head of Anti-Fraud	Resources	Directed Surveillance & the Designated Person for Acquisition of Communications Data
Simon Maddocks	Director of Governance	Resources	Directed Surveillance
Andy Opie	Director of Safety	Place	Directed Surveillance
Shayne Coulter	Head of Public Protection	Place	Designated Person for Acquisition of Communications Data

21.4 Responsibilities of Designated Authorised Officers

- Authorised Officers are personally responsible for providing copies of RIPA Authorisations to the Director of Law as soon as practicable, including 'nil returns' for the preceding month where no

authorisations have been granted.

- Where a juvenile CHIS is to be used, prior to seeking the agreement of the Chief Executive,the Director of Law must be informed to ensure that the appropriate legal advice is made available.

21.4 An Authorised Officer may have their authorised status rescinded at any time by the Director of Law.

21.5 Where an Authorised Officer becomes aware of an error in applying and/or a misuse of the application of RIPA they are required to inform the Director of Law as soon as practicable. The Director of Law will then decide upon the most appropriate course of action.

22.0 Security of Documentation & Communications

The following arrangements shall apply for the storage, retention and communication of the documents and information regarding RIPA activities.

Method of Communication / Actions	Procedure
Marking of documents	Marked OFFICAL SENSITIVE on the top and bottom of every page.
Storage of information	Protected by one barrier,e.g. locked cabinet within a secure building, password protected file/folder on the Council network
Disposal of hard copy information	Use confidential information bins
Disposal of Removable storage devices (i.e. floppy discs, USBs, CD & DVD's.)	The disposal of these items must be carried out via the ICT Team.
Internal mail within the Council	In a sealed envelope with OFFICAL SENSITIVE marking shown. Internal reusable envelopes must not be used
Movement of documents between externally based Council departments and/or agencies	By post or courier, in a sealed envelope. Do not show protective marking on the envelope.

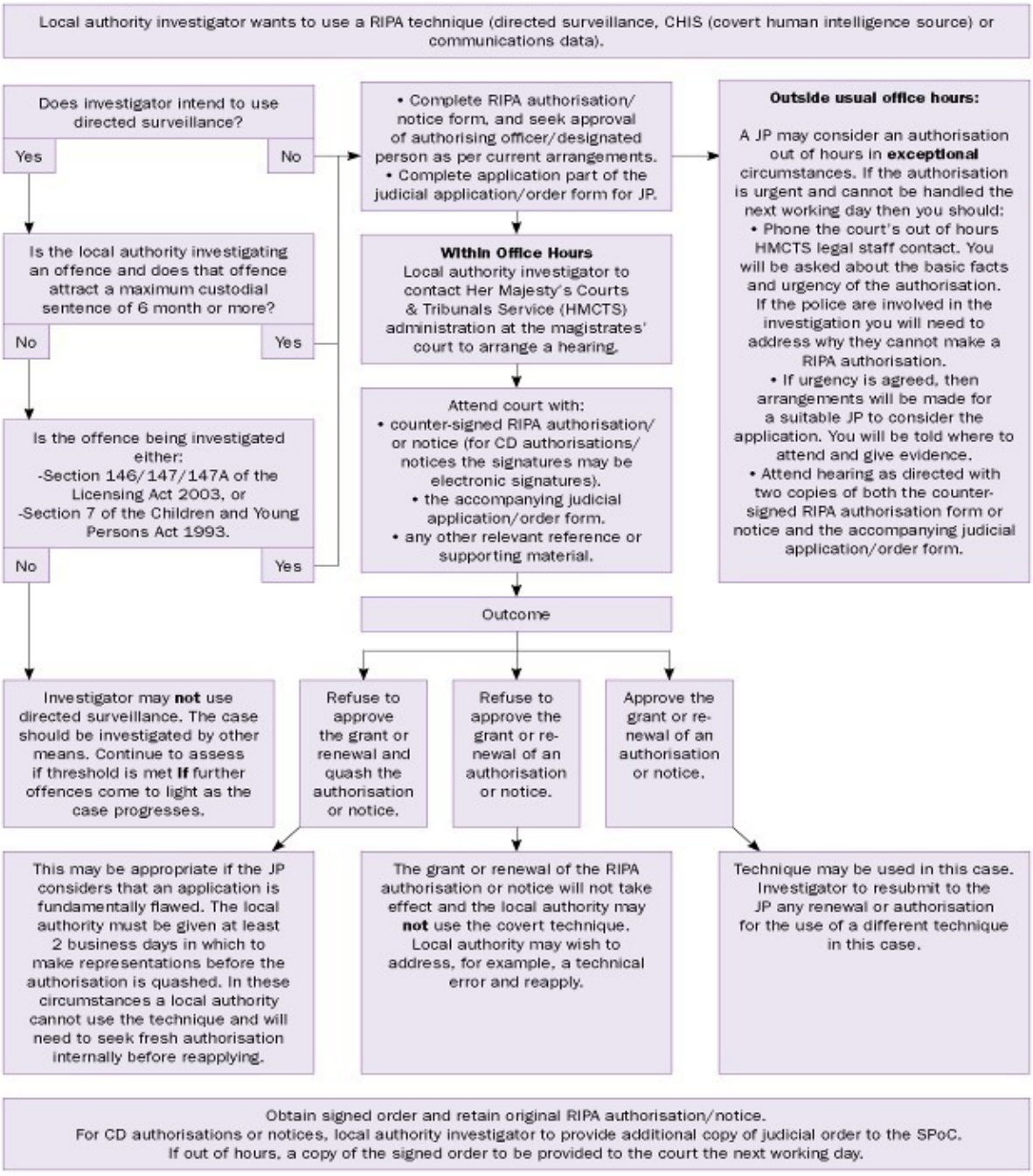
Internal and public telephone networks (including the use of text messages)	May be used. Care should be taken if making calls in a public place; use guarded speech and keep conversation brief. Mobile phones may be used.
PDA's	Not to be used.
Pagers	Not to be used.
Government Secure Intranet and Email systems to be used	When available should be used.
LBC Croydon internal emails and attachments	Egress email when available should be used.
Internet emails	Not to be used
Fax	Check that recipient is on hand to receive

23.0 Consequential Amendments

The Council's Director of Law may authorise consequential amendments to this policy as a result of legislative changes or internal reorganisations within the Council.

ANNEX A

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



This page is intentionally left blank

REPORT TO:	**ETHICS COMMITTEE** **28 February 2018**
SUBJECT:	**USE OF THE POWERS AVAILABLE UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000 YEAR ENDING 31 DECEMBER 2017**
LEAD OFFICER:	**DIRECTOR OF LAW AND MONITORING OFFICER**
WARDS:	**ALL**
CABINET MEMBER:	**Councillor Hamida Ali - Communities, Safety and Justice**
CORPORATE PRIORITY/POLICY CONTEXT: Monitoring compliance with the Regulation of Investigatory Powers Act supports the Council's approach to corporate governance.	
FINANCIAL IMPACT The recommendation contained in this report has no financial implications	
KEY DECISION REFERENCE NO: This is not a key decision.	

1. RECOMMENDATION

The Committee is asked to:

1.1 Note the use of the Regulation of Investigatory Powers Act 2000 by the Council over the past calendar year.

2. EXECUTIVE SUMMARY

2.1 The purpose of this report is to inform the Committee how the powers available to the Council under Regulation of Investigatory Powers Act 2000 (RIPA) have been used over the last calendar year.

3. DETAIL

3.1 RIPA legislates for the use by local authorities of covert methods of surveillance and information gathering to assist the detection and prevention of crime in relation to an authorities core functions. Evidence obtained by any covert surveillance could be subject to challenges under Article 8 of the European Convention on Human Rights (ECHR) - the right to respect for private and family life. However, properly authorised covert surveillance under RIPA makes lawful what might otherwise be a breach of Article 8 of the ECHR and protects the Council from any civil liability. A public authorities "core functions" are the specific public functions it undertakes when providing services, in contrast to the "ordinary functions" which are those undertaken by

all authorities (e.g. employment issues, contractual arrangements etc). Therefore a public authority may only engage in the use of RIPA when in performance of its “core functions”.

3.2 Using RIPA, but only for the purpose of investigating crime and disorder, the Council is able to:

- Carry out covert directed surveillance;
- Use covert human intelligence sources;
- Acquire data relating to communications (e.g. telephone subscriber information).

3.3 ’Covert’ in this context means carried out in a manner calculated to ensure that those subject to the surveillance are unaware that it is or may be taking place. It usually involves personal observation, the use of CCTV, or accessing communications data such as mobile phone number subscriber or website details. However, even using these powers, the Council cannot carry out intrusive surveillance, such as putting a hidden camera in a suspect’s home to observe them, or listening to or obtaining the contents of telephone call or emails; such intrusive surveillance can only be carried out by the Police and government security services.

3.4 Further, even where the covert investigations are for the purpose of preventing crime and disorder, the Council must also show that the surveillance is necessary and proportionate and can be balanced against an individual’s right to their private and family life.

3.5 Covert Human Intelligence Sources (CHIS) are individuals who by the nature of the situation they are in are able to provide information in a covert manner to aid an investigation. The use of CHIS is very tightly controlled under RIPA and historically the Council has not made use of this aspect of RIPA.

3.6 It should also be noted that in respect of communications data, no information regarding the actual content of the communication can be obtained by a local authority. The information obtained is information regarding who pays the bill for a phone, website or where an item of post originated etc. This type of information is most often obtained as part of a Trading Standards investigation where, for example, they are trying to identify and/or locate a trader in counterfeit goods operating from a website, or rogue trader who has billed (often a vulnerable) person for work and where the only point of contact is via a mobile phone number.

3.7 Local Authorities require judicial approval from a Court for the use of covert directed surveillance, covert human intelligence sources (CHIS) and access to communications data (i.e. billing and subscriber information). The use of RIPA to authorising directed surveillance is now limited to cases where the offence under investigation carries the possibility of minimum custodial sentence of 6 months or more being passed on conviction. When access to communications is sought or for test purchasing exercises, this restriction does not apply; nor

does it apply to those directed surveillance operations where investigations into underage sales of alcohol and tobacco are being undertaken.

3.8 **Authorisation Arrangements**

3.9 Overall supervision of the Council's use of RIPA lies with the Director of Law and Monitoring Officer. Day to day monitoring of and advice on authorisations, to ensure that the issues of necessity and proportionality are fully considered and to ensure that all applications meet the necessarily high standard that is required. The application is then made to the Magistrates Court. In accordance with statutory requirements, this team also maintains the Council's Central Register of covert surveillance applications.

4.0 **Occasions when the powers available under RIPA has been used to Support Investigations**

4.1 The occasions and outcomes where the use of the powers available under RIPA to aid the following investigations listed below, were authorised during 2017: Directed Surveillance - None; Communications Data, as detailed below:

Applicant	Purpose	Outcome
Trading Standards (11 applications for subscriber information)	Doorstep crime/fraud investigation; part of national investigation managed jointly by Police and Trading Standards	Investigations ongoing
Environmental Enforcement (5 applications to Royal Mail)	Illegal Waste Transfer/Storage	Prosecution pending

4.2 The Council's use of these powers, its policy and procedures where subject to inspection and audit by the Office of the Surveillance Commissioner and in respect of covert surveillance authorisations under RIPA and the Interception of Communications Commissioner Inspections in respect of communications data in the previous year. During these inspections individual applications and authorisations were closely examined and Authorising Officers are interviewed by the inspectors.

4.3 With the changes being brought about by the passing into law of the Investigatory Power Act 2016, these organisations will be brought together as the Investigatory Powers Commissioner's Office, who now have oversight of the inspection regime.

5. FINANCIAL AND RISK ASSESSMENT CONSIDERATIONS

5.1 There are no direct financial implications arising from this report.

6. LEGAL IMPLICATIONS

6.1 There are no direct legal consequences arising from the contents of this report beyond those set out in the body of the report.

CONTACT OFFICER: Jacqueline Harris-Baker, Director of Law and Monitoring Officer

(ext 62328)

BACKGROUND PAPERS: None

REPORT TO:	**ETHICS COMMITTEE** **28 FEBRUARY 2018**
SUBJECT:	**RECENT DEVELOPMENT ON THE REGULATION OF COUNCILLOR CONDUCT**
LEAD OFFICER:	**DIRECTOR OF LAW AND & MONITORING OFFICER**
CABINET MEMBER:	**CLLR SIMON HALL – CABINET MEMBER FOR FINANCE AND TREASURY**
WARDS:	**ALL**

CORPORATE PRIORITY/POLICY CONTEXT:

The Council has determined that the Ethics Committee shall be responsible for receiving and considering reports on matters of probity and ethics and to consider and recommend revisions to the Code of Conduct.

FINANCIAL IMPACT

Implementation of the recommendations contained in this report have no financial implications.

FORWARD PLAN KEY DECISION REFERENCE NO: This is not a key decision**.**

1. RECOMMENDATIONS

The Committee is asked to:

1.1 Note the recent Department for Communities and Local government (DCLG) consultation: *Disqualification criteria for Councillors and Mayors.*

1.2 (i) Note the recent Committee on Standards in Public Life (CSPL) consultation: *Review of local government ethical standards* (ii) advise the Monitoring Officer of any response the Standards' Committee wishes to make to the consultation and (iii) delegate to the Monitoring Officer in consultation with the Chairman of the Standards' Committee authority to respond to the consultation on behalf of the Committee.

1.3 Note the outcome of a recent case in relation to the regulation of Councillor conduct.

2. EXECUTIVE SUMMARY

2.1 This report provides details of the recent consultation by the DCLG: *Disqualification criteria for Councillors and Mayors*. The consultation seeks views on extending the current disqualification criteria to include anyone subject to:

- the notification requirements set out in the Sexual Offences Act 2003 (commonly referred to as "being on the sex offenders register");

- a civil injunction granted under section 2 of the Anti-social Behaviour Crime and Policing Act 2014; or
- a Criminal Behaviour Order under section 22 of the Anti-social Behaviour, Crime and Policing Act 2014

from standing or holding office as a local authority Member, Directly Elected Mayor or Member of the London Assembly during subsistence of those requirements or sanctions.

2.2 This report also provides details of a case where the former Deputy Leader of Sandwell Metropolitan Borough Council breached the local authority's code of conduct over the alleged sale of three public toilet blocks at an undervalue and the cancellation of parking tickets.

3. DETAIL

DCLG Consultation: Disqualification criteria for Councillors and Mayors.

3.1 The DCLG have recently held a consultation on extending the disqualification criteria for Councillors and Mayors. The consultation ran from 18 September 2017 to 8 December 2017. Responses are currently being analysed. The consultation paper sets out the government's proposals for updating the criteria for disqualifying individuals from being elected or holding office as a local authority member, directly elected mayor or member of the London Assembly.

3.2 The capacity for councillors to hold and remain in office is currently regulated by statute. The current criteria relating to disqualification is set out in the Local Government Act 1972 section 80 and provides that councillors or prospective councillors are disqualified if five years before or since election they have been convicted of an offence and imprisoned "for a period of not less than three months without the option of a fine." Other specified disqualification conditions also apply including employment by the authority or authorities in question, bankruptcy and disqualification under Part III of the Representation of the People Act 1983 (legal proceedings). Similar provisions affect elected mayors of combined authorities (under paragraph 9 of Schedule 5B to the Local Democracy Economic Development and construction Act 2009) and London mayors or assembly members under section 21 of the Greater London Authority Act 1999.

3.3 The government considers that the law should be updated to reflect new options which exist to protect the public and address unlawful and unacceptable behaviour. As a result the government is consulting on extending the current disqualification criteria to include anyone subject to:

- the notification requirements set out in the Sexual Offences Act 2003 (commonly referred to as "being on the sex offenders register");
- a civil injunction granted under section 2 of the Anti-social Behaviour Crime and Policing Act 2014; or
- a Criminal Behaviour Order under section 22 of the Anti-social Behaviour, Crime and Policing Act 2014

from standing for or holding office as a local authority member, directly elected member or member of the London Assembly.

3.4 Any changes to the disqualification criteria would require changes to primary legislation, in particular the Local Government Act 1972, the Local Democracy Economic Development and Construction Act 2009 and the Greater London Authority act 1999.

3.5 The proposed changes would not act retrospectively.

3.6 The Local Government Association (LGA) has provided a written response to the DCLG consultation. The LGA supports the objective of ensuring the highest standards of integrity and conduct among councillors and mayors. It supports measures intended to improve public confidence in elected officials.

3.7 The LGA is supportive of some of the measures in the consultation, specifically the proposal to disbar individuals on the sex offenders register. The current inability to require individuals who have been placed on the sex offenders register to stand down from their local elected office has undermined public confidence in local government.

3.8 However, the LGA raised concerns as to why the proposals only applied to local councillors. If individuals that are on the sex offenders list or subject to an ASB order are unable to hold elected office, then this should also apply to Police and Crime Commissioners, Parliamentary candidates and Members of both Houses of Parliament. Uneven standards are unjustifiable and should be the same for all elected individuals.

3.9 Individuals who are subject to a sexual risk order should also be disqualified from seeking or holding office, on the basis that they could also pose a safeguarding risk and undermine public confidence. This should also apply to all elected individuals.

3.10 The LGA also raised concerns regarding the lack of information put forward to support the wider proposals e.g. for disqualification of individuals subject to a civil injunction or Criminal Behaviour Order. There are many different types of anti-social behaviour behaviours and they could include ‘legitimate protests’ thereby preventing protests of a cause that has significant local support. The LGA is concerned that the criteria could be abused by political opponents seeking to have these sanctions imposed where there is a disagreement on local issues.

3.11 The LGA do recognise that there are some specific categories of anti-social behaviour, such as hate crime, for which there may be justification for excluding individuals found guilty of them from the democratic process. However, the LGA believe that the Government has failed to provide a strong enough rationale or sufficiently describe what the issue is that it is trying to address.

3.12 Members can view the full DCLG consultation paper at:

https://www.gov.uk/government/consultations/disqualification-criteria-for-councillors-and-mayors

3.13 The LGA response can be viewed at:

https://www.local.gov.uk/sites/default/files/documents/LGA%20submission%20to%20the%20consultation%20on%20disqualification%20criteria%20for%20councillors%20and%20mayors.pdf

Committee on Standards in Public Life (CSPL) Stakeholder Consultation: Review of Local Government Ethical Standards

3.14 The CSPL is undertaking a review of local government ethical standards. As part of this review the Committee is holding a public stakeholder consultation. The consultation is open from 12:00 on Monday 29 January 2018 and closes at 17:00 on Friday 18 May 2018.

3.15 ***Terms of Reference.*** The terms of reference for the review are to:

1. Examine the structures, processes and practices in local government in England for:

    a. Maintaining codes of conduct for local councillors;
    b. Investigating alleged breaches fairly and with due process;
    c. Enforcing codes and imposing sanctions for misconduct;
    d. Declaring interests and managing conflicts of interest; and
    e. Whistleblowing.

2. Assess whether the existing structures, processes and practices are conducive to high standards of conduct in local government.

3. Make any recommendations for how they can be improved; and

4. Note any evidence of intimidation of councillors, and make recommendations for any measures that could be put in place to prevent and address such intimidation.

3.16 The review will consider all levels of local government in England, including town and parish councils, principal authorities, combined authorities (including Metro Mayors) and the Greater London Authority (including the Mayor of London).

3.17 Submissions will be published online alongside our final report, with any contact information (for example, email addresses) removed.

3.18 ***Consultation questions:*** The Committee invites responses to the following consultation questions.

a. Are the existing structures, processes and practices in place working to ensure high standards of conduct by local councillors? If not, please say why.

b. What, if any, are the most significant gaps in the current ethical standards regime for local government?

Codes of conduct

c. Are local authority adopted codes of conduct for councillors clear and easily understood? Do the codes cover an appropriate range of behaviours? What examples of good practice, including induction processes, exist?

d. A local authority has a statutory duty to ensure that its adopted code of conduct for councillors is consistent with the Seven Principles of Public Life and that it includes appropriate provision (as decided by the local authority) for registering and declaring councillors' interests. Are these requirements appropriate as they stand? If not, please say why.

Investigations and decisions on allegations

e. Are allegations of councillor misconduct investigated and decided fairly and with due process?

i. What processes do local authorities have in place for investigating and deciding upon allegations? Do these processes meet requirements for due process? Should any additional safeguards be put in place to ensure due process?
ii. Is the current requirement that the views of an Independent Person must be sought and taken into account before deciding on an allegation sufficient to ensure the objectivity and fairness of the decision process? Should this requirement be strengthened? If so, how?
iii. Monitoring Officers are often involved in the process of investigating and deciding upon code breaches. Could Monitoring Officers be subject to conflicts of interest or undue pressure when doing so? How could Monitoring Officers be protected from this risk?

Sanctions

f. Are existing sanctions for councillor misconduct sufficient?

i. What sanctions do local authorities use when councillors are found to have breached the code of conduct? Are these sanctions sufficient to deter breaches and, where relevant, to enforce compliance?
ii. Should local authorities be given the ability to use additional sanctions? If so, what should these be?

Declaring interests and conflicts of interest

g. Are existing arrangements to declare councillors' interests and manage conflicts of interest satisfactory? If not please say why.

i. A local councillor is under a legal duty to register any pecuniary interests (or those of their spouse or partner), and cannot participate in discussion or votes that engage a disclosable pecuniary interest, nor take any further steps in relation to that matter, although local authorities can grant dispensations under certain circumstances. Are these statutory duties appropriate as they stand?

ii. What arrangements do local authorities have in place to declare councillors' interests, and manage conflicts of interest that go beyond the statutory requirements? Are these satisfactory? If not, please say why.

Whistleblowing

h. What arrangements are in place for whistleblowing, by the public, councillors, and officials? Are these satisfactory?

Improving standards

i. What steps could *local authorities* take to improve local government ethical standards?
j. What steps could *central government* take to improve local government ethical standards?

Intimidation of local councillors

k. What is the nature, scale, and extent of intimidation towards local councillors?
   i. What measures could be put in place to prevent and address this intimidation?

3.19 The consultation is aimed particularly at the following stakeholders, both individually and corporately:

- Local authorities and standards committees;
- Local authority members (for example, Parish Councillors, District Councillors);
- Local authority officials (for example, Monitoring Officers);
- Think tanks with an interest or expertise in local government;
- Academics with interest or expertise in local government; and
- Representative bodies or groups related to local government.

3.20 Members can view the full CSPL consultation paper at:

https://www.gov.uk/government/consultations/local-government-ethical-standards-stakeholder-consultation

Case: Sandwell Metropolitan Borough Council Standards' Committee decision.

3.21 In the Sandwell Council case the authority's Standards' Committee considered allegations that the Deputy Leader Councillor Mahboob Hussain had breached the councillor code of conduct in connection with the sale at an undervalue of three public toilet blocks to a family friend and the cancellation of parking tickets issued to family members. After a three day hearing the Standards' Committee found Councillor Mahboob Hussain had breached the code of conduct in connection with the sale of the three public toilet blocks at an undervalue to a family friend. The Standards' Committee also found that the councillor had instructed officers to reduce or cancel three parking tickets for his wife and sons.

3.22 Councillor Hussain's lawyers sought an adjournment of the hearing but this was unsuccessful and the hearing went ahead without him. He is reported to have

said that he refuted the allegations and would have liked to have had the opportunity to defend himself.

3.23 The Standards' Committee found that the actions of Councillor Hussain brought the council into disrepute, compromised officers' impartiality and gave an unfair advantage to the family friend who bought the public toilet blocks and his wife and sons regarding the parking tickets.

3.24 A further hearing in the next few weeks will consider what action is to be taken.

3.25 Members can read further details at:

http://localgovernmentlawyer.co.uk/index.php?option=com_content&view=article&id=33783%3Acouncillor-breached-code-of-conduct-over-toilet-sales-parking-tickets&catid=59&Itemid=27

4. FINANCIAL AND RISK ASSESSMENT CONSIDERATIONS

4.1 There are no direct financial implications arising from this report.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal consequences arising from the contents of this report beyond those set out in the body of the report.

CONTACT OFFICERS: Jacqueline Harris-Baker, Director of Law and Monitoring Officer (ext. 62328)

BACKGROUND DOCUMENTS: None

This page is intentionally left blank

REPORT TO:	**ETHICS COMMITTEE** **28 FEBRUARY 2018**
SUBJECT:	**ANNUAL UPDATE ON ETHICS COMPLAINTS RECEIVED YEAR ENDING 31 DECEMBER 2017**
LEAD OFFICER:	**DIRECTOR OF LAW, COUNCIL SOLICITOR & MONITORING OFFICER**
CABINET MEMBER:	**CLLR SIMON HALL CABINET MEMBER •FINANCE AND TREASURY**
WARDS:	**ALL**

CORPORATE PRIORITY/POLICY CONTEXT:
The Council has determined that the Ethics Committee shall be responsible for receiving and considering reports on matters of probity and ethics and to consider matters relating to the Code of Conduct.

FINANCIAL IMPACT

Implementation of the recommendations contained in this report shall be contained within existing budgets

FORWARD PLAN KEY DECISION REFERENCE NO.: N/A

1. RECOMMENDATIONS

The Committee is asked to:

1.1 Note the contents of the report

2. EXECUTIVE SUMMARY

2.1 The Council has determined that the Ethics Committee shall be responsible for receiving and considering reports on matters of probity and ethics. This is the first annual report to the Ethics Committee to update members on any complaints or investigations undertaken by the Monitoring Officer during the past year.

3. DETAIL

3.1 The 2011 Act requires local authorities to have mechanisms in place to investigate allegations that a member has not complied with the code of conduct, and arrangements under which decisions on allegation may be made.

3.2 Pursuant to the current arrangements which the Committee has approved on behalf of the Council, any complaints which pertain to Members Conduct are made in the first instance to the Monitoring Officer.

3.3 The Monitoring Officer has authority to undertake an initial assessment of the complaint in accordance with the Assessment Criteria which the Committee have specifically adopted for these purposes.

https://www.croydon.gov.uk/sites/default/files/articles/downloads/criteriacomplaints.pdf

3.4 The initial assessment by the Monitoring officer will indicate whether or not the complaint is one which ought to be referred for investigation and if that occurs, the matter is then referred to Members in accordance with the arrangements for dealing with allegations of breach of the code of conduct under the Localism Act 2011.

https://www.croydon.gov.uk/sites/default/files/articles/downloads/Arrangements%20under%20the%20Localism%20Act%202011_July%202012.pdf

3.5 Since the last updating report to members, the Monitoring officer has received 31 complaints. In respect of 10 complaints, the Monitoring Officer requested further information and of those, 6 complainants did not provide further information and accordingly it was not possible to consider or progress the matter.

3.6 In relation to the remaining 25 matters where sufficient information had been provided, the Monitoring Officer undertook an assessment and determined that none of the matters were appropriate to be referred for investigation.

3.7 Over the last year the complaints have related predominantly to planning applications, which can arouse significant public feeling. Just less than half the complaints related to a single planning application. Only 4 of the complaints which were considered for assessment did not relate to complaints arising from planning and were about alleged member conduct at Council meetings and responses to constituent correspondence.

4. FINANCIAL AND RISK ASSESSMENT CONSIDERATIONS

4.1 There are no direct financial implications arising from this report.

5. LEGAL CONSIDERATIONS

5.1 There are no additional legal considerations arising from the contents of this report which are not set out in the body of the report.

CONTACT OFFICERS: Jacqueline Harris-Baker, Monitoring Officer and Council Solicitor (ext 62328)

BACKGROUND DOCUMENTS: None

REPORT TO:	**ETHICS COMMITTEE** **28 FEBRUARY 2018**
SUBJECT:	**ANNUAL WHISTLEBLOWING REPORT FOR YEAR ENDING 31 DECEMBER 2017**
LEAD OFFICER:	**DIRECTOR OF LAW AND MONITORING OFFICER**
WARDS:	**ALL**
CABINET MEMBER:	**CLLR SIMON HALL – CABINET MEMBER FOR FINANCE AND TREASURY**
CORPORATE PRIORITY/POLICY CONTEXT: The Council has determined that the Ethics Committee shall be responsible for receiving and considering reports on matters of probity and ethics and to consider matters relating to the Code of Conduct.	
FINANCIAL IMPACT The recommendation contained in this report has no financial implications	
KEY DECISION REFERENCE NO: This is not a key decision.	

1. RECOMMENDATION

The Committee is asked to:

1.1 Note the use of the Council's Whistleblowing Procedure during the past calendar year.

2. EXECUTIVE SUMMARY

2.1 The Whistleblowing legislation under the Public Interest Disclosure Act 1998 requires employers to refrain from dismissing workers and employees, or subjecting them to any other detriment because they have made a protected disclosure ("whistleblowing"). Whistleblowing occurs when an employee or worker draws attention to a concern or concerns of wrongdoing in their organisation.

3. DETAIL

3.1 The Council uses Public Concern at Work, a third sector provider, (PCaW) to provide independent advice to those who may wish to either raise a concern with the Council to be considered under the Whistleblowing Policy or make a referral to another statutory body. This enables employees to call for confidential advice on whistle blowing and related issues.

3.2 A Whistleblowing situation occurs when an employee draws attention to a concern or concerns of wrongdoing in the organisation which pertains to matters of public interest often referred to as a “protected disclosure”.

3.3 The Council’s Whistleblowing policies are aimed at fostering a climate of openness and transparency in which individuals in the workplace do not feel that they will be victimised if they raise concerns about wrongdoing, and provides the facility to raise these with PCaW an independent organization from whom they can seek advice.

3.4 A copy of the Council’s Whistleblowing policy is attached as Appendix 1. Member’s may wish to note the following sections of the policy which set out its aims and method of operation, as well as the safeguards for employees, who may wish to make use of its provisions.

3.5 A distinction is drawn between a situation where Council employees may wish to raise a grievance or a complaint of bullying and/or harassment which can be dealt with under the Employee Complaints Procedure. In order to make a protected disclosure, which would bring concerns specifically within the ambit of the Whistleblowing procedure rather than the Employee Complaints Procedure, the disclosure must be one which is made in the public interest. As such, it is likely that the appropriate route for some complaints which may in the past have been raised under the Whistleblowing procedure, is now via the Employee Complaints Procedure.

3.6 For the calendar year 2017 three disclosures were formally investigated under the Whistleblowing Policy. The outcomes and recommendations arising from these investigations have either required no further action or recommended actions have been taken forward by the Council.

4. FINANCIAL AND RISK ASSESSMENT CONSIDERATIONS

4.1 There are no direct financial implications arising from this report.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal consequences arising from the contents of this report beyond those set out in the body of the report.

CONTACT OFFICER: Jacqueline Harris-Baker, Director of Law and Monitoring Officer (ext 62328)

BACKGROUND PAPERS: None

REPORT TO:	**ETHICS COMMITTEE** **28 FEBRUARY 2018**
SUBJECT:	**MEMBER LEARNING AND DEVELOPMENT 2017-18 UPDATE**
LEAD OFFICER:	**Jacqueline Harris-Baker,** **Council Solicitor & Monitoring Officer**
WARDS:	**ALL**
CORPORATE PRIORITY/POLICY CONTEXT/AMBITIOUS FOR CROYDON: The Council has determined that the Ethics Committee shall be responsible for receiving reports from the Monitoring Officer on matters of probity and ethics for consideration.	
FINANCIAL IMPACT: There are no additional financial implications arising from the contents of this report.	

1. RECOMMENDATIONS

The Committee is asked to:

1.1 Note the contents of the report.

2. EXECUTIVE SUMMARY

2.1 This report provides the Committee with a log of Member Learning and Development activity in the 2017-18 Municipal Year. This activity is led and monitored by the Member Learning and Development Panel.

3. MEMBER LEARNING AND DEVELOPMENT ACTIVITY 2017-18

3.1 The Council has a £21,000 annual budget for Member training and conferences. This is managed through the cross party Member Learning and Development Panel.

3.2 Activity in the 2017-18 Municipal Year has been as follows:

Event	Date	Attendance
Dealing with dangerous dogs	3 May 2017	Individual event
Health devolution in London	11 May 2017	Individual event
Choice Based Lettings	17 May 2017	9
Prevention Matters: how Elected Members can improve the health of their communities	15 June 2017	7
Licensing	27 June 2017	9
Powering the Electric and Low Emission Vehicle Future	5th July 2017	Individual event
Enhancing Housing Services Conference	11th July 2017	Individual event
The work of the resilience team	14 September 2017	6
Visit to Fairfield Halls	16 September 2017	8
Prince2 weekend	29 September 2017	Individual event
Croydon Observatory	Oct-Dec 2017	5
Children's Services Improvement	16 October 2017	52
What is the Mental health agenda for the new Government?	19 October 2017	Individual event
Focus on Leadership: Effective Opposition - (LGA)	19-20 October 2017	Individual event
Leadership Essentials Finance programme	21-22 October 2017	Individual event
MASH and Children's Social Care Front Door	6 December 2017	12
CfPS The National Scrutiny Conference	6 December 2017	Individual event
Managing Successful Programmes foundation and practitioner training	8 December 2017	Individual event
Excel intermediate	January 2018	Individual event
Care Proceedings	17 January 2018	11
Community economic development training	February 2018	Individual event
Looked After Children	21 February 2018	TBC

4. MEMBER LEARNING & DEVELOPMENT 2018/19

4.1 As 2018/19 is a local election year for all local authorities in London, an induction programme for all 70 Councillors is being developed for May. This will dovetail and complement the Member Learning and Development programme for 2018/19.

5. FINANCIAL AND RISK ASSESSMENT CONSIDERATIONS

5.1 There are no direct financial or other implications arising from this report. Approved by Lisa Taylor, Director of Finance, Assurance and Risk.

CONTACT OFFICER: Stephen Rowan, Head of Democratic Services and Scrutiny.

BACKGROUND DOCUMENTS: None.

This page is intentionally left blank

REPORT TO:	**ETHICS COMMITTEE** **28 February 2018**
SUBJECT:	**DISPENSATIONS APPLICATIONS FOR MEMBERS**
LEAD OFFICER:	**JACQUELINE HARRIS-BAKER, DIRECTOR OF LAW AND MONITORING OFFICER**
CABINET MEMBER:	**COUNCILLOR SIMON HALL**
WARDS:	**ALL**

CORPORATE PRIORITY/POLICY CONTEXT:
The Council has determined that the Ethics Committee shall consider dispensations for Members under the new ethics regime.

FINANCIAL IMPACT

Implementation of the recommendations contained in this report shall be contained within existing budgets

FORWARD PLAN KEY DECISION REFERENCE NO.: N/A

1. RECOMMENDATION

The Committee is asked to:

1.1 In the event of applications for dispensations received, consider the application from the Members and determine whether to grant the dispensation, and if so, the length of time for which such dispensation is to be granted.

2. EXECUTIVE SUMMARY

2.1 Following statutory amendments to the ethics regime, full Council adopted a new Code of Conduct and delegated to the Monitoring Officer and the Ethics Committee the power to consider dispensations under the new ethics regime.

3. DETAIL

3.1 Under Section 31 of the Localism Act 2011 (“the Act”), a Member or co-opted Member who has a disclosable pecuniary interest (DPI) in a matter to be considered or being considered at a meeting of the authority at which that Member or co-opted Member is present and the DPI is one which the Member or co-opted Member is aware of, the Member or co-opted Member may not participate or participate further in any discussion or vote on the matter at the meeting unless he/she has first obtained a dispensation in accordance with the Council’s dispensation procedure.

3.2 The Council has adopted dispensation criteria which are attached for Members' ease of reference at Appendix 1. There are 5 circumstances in respect of which a dispensation may be granted, namely:

i) That so many members of the decision-making body have disclosable pecuniary interests (DPIs) in a matter that it would "impede the transaction of the business";

ii) That, without the dispensation, the representation of different political groups on the body transacting the business would be so upset as to alter the outcome of any vote on the matter;

iii) That the authority considers that the dispensation is in the interests of persons living in the authority's area;

iv) That, without a dispensation, no member of the Cabinet would be able to participate on this matter; or

v) That the authority considers that it is otherwise appropriate to grant a dispensation.

3.3 The Council has determined that in respect of grounds (i) and (iv) above, which involve an objective assessment of whether the requirements are met, it is appropriate to delegate dispensations on these grounds to the Monitoring Officer for determination. The Monitoring Officer is permitted, but not required, to consult with the Ethics Committee prior to determining an application for dispensation on grounds (i) or (iv).

3.4 In respect of grounds (ii), (iii) and (v) above, assessment of these grounds involve a value judgement and are less objective and Council has therefore considered it appropriate that the discretion to grant dispensations on these grounds is delegated to the Ethics Committee, after consultation with the Independent Person.

3.5 The Council currently does not have any outstanding applications for dispensations, however should any be received following the dispatch of the agenda they will be circulated on the evening for consideration.

3.6 In considering the matter, the Ethics Committee is required to assess whether, in light of the contents of the application, the public interest in excluding a Member from participating where a Disclosable Pecuniary Interest exists is outweighed by the considerations set out in the application which support the public interest in the Member being able to participate.

3.7 The Committee is also asked to set out the time period in respect of which it is appropriate to grant the dispensation. In this regard, Members should be mindful of the fact that any dispensation may not be granted for a period exceeding four calendar years, nor is it recommended that a dispensation be granted for a period longer than the remaining term of office of the relevant Member.

4. FINANCIAL AND RISK ASSESSMENT CONSIDERATIONS

4.1 There are no direct financial implications arising from this report.

5. LEGAL IMPLICATIONS

5.1 There are no direct legal consequences arising from the contents of this report beyond those set out in the body of the report.

CONTACT OFFICERS: Jacqueline Harris-Baker,
Director of Law and Monitoring Officer
(ext 64985)

BACKGROUND DOCUMENTS: None

Appendices: Appendix 1 – Dispensation Criteria

This page is intentionally left blank

Appendix 1

Determination of Dispensation Applications:

Under Section 31 of the Localism Act 2011 ("the Act"), a Member or co-opted Member who has a disclosable pecuniary interest (DPI) in a matter to be considered or being considered at a meeting of the authority at which that Member or co-opted Member is present and the DPI is one which the Member or co-opted Member is aware of, the Member or co-opted Member may not participate or participate further in any discussion or vote on the matter at the meeting unless he/she has first obtained a dispensation in accordance with the Council's dispensation procedure.

The provisions on dispensations are significantly changed by the Localism Act 2011. There are 5 circumstances in respect of which a dispensation may be granted, namely:

1.1 That so many members of the decision-making body have disclosable pecuniary interests (DPIs) in a matter that it would "impede the transaction of the business"

1.2 That, without the dispensation, the representation of different political groups on the body transacting the business would be so upset as to alter the outcome of any vote on the matter. ;

1.3 That the authority considers that the dispensation is in the interests of persons living in the authority's area;

1.4 That, without a dispensation, no member of the Cabinet would be able to participate on this matter or

1.5 That the authority considers that it is otherwise appropriate to grant a dispensation.

Any grant of a dispensation must specify how long it lasts for, up to a maximum of 4 years.

The Localism Act gives discretion for the power to grant dispensations to be delegated to a Committee or a Sub-Committee, or to the Monitoring Officer.

This Council has determined that in respect of grounds 1.1 and 1.4 above, which involve an objective assessment of whether the requirements are met, it is appropriate to delegate dispensations on these grounds to the Monitoring Officer for determination. The Monitoring Officer is permitted, but not required, to consult with the Ethics Committee prior to determining an application for dispensation on grounds 1.1 or 1.4.

In respect of grounds 1.2, 1.3 and 1.5 above, assessment of these grounds involve a value judgement and are less objective and Council has therefore considered it appropriate that the discretion to grant dispensations on these grounds is delegated to the Ethics Committee, after consultation with the Independent Person.

Members wishing to apply for a dispensation are advised to complete the dispensation application form, Appendix 1 hereto.

Adopted: July 2012

This page is intentionally left blank