NORTH YORKSHIRE COUNTY COUNCIL

STANDARDS COMMITTEE

18 May 2009

Employee Surveillance Procedures

1.0 PURPOSE OF REPORT

1.1 To consider the Council's arrangements re employee surveillance and whether there is any need to add this area to the Committee's Work Programme.

2.0 BACKGROUND

2.1 The Committee has considered previous reports concerning whether to add to its Work Programme the issue of looking into, from an ethical perspective, the Council's procedures regarding surveillance over employees under regulatory powers in the Regulation of Investigatory Powers Act 2000 ("RIPA") and under the Data Protection Act 1998 and the way in which any information gained is held.

2.2 The Committee felt that there may be some overlap with other parts of the Authority which may be looking at such matters and requested that the issue be discussed with the Corporate Director Finance and Central Services before the item was placed on the Committee's Work Programme.

3.0 EMPLOYEE SURVEILLANCE ARRANGEMENTS

3.1 Not all surveillance of employees is covered by RIPA. Local authorities can only undertake 'directed surveillance' under RIPA for the purposes of crime prevention, detection and preventing disorder. Even then, it must be for a core authority function linked to a regulatory function, eg trading standards. The Council's procedure for RIPA surveillance is attached at Appendix 1 for Members' information.

3.2 In terms of the Council's procedure in this regard, in summary, an application for authorisation to carry out directed surveillance under RIPA must be made by an assistant chief officer or the officer in charge of the investigation (head of the relevant service). The application is made to the Council's Trading Standards and Regulatory Services and any authorisation must be made in accordance with the Act. Authorising officers should not be responsible for authorising matters in which they are directly involved. Any authorisation given makes the surveillance lawful for all purposes and there is no civil liability for any incidental conduct.

3.3 Council Directorates report to Trading Standards and Regulatory Services every quarter on how often they use surveillance procedures. This information is firstly collated by Legal and Democratic Services. Six monthly audit reports are also collated and forwarded to Trading Standards and Regulatory Services for their records. The Council is periodically audited by the Surveillance Commissioner and on the two occasions that the Council has been audited, it has been praised by the auditor.

3.4 Where surveillance is not being conducted for the purposes of the prevention or detection of crime, then this falls outside the RIPA regime, and falls to be dealt with by Internal Audit under the provisions of the Data Protection Act 1998. The Head of Internal Audit has confirmed that surveillance by Internal Audit is rarely undertaken:

in most cases where surveillance would be required, there would be likely to be some suspected criminal activity and therefore any surveillance would be undertaken under the RIPA procedures.

3.5 The procedure attached at Appendix 1 shows the arrangements which must be put in place and adhered to before any surveillance can be undertaken. All officers involved in the surveillance process must undergo specific training. Authorisation for surveillance and the use of covert human intelligence sources should only be carried out where it is necessary and proportionate. Provisions regarding the use, dissemination and retention of any material gathered during such surveillance are set out in section 4 of the procedure (Authorisation of Covert Investigations). Such material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose. Any such information/material gained which is not relevant to an investigation should be immediately destroyed.

3.6 Given the above information, it is recommended to Members that appropriate arrangements, procedures and monitoring are already in place within the County Council regarding employee surveillance (where this is necessary) and that little would be gained by adding this area to the Standards Committee's Work Programme.

4.0 RECOMMENDATIONS

4.1 That Members note the contents of this report.

CAROLE DUNN
Assistant Chief Executive (Legal and Democratic Services) and Monitoring Officer

Background Papers:
None

County Hall
NORTHALLERTON

5 May 2009

APPENDIX 1

PROCEDURES FOR THE AUTHORISATION

OF COVERT INVESTIGATIONS.

1.0 INTRODUCTION:

1.1 Investigations and enquiries across the County Council may involve covert techniques. That is the gathering of information in a manner calculated to ensure that persons subject to observation are unaware it is taking place. Such operations will come within the scope of the Regulation of Investigatory Powers Act 2000 (RIPA). This Act came into force on 25th September 2000.

1.2 In respect of such activities, the Act regulates two broad areas of activity.

i. Surveillance; and

ii. The use of covert human intelligence sources (e.g. informants and under cover officers).

1.3 The Act establishes a legal basis for public bodies to undertake these operations following the introduction of The Human Rights Act into UK law in October 2000. **However, the Act does require that strict rules of authorisation are followed in respect of covert investigations.**

1.4 The purpose of the legislation is to enable covert investigations to take place and yet maintain respect for a person's human rights. In authorising any covert activity to take place officers should have regard to the sensitivities of the local community where the surveillance is to take place, of the likelihood of obtaining confidential material and of the potential for collateral intrusion or interference with the privacy of other persons.

1.5 The Regulation of Investigatory Powers Act 2000 is supported by Codes of Practice on Covert Surveillance and The Use and Conduct of Covert Human Intelligence Sources. These Codes provide guidance on how to ensure operations comply with the Act. Officers who engage in these activities are strongly recommended to read these Codes of Practice.

1.6 These procedures **must** be followed at all times, to ensure any activities undertaken by the County Council are carried out in strict accordance with the relevant legal requirements and Codes of Practice.

1.7 The clear purpose of the RIPA procedures is simply to bring a checks and balancing procedure into covert surveillance type activities to ensure an abuse of authority or power is not taking place.

1.8 Unauthorised surveillance is unlawful and can lead to a civil action against the authority for breach of a person's human rights. In addition it could lead to the exclusion from legal proceedings of any evidence gathered as a result of the unlawful action. Unauthorised surveillance does not, however, lead to the commission of a criminal offence.

1.9 If any County Council employee has not received training in relation to RIPA previously and intends to carry out any activity which MAY fall within paragraph 1.1 they should contact legal services to discuss the proposed activity before seeking an authorisation.

2.0 **SURVEILLANCE:**

2.1 The Act defines surveillance as including any of the following:

a) Monitoring, observing or listening to persons, their movements, their conversation or their other activities or communications;

b) Recording anything monitored, observed or listened to in the course of surveillance; and

c) Surveillance by or with the assistance of a surveillance device.

2.2 It can be seen from this definition that a wide range of activities potentially fit within it. For example:

- Observing a person's home and taking details of cars parked on the drive and their movements.
- Recording covertly conversations between individuals who are the subject of an investigation.
- Covertly watching a person's movements even though those movements are in a public place, e.g. fly tipping.

2.3 In practice, virtually any use that is made of the surveillance equipment such as covert cameras and tape recorders, within an investigation, is likely to come within this definition. However, use of surveillance equipment is not necessarily required for an activity to fall within the definition of surveillance.

2.4 It should be noted that where an officer tape records a telephone conversation they are having with another person, in the course of an

investigation, this is classed as directed surveillance and will require prior authorisation.

2.5 The surveillance examples illustrated above will be lawful provided they are authorised in accordance with **Section 4** of these procedures.

2.6 Surveillance is split into two categories by the Act:

i. Directed surveillance;

ii. Intrusive surveillance.

2.7 Intrusive surveillance is covert surveillance carried out in a person's home or other residential premises or in a private vehicle without consent, and can only be undertaken by the Police and other specialist agencies after the highest level of authorisation, for example by the Chief Constable. **County Councils cannot undertake intrusive surveillance under any circumstances.**

2.8 **Directed surveillance** is covert surveillance which is undertaken:

a) For the purposes of a specific investigation or a specific operation;

b) In such a manner as is likely to result in the obtaining of <u>private information</u> about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

c) Otherwise than by way of an immediate response to events which would make it impossible to gain the appropriate authorisation.

2.9 Directed surveillance is the category of surveillance that will be undertaken by County Council services. To be lawful it must be authorised in accordance with **Section 4**.

2.10 Officers should note the following passage from the Code of Practice on Covert Surveillance which states:

"Public Authorities are strongly recommended to seek an authorisation where the purpose of a covert surveillance, wherever that takes place, is to obtain private information about a person, whether or not that person is the target of the investigation or operation. Obtaining an authorisation will ensure that the action is carried out in accordance with the law and subject to stringent safeguards against abuse. It will

also make the action less vulnerable to challenge under the Human Rights Act 1998".

2.11 Section 26(10) of RIPA defines private information as "in relation to a person, includes any information relating to his private or family life". This definition has been expanded by the European Court of Human Rights in its judgment in the case of Amann – v – Switzerland in respect to Article 8 which says "respect for private life comprises the right to establish and develop relationships with other human beings; there appears, furthermore, to be no reason in principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature". Officers must therefore assume that information gathered from surveillance at a business premises is likely to come within the definition of "private information".

3.0 COVERT HUMAN INTELLIGENCE SOURCES:

3.1 A covert human intelligence source is defined as a person who:

a) Establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs (b) or (c).

b) Covertly uses such a relationship to obtain information or to provide access to any information or another person.

c) Covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

3.2 In practice there will be two main types of covert human intelligence sources

i. Informants (paid or unpaid); and
ii. Officers working under cover

3.3 In relation to informants, authorisation in accordance with the Act will be required when the informant is first registered. This authorisation should indicate the purpose for which the source will be tasked or deployed. If the informant is to be tasked for a different purpose then another authorisation should be sought.

3.4 **Working with covert human intelligence sources carries risks and should only be undertaken by trained officers**. These procedures should be followed at all times to ensure the safety of officers and the source, and all officers involved in the use of covert human intelligence sources should ensure they are familiar with the Guidance Notes at **appendix 1.**

3.5 An officer working under cover, gathering information by concealing his or her identity, will usually require the activity to be authorised in accordance with **Section 4.** The authorisation would also cover the use of any body worn covert recording device. Other directed surveillance of a covert human intelligence source would require separate authorisation.

3.6 Routine test purchases will not require authorisation because they involve nothing more than an officer or a young person visiting a shop or market stall and buying a particular item. The purchaser does not form any sort of relationship with the seller. He does not enter into anything more than the minimum conversation required to make the purchase, and does not mislead the seller. This last point is of particular relevance in relation to young purchasers. If challenged by the seller on the question of age, the young purchaser must not mislead the seller but must give their true age. An attempt to mislead will be likely to bring the young person within the Section 26(8) definition and require authorisation in accordance with **Section 4.** The LACORS "Practical Guide to Test Purchasing" (**appendix 11**) considers a number of issues arising from age restricted test purchases, including RIPA implications. The guide reproduces a letter from the Home Office to LACORS which confirms the position as stated above. Officers should familiarise themselves with the code and follow it in relation to age-related test purchases.

However, in situations where the purchaser may have to gain the trust of the seller before the purchase can be made it is likely that the potential purchaser will be a CHIS. An example of this would be a test purchase of unclassified or counterfeit DVDs via the internet where the purchaser must establish an e-mail relationship with the seller before the seller is comfortable enough to confirm that material of that type is available and to make the sale. Authorisation will be required in accordance with **Section 4**.

Officers should also note that the definition in Section 26(8) makes no reference to "private" information. This is in contrast to the definition of directed surveillance in Section 26(2) which does refer to private information.

3.7 Officers may on occasion be offered unsolicited information from what may be termed a "confidential source". An individual who volunteers information without being tasked will not be a CHIS. Such individuals can broadly be categorised into three groups, reflecting that s.26(8) includes both a 'personal or other relationship' :

1. Public spirited individuals who volunteer information as part of their civic duty;

2. Individuals passing on information in the course of their employment where there is no duty to do so;

3. Individuals, usually offenders themselves, who volunteer information about criminal associates.

In the majority of cases, it is likely that a confidential source will be an individual doing no more than his civic duty in passing on information about the sale of counterfeit goods, the sale of age-restricted products to minors and so on. In such cases the source will not become a CHIS. This is made clear in para 1.3 of the CHIS Code of Practice. However, officers must be clear that, if they go on to task that individual to build or maintain a relationship with someone to obtain further information covertly, the source will become a CHIS and authorisation will be required.

It is less likely that individuals falling into the second and third categories will provide information. However, the situation is the same. If the source simply volunteers information they are not are CHIS, but if asked to build or maintain a relationship to obtain information covertly they will become a CHIS and authorisation will be required.

Officers must pay particular attention to the risk of 'status drift' when dealing with confidential sources. This term describes the situation where an individual repeatedly offers information and so drifts into the position of a CHIS by implication. Officers who are offered information by the same source on more than two occasions must take advice from the Section Leader (Fraud & Special Investigations) or the Section Leader (Enforcement, Licensing & Process) about seeking CHIS authorisation.

3.8 Where an individual provides information as a confidential source rather than as a CHIS, their details must be recorded in the Confidential Source Register (CSR). Officers should complete a CSR application form (**appendix 12**) which is submitted to the Section Leader (Fraud & Special Investigations). (For trading standards staff this can be done directly, and for other services it should be done via Legal Services.) If the application is approved the details will be entered into the paper register held by the Section Leader (Fraud & Special Investigations) and a unique CSR number will be allocated. The details of the source and the information will also be recorded on the trading standards Flare database, however, once the CSR number has been allocated the investigating officer should immediately remove the source's name and address or other identifying details from Flare and replace them with the CSR number.

4.0 AUTHORISATION OF COVERT INVESTIGATIONS:

4.1 Any covert activity which comes under the definition of directed surveillance or the use of a covert human intelligence source requires **prior authorisation**. This authorisation can only be granted by an Assistant Head of Service or Head of Service. In respect of the different County Council services, officers should seek authority from the following individuals:

a) For the Trading Standards Service, officers should first seek approval for the activity from their line manager / supervisor, prior to the authorisation being sent to the Section Leader (Enforcement, Licensing and Process) (Assistant Head of Service) / Head of Service.

b) For Internal Audit, officers should seek authority from the Head of Internal Audit.

c) For any other Service, officers should first seek approval from their line manager / supervisor, to agree the planned activity is satisfactory and that the officer can seek the relevant authority. The supervisor should, if appropriate, also seek approval from a member of the Service's senior management, prior to the officer seeking the relevant authority. An approach should then be made, if not already done so, to the Head of Legal Services for advice and assistance. A record should be made of this request by both the Manager seeking the advice and the Head of Legal Services. Once agreement has been reached about the nature of the activity to be undertaken, the officer should contact the either the (Section Leader, Enforcement Licensing and Process) or the Section Leader (Fraud and Special Investigations) of Trading Standards & Regulatory Services for advice about completion of the application form if necessary. The form should then be submitted to the Section Leader, (Enforcement, Licensing & Process) for authorisation. In her absence the form should be submitted to the Section Leader, (Fraud & Special Investigations) or the Head of Service. The officer in question will then be notified by the RIPA Systems Administrator at Trading Standards as to whether or not authorisation has been granted.

Authorisation for surveillance and the use of a covert human intelligence sources should only be carried out where it is necessary for the purposes of the investigation being carried out and is proportionate to what it seeks to achieve. **It is essential to demonstrate that the information sought from the surveillance is required for the prevention and detection of crime or preventing disorder. If this is not possible, the surveillance will not be authorised.**

4.2 Officers should complete all relevant sections of the authorisation forms, pro-formas of which are to be found in **appendix 10**.

Before covert activity can be properly authorised it must be shown to be necessary. Authorisation must not be given where the information sought can be found by other means. Other possible avenues must have been considered and discounted before covert activity is used. Necessity may arise because there is no other way of gathering the information, or because to seek the information from elsewhere would compromise the investigation.

Once it is established that the covert activity is necessary, it must then be shown to be proportionate. Proportionality can broadly be divided into three elements; that the covert methods used are not excessive in relation to the seriousness of the offence, that the method is the least invasive of the suspect's privacy and that collateral intrusion is minimised.

Officers must consider each of these points carefully for each case. The extent of the covert activity to be used should be carefully determined having regard to the seriousness of the offences under investigation. In some cases, the seriousness may speak for itself, for example, in cases of deceptions against the elderly or vulnerable involving large amounts of money. In others the offending may become more serious because a minor offence, for example a scam costing each victim only a few pounds, is repeated on a large scale across the county, region or country.

Officers should also plan the intended covert activity so it does not exceed the type and scale of activity needed to obtain the necessary information. For example, if an activity is planned only to establish that an individual resides at a particular address, it would not be proportionate to continue surveillance of his movements after that had been confirmed. In contrast, if it is necessary both to establish his place of residence and also to confirm links with other individuals at other premises it may be proportionate for surveillance to continue to determine whom and where he visits.

Careful attention should be paid to the risk assessments, to ensure any risk to anybody who may be involved within the operation, or affected by it, is minimised and that the methods to achieve this are specified in the operational risk plan. The potential for incurring any collateral intrusion into any other person's privacy should be identified and an appropriate plan developed to minimise this risk where relevant. In respect of confidential material the following general principles should be observed.

(a) Those handling information/material from operations should be alert to matters which may fall within the definition of confidential material. Where there is any doubt about the status of the material, advice should be sought from the officer in charge of the operation

and/or an Assistant Head of Service before any further dissemination.

(b) Such material should not be copied or retained unless it is necessary for a specific purpose.

(c) Material should be disseminated only where an appropriate officer (Assistant Head of Service or above) is satisfied it is necessary for a specific purpose.

(d) Any retention or dissemination of such material should be accompanied by a clear warning of its confidential nature and reasonable steps should be taken to ensure that there is no possibility of it becoming available, or its contents becoming known to any person whose possession of it might prejudice any related criminal or civil proceedings.

(e) Such material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose. The destruction of material should be supervised by an appropriate senior officer.

4.3 Authorising officers should carefully consider each application and scrutinise them on the following points:

a) Is the operation necessary?

b) Are the covert techniques proportionate to the criminal act?

c) Is the information required for the prevention or detection of crime or the prevention of disorder?

d) What are the risks of collateral intrusion and are these justified by the operation?

e) Do you need to put conditions in place to limit the likelihood of collateral intrusion?

f) What are the risks of obtaining sensitive material?

g) Does the operation take into account all the relevant health and safety risks?

h) When will the operation be reviewed? Do you need to suggest/stipulate an earlier review period?

It is important for the authorising officer to indicate the reasons for their decision and the thought processes applied to the request.

4.4 If an officer wishes to use a covert human intelligence source in one of the following ways:

a) Initially register an informant;

b) Task an informant, or

c) Undertake an operation with an officer working under cover, including the cultivation of a source;

then the officer will need to seek authorisation by completing the relevant forms. For officers working under cover, then a separate form needs to be completed.

4.5 The initial authorisation to use a CHIS (informant) will detail the conduct the CHIS (informant) will undertake. If the CHIS (informant) is to be tasked to obtain information in a different way potentially interfering with the privacy of different individuals then that conduct will require further separate authorisation to be assessed on its own merits.

4.6 Authorisations for surveillance operations will last for a period of 3 months and authorisations for the use of a covert human intelligence source will last for a period of 12 months. If, after this period of time, continuing authorisation is required then consent will need to be obtained from the Section Leader, Enforcement, Licensing & Process or Head of the Trading Standards Service. The relevant forms must be completed.

4.7 Each authorisation will contain a review period at which time the investigating officer and the respective supervising officer should review the covert activity to decide if the authorisation needs to be cancelled or altered in any way. Again, the relevant forms should be completed.

4.8 Authorisations should be completed, **prior** to the activity an officer is seeking to authorise taking place. However, in **urgent cases**, authorisations may be given orally. In such circumstances, a statement that the authorising officer has expressly authorised the action should be recorded as soon as is reasonably practicable. This should be done by the person to whom the authorising officer spoke but should later be endorsed by the authorising officer. As soon as is reasonably practicable, the relevant forms should be completed, with the urgent authorisation section also being completed.

4.9 If an operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or who are not covered by the original authorisation then those carrying out the covert operation should inform the authorising officer. If the operation

is to continue it may be that the original authorisation is not sufficient and consideration should be given to whether separate authorisation is required.

4.10 All authorisations need to be cancelled once the activity has been completed and before the expiry of the authorisation.

4.11 Guidance notes for the use of covert human intelligence sources are contained in **Appendix 1**. Examples (provided by Trading Standards Service) of additional forms to be completed by officers, contained in **Appendices 2 – 8.**

4.12 All records of authorisations will be kept for a minimum of six years and should only be destroyed with the consent of the Section Leader, Enforcement, Licensing & Process or Head of Trading Standards and Regulatory Services, or in the case of Internal Audit, by the Head of Internal Audit.

4.13 Any information/material gained as a result of surveillance or the use of a covert human intelligence source which is not relevant to an investigation is to be immediately destroyed. The destruction of such material should be supervised by the appropriate supervising officer.

4.14 All material/information gained which may be relevant to an investigation should be retained in the investigation file or as unused material in accordance with the Trading Standards and Regulatory Service's procedures or the procedures of Internal Audit, or as directed by Head of Legal Services.

5.0 TRAINING:

5.1 The Head of Legal Services has responsibility for ensuring Business Unit Heads are kept up to date with developments in the legislation and Codes of Practice regarding the Regulation of Investigatory Powers Act 2000.

5.2 In addition, all those involved in carrying out activities which fall within the scope of the Regulation of Investigatory Powers Act must receive at least one training session a year to act as refresher training, to update and improve their existing knowledge. This training will be organised by the Training Officer of Trading Standards and Regulatory Services, in conjunction with the Assistant Head of Service. The training will be made available to officers from all other County Council Services.

5.3 The Training Officer for Trading Standards and Regulatory Services will also maintain records of officers attending such training and will make the records available to the Systems Administrator at Trading Standards.

6.0 INVENTORY:

6.1 Any County Council Service using surveillance equipment used in relation to authorisation of surveillance shall make an inventory of such equipment and its uses. The Special Investigations Unit of the Trading Standards and Regulatory Services should maintain an inventory of all surveillance equipment used in relation to authorisations granted for surveillance. The inventory should be kept in the surveillance equipment cupboard in the Special Investigations Unit room. A copy of the form at Appendix 9 should be used in respect of each separate piece of surveillance equipment. Officers using the equipment should use the form to book out the equipment and make reference to the RIPA authorisation number granted for the surveillance in the relevant box on the form.

6.2 The Head of Internal Audit should also maintain a log of use of any equipment used for surveillance work. Again, this should include reference to the RIPA authorisations granted for the surveillance.

7.0 AUDIT:

7.1 The Systems Administrator at Trading Standards and Regulatory Services has
responsibility for carrying out periodic reviews of the operation of these procedures.

7.2 On a quarterly basis the Systems Administrator will carry out an audit of all authorisations. The audit should examine the number and status of all authorisations in the system. This should include checking that cancellation, review and renewal dates have been met and that there are no outstanding actions required in respect of any authorisations. If any discrepancies are found, these should be reported to the Section Leader, Enforcement, Licensing & Process or Head of Service for Trading Standards and Regulatory Services, or the Head of Internal Audit, as appropriate, in order for them to take appropriate action.

7.3 In addition to the above quarterly audit, the Systems Administrator should also, on a six monthly basis, contact all relevant Directorates of the County Council, to check whether they have engaged in any activities which required RIPA authorisation. In addition they should check for any training needs and ensure that awareness of RIPA is maintained. Records should be maintained of these checks. If such activities have been undertaken without appropriate authorisations, notification of this should be given to the Head of Legal Services, Head of Internal Audit, or Section Leader, Enforcement, Licensing & Process for Trading Standards and Regulatory Services, as appropriate.

7.4 On an annual basis the Systems Administrator will request each service using surveillance equipment to carry out an audit of the equipment and an update of the inventory.

8.0 COMPLAINTS:

If any officer receives a complaint from a member of the public in relation to a covert operation then the complaint should be notified to the Section Leader, Enforcement, Licensing & Process and the matter referred to the Investigatory Powers Tribunal established by the Government. The Tribunal can be contacted at the Investigatory Powers Tribunal at the following contact point.

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ.

Telephone 0207 0353711