



East Cambridgeshire District Council

CORPORATE POLICY  
FOR THE USE OF  
COVERT SURVEILLANCE  
AND  
COVERT HUMAN INTELLIGENCE  
SOURCES (CHIS)

**This document has been prepared following the implementation of the  
REGULATION OF INVESTIGATORY POWERS ACT 2000**

## CONTENTS

1. Introduction
2. Relevant legislation
3. Policy and Guidance
4. Audit & Monitoring
5. Procedure for obtaining Authorisation
6. Documentation & Guidance on Completing the Forms
7. Duration of Authorisations. Details of Reviews, Renewals and Cancellations.
8. Handling Material Obtained from Directed Surveillance (DS) and CHIS operations.
9. Telecommunications Data, Recording of Telephone conversations etc
10. Further information
11. Glossary of Terms

### **FORMS (– these are not enclosed, but separately under “Form” on intranet)**

- Appendix 1 - Application for DS.
- Appendix 2 - Review of DS Form.
- Appendix 3 - Application for Renewal of DS.
- Appendix 4 - Cancellation of DS Form.
- Appendix 5 - Application for use of a Covert Human Intelligence Source (CHIS).
- Appendix 6 - Review of CHIS.
- Appendix 7 - Application for Renewal of CHIS.
- Appendix 8 - Cancellation of CHIS.

### **OTHER APPENDICES**

- Appendix 9 - List of Authorised Officers.
- Appendix 10 CCTV system service for East Cambridge District Council (Cambridge City Council Policy)
- Appendix 11 CHIS IDENTITY INFORMATION.
- Appendix 12 Cambridge City CCTV Code of Practice (June 2009)

Home Office Codes of Practice *A: Covert Surveillance & B: Covert Human Intelligence Sources* – can be accessed through direct link at 1.6 below.

## 1.0 INTRODUCTION

- 1.1 This document sets out the Council's obligations under the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA came into force in October 2000 and regulates, amongst other things, types of covert surveillance that can be undertaken and the use of a Covert Human Intelligence Source (CHIS). Under RIPA the Council must have procedures in place that ensure surveillance is properly authorised, with full consideration given to the necessity and proportionality of the covert surveillance or CHIS in the context of individuals rights under the Human Rights Act 1998 (the HRA). RIPA also provides a number of safety measures in that it limits those that can or should use covert surveillance, the grounds and circumstances in which it can be used and how the material obtained must be dealt with. In the main Local Authorities have restricted powers to undertake surveillance, with more intrusive techniques restricted to intelligence and law enforcement agencies investigating the most serious crimes, including in the interests of national security. Even where this is consider an important tool to take an investigation further, these should be the exception, rather than the rule. RIPA also provides for oversight by an independent Surveillance Commissioner and with a tribunal to hear complaints from those that believe that techniques have been used inappropriately.
- 1.2 The HRA requires the Council and any organisations working on its behalf to respect the private life and family of citizens, their home and their correspondence. This is not an absolute right and as such the Council may interfere in the citizens rights mentioned above if, the interference is: -
- a) In accordance with the law,
  - b) Necessary, and
  - c) Proportionate.
- 1.3 Covert surveillance or the use of a CHIS is usually a last resort in an investigation. RIPA sets out a statutory mechanism for authorising covert surveillance or a CHIS, and this will only be undertaken where there is no reasonable and less intrusive means of obtaining the information.
- 1.4 Staff directly employed by the Council and external agencies working for the Council are covered by RIPA whilst they are working for the Council in a relevant investigatory capacity. The main agency that will be involved in such work for the Council, is the Anglian Revenues Partnership. Authorisation of any covert surveillance or use of a CHIS, within the Council's District, will be in accordance with this Policy and authorised by the Authorising Officers (AO) identified in Appendix 9.
- 1.5 Compliance with RIPA/ Codes of Practice/ relevant legislation and the procedures set out in this Policy, protects the Council and its Officers against legal challenge. Section 27 of RIPA states that "conduct...shall be lawful for all purposes if an authorisation...confers an entitlement to engage in that conduct on the person whose conduct it is and his conduct is in accordance with the authorisation". Failure to abide by RIPA/ this Policy renders the Council liable to claims and or could affect the use of the information in any subsequent criminal proceedings.
- 1.6 In addition to setting out the procedures that must be followed, this Policy aims to provide guidance to Officers about the circumstances where they are permitted to embark on covert surveillance or use a CHIS. The forms detailed above also have relevant guidance notes in commentary boxes within the documents to assist Officers. However, Officers can *and should* obtain further assistance/ guidance from Legal Officers within Legal & Democratic Services. Any Officer who is likely to make applications or authorise them should undertake training (which will be arranged periodically or on request by Legal & Democratic Services) and in all cases Officers should be familiar with the

relevant Codes of Practice before making any application. The Codes are currently being revised and any queries should be directed to legal. Hyperlinks will be inserted when available:

## GENERAL

- 1.7 There will be times when Council Officers need to conduct surveillance in the course of their investigatory duties: for example, fraudulent housing benefit claims, nuisance investigations etc. *Surveillance is a last resort that an investigator will use to prove or disprove an allegation.* Officers should always consider using other overt investigatory tools (such as community advice, warnings, signposting, inspections) before considering whether an authorisation under RIPA is required. Most of the time, however, the surveillance will be “low-level” or “overt” (see 3.1.10-3.1.11). Low-level or overt surveillance does not usually require any RIPA authorisation. However, each individual situation must be considered separately in the light of RIPA to ensure compliance.
- 1.8 Covert surveillance may, however, be required for some investigations; this means surveillance carried out in a manner calculated to ensure that the person subject to surveillance is unaware that it is or may be taking place and it can be **intrusive or directed**. Surveillance is *intrusive* if it is carried out by an Officer or with the use of a surveillance device, in a residential premises or private vehicle. Local Authorities are **NOT** authorised to conduct intrusive surveillance.
- 1.9 With the exception of low-level or overt surveillance, all other surveillance carried out by the Local Authority must therefore be ‘directed’. This is covert but not intrusive surveillance, conducted in a manner that “*involves the observation of a person or persons with the intention of gathering information to produce a detailed picture of a person’s life, activities and associations for the purpose of a specific investigation or operation*”.
- 1.10 There may also be situations where the use of a **CHIS** (which can be a Council employee), is required. Their use is also regulated by RIPA (under section 29). A CHIS is a person who establishes or maintains a relationship with someone in order to covertly obtain information, to provide another person with access to information or to disclose information as a consequence of that relationship. Examples include the covert use of an Officer to establish whether a particular person has been fly tipping/ or and in accordance with OSC guidance<sup>1</sup>, if Officers are considering undertaking a Test Purchase case, this may need CHIS authorisation (for example “pretending” to be a legitimate customer for detection of unlicensed taxi drivers). ***A CHIS should not be engaged/ authorised until advice has been sought from Legal Officers within Legal & Democratic Services.***
- 1.11 Directed surveillance (DS) or the use of a CHIS must be carried out in accordance with RIPA and only commence when authorisation has been granted.
- 1.12 **Scope of this Policy**  
This document is intended to cover the surveillance and information gathering techniques, which are most appropriate to local authority work. In this context this also includes the investigation of internal fraud. Other techniques, such as some of those listed below, which are not regularly undertaken by local authorities have not regulated by this Policy.

---

<sup>1</sup> Office of Surveillance Commissioners Procedures and Guidance – December 2008\*  
RIPA POLICY 07/07 reviewed 11/09

- The interception of any communication such as postal, telephone or electronic communications without both the sender and receiver's permission. (See below for summary of powers to obtain information about communications from communications services providers)
- The covert use of surveillance equipment within any premises or vehicle, including business premises and vehicles, with the intention of covertly gathering information about the occupants of such premises or vehicles, unless undertaken as part of a CHIS authorisation.
- The control and disclosure of information held on computer or paper records covered by the Data Protection Act or Freedom of Information Act.

If it is intended to carry out such activity further guidance should be sought from Legal Officers within Legal & Democratic Services.

In addition, this document does not address the detailed assessment of risks that Officers will need to undertake as part of any investigation. Normal departmental policies on identifying such risks should be adopted if it is perceived that any risk might arise from a specific operation. The CHIS authorisation form in Appendix 5 at section 8 specifically refers to risk assessment, and should be considered and completed in full before any application is considered.

## 2.0 RELEVANT LEGISLATION

### 2.1 The Data Protection Act 1998 (DPA)

2.1.1 The DPA provides eight principles to be observed to ensure that the requirements of the Act are complied with. They provide that personal data, which includes personal data obtained from covert surveillance techniques, must:

- (1) be fairly and lawfully obtained and processed;
- (2) be processed for specified purposes and not in any manner incompatible with those purposes;
- (3) be adequate, relevant and not excessive;
- (4) be accurate;
- (5) not be kept for longer than is necessary;
- (6) be processed in accordance with individuals' rights;
- (7) be secure;
- (8) not be transferred to non-European Economic Area countries without adequate protection.

### 2.2 The Human Rights Act 1998 (HRA)

2.2.1 The HRA gives effect to the rights and freedoms guaranteed under the European Convention on Human Rights. **Article 8** of the Convention is relevant in the context of covert surveillance, in that everyone has the right to respect for his/her private and family life, home and correspondence. Private and family life must be given a wide interpretation and it may include something as simple as gaining information about a person's associates or contacts. **Article 6** of the Convention is relevant in the context of covert surveillance in that everyone has the right to a fair trial, including internal procedures or hearings, and fairness extends to the way in which evidence is obtained.

2.2.2 There should be no interference with the exercise of these rights by any public authority, including a local authority, except where such interference is

in accordance with the law and is necessary. Local Authorities can only do this if the basis is to detect or prevent crime or disorder.

2.2.3 Non-compliance with HRA: Although it is not a criminal offence to act unlawfully, the consequences of such action are that any notices, convictions, ASBOs etc. may not be valid and the victim could take civil action against the Authority.

### 2.3 **The Regulation of Investigatory Powers Act 2000 (RIPA)**

2.3.1 This Act and its associated regulations/ Codes tries to strike a balance between community responsibilities (including effective law enforcement), and individual rights and freedoms.

2.3.2 The use of DS or a CHIS is likely to result in obtaining private information about a person, but is permitted by RIPA and its associated regulations if such surveillance has been authorised in the manner provided by the Act, the Home Office Codes of Practice and the prescribed standard forms used.

2.3.3 Home Office guidance suggests that the use of equipment such as binoculars or cameras, to reinforce normal sensory perception by enforcement Officers as part of *general* observation does not need to be regulated by RIPA, as long as the *systematic* surveillance of an individual is not involved. Information gathered in such a way by, for example, Planning Officers, Parking Attendants, Licensing Officers and Environmental Health Officers would normally fall outside the provisions of the Act. Once surveillance becomes systematic as a means of gathering information, for example, by being carried out over a lengthy period of time or on a regular basis, it will be regarded as DS and RIPA will apply. However, it is worth noting that recent OSC Guidance <sup>(1 above)</sup>, indicates<sup>2</sup> that use of binoculars and cameras in relation to residential premises can be intrusive even if use is only “fleeting”, if the information quality is the same as is obtained if present on the premises or in the vehicle. Care therefore needs to be taken.

## 3.0 **POLICY and GUIDANCE**

### 3.1 **All Forms of Covert Surveillance**

#### **General**

3.1.1 The Council will conduct its covert surveillance operations within the DPA's eight principles and restrict those operations to situations falling within the permitted exceptions of the HRA and RIPA. Additionally, the Council can only carry out surveillance for the following purpose [S.28 (3)(b) & 29(3)(b)]:-

***“for the purpose of preventing or detecting crime or of preventing disorder”;***

Previously Local Authorities were entitled to carry out covert surveillance for more extensive purposes. However, Statutory Instrument 2003/3171 restricted the Council's powers, and the Council **cannot** give authorisation under RIPA for anything other than the above. Covert surveillance will only be used for this ground, when sufficient evidence exists and has been documented to warrant the exercise. Furthermore, surveillance must be the least harmful means of meeting that purpose and be **proportionate** to what it seeks to achieve [S.28(2). See below and Glossary for definition].

---

<sup>2</sup> At Paragraph 234.  
RIPA POLICY 07/07 reviewed 11/09

- 3.1.2 When undertaking an investigation, it is extremely important that all reasonable alternative methods of investigation (such as naked-eye observation, interview or changing methods of working or levels of security), are considered/ and or attempted before embarking on an application for covert surveillance.
- 3.1.3 All requests to conduct (other than under emergency provisions), extend or discontinue covert surveillance or use of a CHIS must be made in writing on the appropriate forms (see Appendices 1 to 8). All such requests must be submitted to one of the Council's AOs (for a list of AOs see Appendix 9). All requests must be considered and authorised in writing by an AO, before any covert surveillance operation commences. Authorisation will only be granted where covert surveillance or use of a CHIS is believed is necessary and proportionate. The power to grant, extend and discontinue authorisations will be limited to these Officers, in order to ensure greater independence and consistency.
- 3.1.4 When deciding whether authorisation for DS or a CHIS is required, Officers should consider the points contained within this Policy and any Guidance given here/ Codes of Practice or in the Appendices 1-8.
- 3.1.5 Written authorisations for a DS operation will be valid for **3 months** and for a CHIS **12 months**, both from the date of the original authorisation or extension.
- 3.1.6 The Council's requirements for covert surveillance should normally be carefully planned so that the necessary consultations regarding risk assessment, insurance and health and safety can be carried out and the required provisions put in place before surveillance commences. On rare occasions, covert surveillance may need to be carried out in an emergency, and authorisation will still be required (unless this is an immediate response to events- see below). In an extreme situation, where it is not possible for the requesting Officer to complete the form, the AO must still be consulted. The Home Office's Code of Practice on Covert Surveillance makes provision for emergency oral authorisation to be granted for a maximum of 72 hours; however, as soon as possible following the oral Authorisation, the written application for Authorisation must be completed.
- 3.1.7 Surveillance that is unforeseen and undertaken as **an immediate response** to a situation normally falls outside the definition of DS and therefore authorisation is not required. If later, however, a specific investigation or operation follows an unforeseen response, authorisation must be obtained in the usual way before it can commence. Under no circumstance will any covert surveillance operation be given backdated authorisation after it has commenced. Embarking upon covert surveillance or the use of a CHIS without authorisation or conducting covert surveillance outside the scope of the authorisation will not only mean that the 'protective umbrella' of RIPA is unavailable, and could cause problems detailed in 1.5 above.

#### **Surveillance equipment**

- 3.1.8 In the main this is a reference to CCTV, and the Council CCTV system is currently facilitated through Cambridge City Council. All applications and processes are therefore dealt with in accordance with Appendix 10 and the Cambridge CCTV Code (Appendix 12). It is possible for the stationary equipment to be used in operations, but only in accordance with the application process set out in this Policy and those of the City Council. Surveillance equipment will only be used in Council led operation or installed with the necessary authorisation of the Council's AOs. It will only be installed in occupied residential premises if a member of the public has requested help or referred a complaint to the Council and such matter can only be

investigated with the aid of covert surveillance techniques after all the issues referred to above have been considered. Any permission to locate surveillance equipment on residential premises must be obtained in writing from the householder or tenant.. Requests from other agencies, such as the Police for CCTV information or surveillance will be processed in accordance with the City Policy and City Code mentioned previously.

- 3.1.9 Applicant's who intend to apply for a camera to be located as part of the DS, must submit the request in accordance with the procedure set out in Cambridge City Council CCTV service document (Appendix 10). A copy of the Authorisation should be forwarded to the Cambridge City CCTV Manager, as per their Policy and the request/ and information handled in accordance with Cambridge City CCTV Code of Practice (June 2009 – Appendix 12). DVD and CD ROMs will be used and their quality checked monthly. A register will be kept to monitor retention periods (28 days).

#### **“Low-level” Surveillance**

- 3.1.10 In accordance with the Home Office Code of Conduct, certain levels of surveillance amounting to general observations in the course of law enforcement can be regarded as “low level” surveillance and are consequently outside the RIPA provisions. An example of low-level surveillance is where an Enforcement Officer merely drives past a site to check whether or not restrictions are being adhered to. However, should Officers revisit the site this may be regarded as systematic and RIPA authority may be required. If in any doubt as to whether or not surveillance falls within the “low level” category, Officers should seek further advice from Legal & Democratic Services.

#### **Overt Surveillance**

- 3.1.11 Overt surveillance does not require any RIPA authorisation. Consequently if verbal notification or a letter is sent to the subject of the surveillance notifying them of the kind of surveillance that is proposed (what equipment will be used and when), then RIPA authorisation is not required; for example in noise nuisance cases, the letter warning the alleged perpetrator, should set out the nature of the complaint and what equipment will be used to monitor this (and when it is likely to be installed)<sup>3</sup>. If a letter is used it is important to ensure that it is sent by Registered Post (or hand-delivered). All such letters and verbal communications should only last for 3 months.

#### **Authorisations and Central file**

- 3.1.12 All AOs will be responsible for ensuring that copies of all Applications, Reviews, Renewals and Cancellations are sent to Legal & Democratic Services, within 5 days of completion and will be retained in the Council's Central file. These will then be checked / signed and date received marked on the top of the form. Relevant information will be entered onto the Central file, which is kept by Legal Services. Applicants/ AOs should also have a way of auditing the requests they receive, retaining copies and diarising relevant dates for Reviews/ Renewals or Cancellation.

- 3.1.13 During a covert operation, recorded material or information collected will be stored and transported securely. The AO concerned will review it regularly, and access will be restricted to the Applicant Officer, the AO concerned and the Monitoring Officer (or other relevant Legal Officers from Legal & Democratic Services). The AO will decide whether to allow requests for access by third parties including Council Officers. Access will generally only

---

<sup>3</sup> OSC Guidance\* has suggested that Planning and Noise Nuisance covert surveillance cannot be authorised as no crime has been committed (until statutory notice has been breached). This does not mean that covert surveillance cannot be done, just that it cannot be given protection through the RIPA application process [Para 102]. In any event if monitoring is undertaken, consideration needs to be given to whether the equipment is capable of measuring volume only or whether it can identify the perpetrators – because if so, this would be intrusive and therefore unlawful surveillance [para 278]

be allowed to limited and prescribed parties including law enforcement agencies, prosecution agencies, legal representatives and the people subject to the surveillance (unless disclosure would prejudice any criminal enquiries or proceedings- see 8 below for further guidance).

- 3.1.14 Once a covert operation results in an individual being under suspicion of having committed a criminal or disciplinary offence, he/she must be informed of this as promptly as is reasonably practicable in order to ensure his/her right to a fair trial or hearing within a reasonable time in accordance with the HRA. In a situation where it is considered that a matter gives rise to a potential criminal prosecution, any interview with the suspect must be under caution and conducted by a suitably trained Officer.

#### **COVERT HUMAN INTELLIGENCE SOURCES (CHIS)<sup>4</sup>**

- 3.1.15 A "Covert Human Intelligence Source" (CHIS) is defined as:  
a person who establishes or maintains a personal or other relationship with another person for the covert purpose of:

- using such relationship to obtain information or to provide access to any information to another person or
- covertly disclosing information obtained by the use of such a relationship or as a result of the existence of such a relationship where the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of its purpose or (in the case of disclosure of information) it is disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the disclosure in question.

- 3.1.16 This would not generally apply to members of the public who volunteer information / or phone contact numbers. If, however, an Officer believes that given the nature of an investigation/ officers or public used would fall into this category (and someone's Human Rights are likely to be infringed), *or that one of their own officers needs to act in this capacity (i.e. a consumer-type test purchase)* then a CHIS Authorisation must be obtained prior to use and the RIPA procedures followed. In the unlikely event that the Council decides that it will need to use a non- Officer CHIS, then consideration will have to be given *before* authorisation as to whether the CHIS would be managed by the Police. OSC guidance has indicated that this may be an effective mechanism to ensure that a local authority is fulfilling its statutory responsibilities. In such cases a written protocol should be agreed to ensure that an identified CHIS is properly managed.

- 3.1.17 There are special safeguards, which apply to the use of juvenile sources under the age of 18. There are no circumstances in which a child under the age of 16 can be authorised to give information against his or her parents' wishes. AOs should also abide by the Home Office Code of Conduct relating to Juveniles. (See S.I. 2000 No. 2793 – The Regulation of Investigatory Powers (Juveniles) Order 2000) Vulnerable individuals, such as the mentally impaired, should only be authorised as a CHIS *in the most exceptional cases* and only by the Chief Executive. A vulnerable individual is a person in need of community care services because of illness, age, mental or other disability, or is unable to take care of himself or herself, or is unable to protect himself or herself against significant exploitation or harm.

- 3.1.18 Prior to authorising a CHIS, the AO shall have regard to the safety and welfare of the CHIS and shall continue to have such a regard throughout. Where a CHIS is deployed, records shall be kept to comply with the Home

---

<sup>4</sup> Note comments at 1.10 re authorisation only after seeking advice from Legal Officers in Legal & Democratic Services

Office Code of Practice. A “Handler” (who can be an Officer of the Council) should be designated to have the day-to-day responsibility for dealing with the CHIS and his/ her security and welfare. Further, a “Controller” should be designated to have the general oversight of the use made of the CHIS. 4.33 of the CHIS Code of Practice states that a Public Authority should have proper oversight and management arrangements in place for sources. IF NONE ARE IN PLACE THEN NO AUTHORISATION SHOULD BE GRANTED.

#### **4.0 AUDIT & MONITORING**

4.1 Formal monitoring and auditing of authorisations will be carried out by the Monitoring Officer/ qualified legal staff in Legal & Democratic Services.

4.2 The role of the Monitoring Officer/ Legal & Democratic Services will be to: -

4.2.1 Maintain a Central file (containing details of Authorisations).

4.2.2 Try to ensure uniformity of practice on issuing Authorisations.

4.2.3 Check each Application, Review, Renewal and Cancellation form to ensure compliance with RIPA.

4.2.4 Provide guidance and training where appropriate.

#### **5.0 PROCEDURE FOR OBTAINING AUTHORISATION FOR DS OR USE OF A CHIS**

##### **Action to be taken by the person applying for Authorisation**

5.1 Officers are advised to discuss the need to undertake DS or the use of a CHIS with their line manager before seeking an Authorisation. As indicated, options to gain the information, which is required, other than by using covert techniques should be fully explored. Where Officers are seeking to use a CHIS, then Legal advice should be obtained *before* authorisation.

5.2 The forms for applying for a DS or CHIS Authorisation can be found at Appendices 1 & 5. The forms are available to complete on screen, and contain relevant commentary guidance boxes. Regard should be given to the guidance below when completing the relevant sections of the forms. If the situation is urgent, verbal authorisation should be obtained from the appropriate AO, and as indicated above, the application then completed (including the parts that deal with the reason/s why the situation was considered urgent).

5.3 Following completion of Parts 1 to 12 the applying Officer should obtain a unique reference number (to enter on the top right hand side of the form), from Legal & Democratic Services (616372). The following information should also be provided to Legal Services:

- Name of Applicant.
- Applicants department.
- Type of Application (DS or CHIS).
- Details of the Target of the Surveillance. (N.B. If an employee of the Council it is permissible for the full name to be withheld).
- Whether confidential information is likely to be obtained.
- Whether ‘urgent provisions’ are or have been used.

The completed form should then be passed to the AO (see Appendix 9).

##### **AOs**

5.4 The Regulation of Investigatory Powers Directed Surveillance and Covert Human Intelligence Order 2003 prescribes that, in a Local Authority setting, the AO shall be an Assistant Chief Officer, Assistant Head of Service, Service

Manager or equivalent. There is no provision for Officers of a lower rank to grant Authorisation, even in cases of urgency.

- 5.5 Authorisation by a designated AO gives lawful authority to surveillance or use of a CHIS. The Authorisation must be given in writing by the AO, except in urgent cases, when Authorisation may be given verbally, although in such instances the procedural difference and duration of verbal Authorisations, as outlined below, should be noted. It is crucial for AOs to address why they consider the Authorisation to be necessary and proportionate, the risk of collateral intrusion and likelihood of acquiring confidential material (see below paragraph 6).

## 6.0 DOCUMENTATION & GUIDANCE ON COMPLETING THE FORMS

- 6.1 The appropriate documentation is detailed at Appendices 1-8. Copies documentation must be held in the Central file. This file will be held for a minimum of 5 years for audit purposes.

### The DS Application form

#### 6.2 Introduction

This section should include the details of the Authority/ Officer who is requesting the Authorisation and Investigation/Operation Name to which the investigation relates. The Operation Reference Number should be the RIPA central file number (URN) given to you by Legal & Democratic Services as detailed above.

**Section 1** - specify the name and precise position of the AO e.g. *Head of Environmental Services & Housing*.

**Section 2** – Set out the purpose of the operation and investigation, so that necessity and proportionality can be considered in that context.<sup>5</sup>

**Section 3** –. A brief description of the activity to be undertaken should be given together with an outline of the purpose of the investigation – specifically what equipment will be used/ length of time this will be used/ number of officers involved.

**Section 4** – Details of the subject or target of the DS should be specified. It might be necessary to state that the identity of the subject is unknown.

**Section 5** – Set out the information you hope to obtain from the surveillance. For example, this may be evidence that a person may be resident at an address when they stipulate that they are not; evidence that the target is causing a nuisance; to identify the person responsible for fly tipping; to identify the person slashing rubbish bags left out for refuse collection. You should NOT write “*to prove Mr X is guilty*”.

---

<sup>5</sup>OSC Guidance\* Para 103-104

Proportionality is a key concept of RIPA and RIP(S)A. It is often poorly articulated. An authorisation should demonstrate how an Authorising Officer has reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the proverbial 'sledgehammer to crack a nut'). Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, technique or tactic is the least intrusive. It is insufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available. It is equally unacceptable to consider lack of resources or a potential cost saving as sufficient ground to use technological solutions which are often capable of being more intrusive than a human being. This critical judgement can only properly be reached once all other aspects of an authorisation have been fully considered.

**Section 6** – One ground of necessity for authorisation purposes i.e. for the purpose of preventing or detecting crime or of preventing disorder.

**Section 7** - This section is very important. YOU MUST set out why in the particular circumstances of the case it is NECESSARY. Consider whether all other reasonable lines of enquiry have been attempted or if not attempted, considered and discounted. Simply put - can the information be obtained by other means? If Yes then unlikely to be necessary.

**Section 8** – Details of any potential **collateral intrusion** should be specified. e.g. details of any personal information that might be collected about parties who are not the subject of the investigation. A plan should be specified as to how the potential for collateral intrusion will be minimised. e.g. by focusing surveillance on a limited area. Applicants should give as much detail as possible in this section as AOs should pay particular regard to the information that is given. AO's should not authorise Applications that either do not state whether collateral intrusion is likely or that do not specify what steps are to be taken to minimise it.

**Section 9** – Proportionality<sup>6</sup> is very important. This involves balancing the intrusiveness of the activity on the target and others who might be affected, by the need for surveillance. The activity will NOT be proportionate if it is excess in the circumstances of the case – or the information could be obtained by other means. Put simply: is this the least intrusive method of obtaining the evidence? If NO then it is not likely to be proportionate.

**Section 10** – This section requires an indication of the likelihood of obtaining confidential and religious information and material, including: matters subject to legal privilege; confidential personal information; and confidential journalistic information (**See Glossary for definitions**). Such material is regarded as particularly sensitive and the likelihood of obtaining such information should be fully considered in terms of the proportionality issues, which it raises. Special care should be taken when handling, retaining, copying or disseminating such information.

**An Authorisation, which may involve the acquisition of confidential material, may only be granted by the Chief Executive.**

**Section 11** – Self explanatory.

**Section 12** – The AO must deal with the 5 “Ws” and “How” in statement form i.e. who, what, where, when and HOW.

---

<sup>6</sup> OSC Guidance Para 104

A potential model answer would make clear that the four elements of proportionality had been fully considered:

- 104.1 balancing the size and scope of the operation against the gravity and extent of the perceived mischief,
- 104.2 explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others,
- 104.3 that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result, and
- 104.4 **evidencing what other methods had been considered and why they were not implemented.**

**Section 13** - that the application is necessary and proportionate. The terms of necessity and proportionality relate to Human Rights of the target and other persons; it is essential that these matters are adequately covered in the sections above.

**2.4 & 2.5 of the Code of Practice [Necessity and Proportionality] states:**

*2.4 Obtaining an authorisation under the 2000 Act, the 1997 Act and 1994 Act will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place. The 2000 Act first requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds in section 28 (3) of the 2000 Act for directed surveillance and in section 32 (3) of the 2000 Act for intrusive surveillance.*

*2.5 Then, if the activities are necessary, the person granting the authorisation must believe that they are proportionate to what they seek to achieve by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.*

**Section 14** – Confidential information: If Authorising Confidential information the Chief Executive will need to complete to show compliance with 3.1-3.12 of the Code of Practice (click on to the link above at 1.6 for DS).

**The first review date should be inserted and diarised.** This will generally be one calendar month from the date of Authorisation. Full name/ position of AO should be inserted and remember to sign, insert date and time of signature!

**Sections 15 – 16** – only need to be completed if this is an urgent authorisation; therefore if not applicable, cross through the remaining part of the document.

#### **Application for CHIS**

6.4. **Introduction** – You need to set out source referral information (where relevant); “Handler”, “Controller Information”, and set out who will hold the source information. If a CHIS is to be sought for a third party source the Investigating Officer must have regard to the provision of section 29(5) RIPA, paragraph 2.14 of the Code of Practice and Statutory Instrument 2000 No 2725. In particular the investigating Officer must ensure that a senior manager in his / her section is tasked with the oversight of the use of CHIS and who shall maintain the records specified in Paragraph 3 of the Statutory Instrument.

The Monitoring Officer will retain the source information under secure conditions. The Applicant will need to complete Appendix 11 and hand-deliver this to Legal & Democratic Services.

**Sections 1 & 2** – see DS application above.

**Sections 3 & 4** – these are reasonably self-evident; you must set out purpose of the CHIS and then how the source will be used in the operation.

**Section 5** – the same as DS section 6 above.

**Section 6** - This section is very important. YOU MUST set out why in the particular circumstances of the case it is NECESSARY. Consider whether all other reasonable lines of enquiry have been attempted or if not attempted, considered and discounted? Simply put - can the information be obtained by other means? If Yes then unlikely to be necessary. State if you cannot obtain by any other means.

**Section 7** - The risk of collateral intrusion must be taken into account before authorising, and measures taken to avoid unnecessary intrusion. These measures / "precautions" should be set out in this section; for example: *"contact will be limited to the target; CHIS discouraged from engaging in contact that will result in third party private information being obtained, source will have contact with Handler X times per week, and source will report any infringement to Handler as soon as practical"* etc. If infringement occurs after the Authorisation, then those tasking the operation MUST inform the AO (AO) – and the AO MUST consider if the original authorisation needs to be amended or a new one issued.

**Section 8** - As part of any risk assessment of the operation, you must consider whether tasking the source to act in a particular way would adversely impact on community confidence or safety. If a conflict is anticipated then seek Legal advice *before* proceeding with the operation.

**Section 9** - Section 29(5)(a) and (b) of RIPA requires Public Authorities to have in place proper oversight and management arrangements for sources. By and large the Council does not use third party sources. However, the Council must still have regard for the health and safety of Officers who act under a CHIS authorisation. The Council must carry out a risk assessment of likely risks to be faced by an Officer during the conduct of the investigation (and after the Cancellation of the Authorisation). Normal departmental risk assessment methods should be utilised and details of the assessment should be recorded on the form.

**Section 10** - Proportionality is a very important consideration. This involves balancing the intrusiveness of the activity on the target and others who might be affected, by the need for the operation. The activity will NOT be proportionate if it is excess in the circumstances of the case – or the information could be obtained by other means. The source must be managed to meet this objective, and should not be used in an arbitrary or unfair way. Put simply: "Is this the least intrusive method of obtaining the evidence? If NO then it is not likely to be proportionate.

**Section 11** - Confidential information includes religious material, material subject to legal privilege, confidential and personal information not connected to your investigation, and confidential journalistic information. If there is a likelihood that you may obtain confidential information the only person who can grant this is the Chief Executive.

**Section 12** – Self explanatory.

**Section 13** - The AO must deal with the 5 "Ws" and "How" in statement form i.e. who, what, where, when and HOW.

**Section 14** – see DS section 13 above.

**Section 15** – see DS section 14 above.

**Section 16 & 17** – you should set down the next review date, which should be one calendar month *or sooner in appropriate circumstances*. Further

review dates may be arranged, but if not, they must be considered when the CHIS is reviewed.

**Section 18** – time and date of signature and when Authorisations end (can be granted for up to 12 months). It can only be renewed at that time if a review has been carried out and the results considered *before* renewing.

Both forms contain a section for use in instances where verbal Authorisation has been given in urgent situations. Details of why the application was considered urgent should be provided.

The form should be considered by the AO who should complete the remaining parts of the form. In cases where approval can only be given by the Chief Executive, the application should be sent to the first level AO for initial consideration, who would then submit the form to the higher level.

**Action to be taken by the AO when completing their parts of the forms**

- 6.5 The AO must firstly consider whether the DS should be undertaken or a CHIS used. Secondly, whether the risk of interfering with a person's private and family life, whether or not the person is the target (i.e. collateral intrusion) of the surveillance, is proportionate to the objective that is to be achieved.
- 6.6 The question of proportionality (see footnotes above) and the risk of collateral intrusion are important considerations for the AO to deal with. If the form does not contain sufficient information to enable an AO to consider both of these matters fully further details should be sought.
- 6.7 Particular consideration should be given to circumstances where confidential or religious material may be obtained. As indicated, if there is a real risk of this then only the Chief Executive can grant.
- 6.8 The AO must complete relevant sections of the Application forms and make a decision as to whether to approve or refuse the application.
- 6.9 Both forms require the AO to specify a date when the Authorisation should be reviewed and the frequency of review thereafter. This should normally be one calendar month after the Authorisation is granted, or sooner if there is a risk of obtaining confidential information. A Review form has to be completed (see Appendix 2 & 6) to record any review that takes place.
- 6.10 A copy of the completed authorisation form, whether approved or refused, should be sent to Legal & Democratic Services within 5 days. The original should be retained by the Applicant on the investigation file.

**7. DURATION OF AUTHORISATIONS. DETAILS ON REVIEWS, RENEWALS AND CANCELLATIONS**

**Authorisations**

- 7.1 DS Authorisations will cease to have effect three months from the date of approval and CHIS authorisations, twelve months from the date approval.
- 7.2 Urgent verbal authorisations will cease to have effect after 72 hours, beginning with the time when the authorisation was granted, unless subsequently endorsed by written authorisation.
- 7.3 It will be the responsibility of the Officer in charge of an investigation to ensure that any DS or use of a CHIS is only undertaken under an appropriate and valid authorisation, and therefore, he/she should be mindful of the date when authorisations and renewals will cease to have effect. Legal Services

shall perform an auditing role in this respect **but the primary responsibility rests with the Officer in charge.**

### **Reviews**

- 7.4 All authorisations should be reviewed once a month whilst they are 'live'. Forms for Reviews are at Appendices 2 and 6 for Directed Surveillance and CHIS respectively.

### **Renewals**

- 7.5 An AO may renew an Authorisation before it would cease to have effect if it is necessary for the Authorisation to continue for the purpose for which it was given. Such renewals would normally extend the authorisation period for a further three months beginning with the day on which initial authorisation would cease to have effect, but for the renewal. Authorisation may be granted more than once, provided they continue to meet the criteria for authorisation. Ideally, an application for renewal must not be made more than seven days before the authorisation is due to expire.
- 7.6 The Officer requesting the Renewal should complete Parts 1 to 7 of the application to Renewal a DS or CHIS Authorisation form (to Part 9 for the latter; Appendix 3 or 7 respectively) and submit this to the AO for consideration and completion of Parts 8/10-11. The AO must consider the application for Renewal in relation to the original purpose for which Authorisation was granted, taking into account any change in circumstances.
- 7.7 If the reason for requiring the Authorisation has changed from the purpose for which it was originally granted, then this should be cancelled and new authorisation sought.

### **Cancellations**

- 7.9 It is essential that the Authorisation is cancelled when the exercise is completed and the Authorisation is not merely left to 'run its course' until the time limit expires. The responsibility to ensure that Authorisations are cancelled rests with the Officer in charge.
- 7.10 To cancel, the person in charge of the investigation should complete parts 1 and 2 of the Cancellation of Authorisation form (Appendices 4 And 8). The form should be submitted to the AO for endorsement and completion of Parts 3 and 4.
- 7.11 In all cases, as indicated, a copy of the completed forms must be sent to Legal & Democratic Services. The original should be retained by the AO and a further copy sent to the Applicant for the investigation file.

## **8. HANDLING MATERIAL OBTAINED FROM DCS AND CHIS OPERATIONS**

- 8.1 Material, or product, such as: written records (including notebook records); DVDs and tape; photographs and negatives; and electronic files, obtained under Authorisation, should be handled, stored and disseminated according to the following guidance.
- 8.2 Where material is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should **not** be destroyed, but retained in accordance with the established disclosure requirements having regard to the Criminal Procedure and Investigations Act 1996 and Civil Procedure Rules (or in any event retained for 5 years).

- 8.3 Where material is obtained, which is not related to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to suspect that it will be relevant to any future civil or criminal proceedings, it should be destroyed immediately.
- 8.4 Material may be used in investigations other than the one that the Authorisation was issued for. However, use of such material outside the Local Authority, or the Courts, should only be considered in exceptional circumstances, and under advice from Legal & Democratic Services.
- 8.5 Where material obtained is of a confidential nature then the following additional precautions should be taken:
- Confidential material should not be retained or copied unless it is necessary for a specified purpose.
  - Confidential material should only be disseminated, on legal advice, that it is necessary to do so for a specific purpose.
  - Confidential material, which is retained, should be marked with a warning of its confidential nature. Safeguards should be put in place to ensure that such material does not come into the possession of any person, which might prejudice any civil or criminal proceedings.
  - Confidential material should be destroyed as soon possible, after its use for a specified purpose.
- 8.6 If in doubt about what constitutes confidential material and the handling etc of such material then advice should be sought from the appropriate RIPA Codes of Practice or from Legal & Democratic Services.

## **9.0 TELECOMMUNICATIONS DATA, RECORDING OF TELEPHONE CONVERSATIONS ETC**

### **Access to telecommunications data**

- 9.1 This Policy does not cover the use of communications data in any depth. However, by way of information, the RIPA (Communications Data) Order 2003 came into force on the 5 January 2004 and allows the Council to acquire information defined as **communications data**. This includes subscriber details and **service data** but not the **traffic data** (latter two terms see Glossary).
- 9.2 The Legislation, however, requires the Council to have a Home Office accredited Single Point of Contact (S.P.o.C) in place. Appropriate authorisation must be channelled through the S.P.o.C to carry out a quality control role and advise the Investigating Officer and the AO whether the application meets the statutory requirements, whether the information being sought can be easily obtained by the Communications Service Providers (CSP) or Internet Service Providers (ISP) and whether the application would be cost effective. The S.P.o.C will also be the contact Officer for all liaisons with CSPs and ISPs. Whilst the Council has an accredited SPo.C (Jeanette Thompson – Monitoring Officer), other systems would have to be put in place to deal with the relevant applications/ and ultimately authorised by a Designated Person. Further information and guidance on this area can be obtained from the Monitoring Officer.

### **Recording of telephone conversations**

- 9.3 The recording of telephone calls between two parties when neither party is aware of the recording **cannot be undertaken**, except under a Warrant granted under Part 1 of RIPA. Such warrants are only granted by the Secretary of State and it is not envisaged that such activity would fall within the remit of local authority investigations.

- 9.4 However, there may be situations where either the caller or receiver consents to the recording of the telephone conversation and, in such circumstances a Part 1 warrant is not required.

#### **Interception of telecommunications**

- 9.5 Part 1 of RIPA does not, however, prevent Local Authorities from lawfully intercepting its employees' e-mail or telephone communications and monitor their internet access for the purposes of prevention or detection of crime or the detection of unauthorised use of these systems (which is covered under Part 1 the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 - *SI 2000/2699*. Further advice on these Regulations should be sought from the Legal & Democratic Services.

### **10.0 FURTHER INFORMATION**

Any enquiries about this policy or queries about RIPA in general should be referred to Legal & Democratic Services.

- 10.1 Further information is set out in the Home Office Codes of Practice, which can be accessed through the direct link above or further guidance from the Home Office webpage at: <http://security.homeoffice.gov.uk/ripa/about-ripa/news/new-website>

- 10.2 All other forms/ guidance are contained with the Appendices.

### **11. GLOSSARY OF TERMS**

**Collateral Intrusion:** Includes situations where there is a risk of the surveillance resulting in private information being obtained about persons other than the subject of the surveillance.

**Communications Data** Is defined in section 21(4) of RIPA. It covers Traffic Data, Service data and Customer Data.

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

**Confidential Material** Includes:

- matters subject to legal privilege;
- confidential personal information; or
- confidential journalistic material.

**Confidential Personal Information** Includes information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:

- to his/her physical or mental health or
- to spiritual counselling or other assistance given or to be given and

- which a person has acquired or created in the course of any trade, profession or other occupation or for the purposes of any paid or unpaid office.

It includes both oral and written information and also communications as a result of which personal information is acquired or created.

Information is held in confidence if:

- it is held subject to an express or implied undertaking to hold it in confidence or
- it is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.

**Covert or Directed Surveillance (DS)**

Means surveillance, which is, carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

**Covert Relationships (CHIS)**

Means a relationship conducted in a manner calculated to ensure that one or more of the parties to the relationship is unaware of its purpose.

**Immediate Response**

Includes a response to circumstances or events, which, by their very nature, could not have been foreseen.

**Matters Subject to Legal Privilege**

Includes both oral and written communications between a professional legal adviser and his/her client or any person representing his/her client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege.

**Necessity**

Refers to the need for surveillance (or use of CHIS). Other options of gathering the evidence etc should be considered before undertaking surveillance.

**Person**

Includes any organisation and any association or combination of persons.

**Private Information**

Includes any information relating to a **person's** private or family life. Private life also includes activities of a professional or business nature (Amann v Switzerland (2000) 30 ECHR 843).

**Private Vehicle**

Means any **vehicle** which is used primarily for private purposes of the person who owns it or otherwise has a right to use it, but would not include any person whose right to use the

vehicle arises from making payment for a particular journey. **Vehicle** also includes any vessel aircraft or hovercraft.

### **Proportionate**

**Very important.** Must be considered separately from **Necessity**. Ask yourself the following question “Is there any less invasive way of finding out the information?”. If the answer is no then you know that it is proportionate to carry out the surveillance. In other words proportionality is the least intrusive way to achieve the objective.

### **Residential Premises**

Means any **premises** occupied by any person, however temporarily, for residential purposes or otherwise as living accommodation (including hotel or prison accommodation), but does not include common areas to such premises.

**Premises** also includes any vehicle or moveable structure used within the definition above.

### **Service data**

This relates to the use of the Service Provider’s services by customers, and includes:-

The periods during which the customer used the service(s)

Information about the provision and use of forwarding and re-direction services by postal and telecommunications service providers

‘Activity’, including itemised records of telephone calls (numbers calls) internet connections, dates and times/duration of calls, text messages sent

Information about the connection, disconnection and reconnection of services

Information about the provisions of conference calling, call messaging, call waiting and call barring telecommunications services

Records of postal items such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection

Top up details for pre-pay mobile phones – credit/debit card voucher /e-top up details

### **Surveillance**

Includes:

- monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications;

- recording anything monitored, observed or listened to in the course of surveillance;
- surveillance by or with the assistance of a surveillance device; and
- the interception of a communication in the course of its transmission by means of a postal service or telecommunication system if it is one sent by, or intended for, a person who has consented to the interception of the communication.

But does not include:

- the conduct of a covert human intelligence source in obtaining or recording (whether or not using a surveillance device) any information which is disclosed in the presence of the source;
- general targeting of a problem area, or covert observation of a premises which does not involve systematic surveillance of an individual, even where such observation may involve the use of equipment which reinforces normal sensory perception, such as binoculars or cameras.

The general use of CCTV systems, because the public are aware of their use, i.e. they are overt. If a CCTV camera were targeted to observe a specific individual then this would fall under RIPA and would need an authorisation.

### **Surveillance Device**

Means any apparatus designed or adapted for use in surveillance.

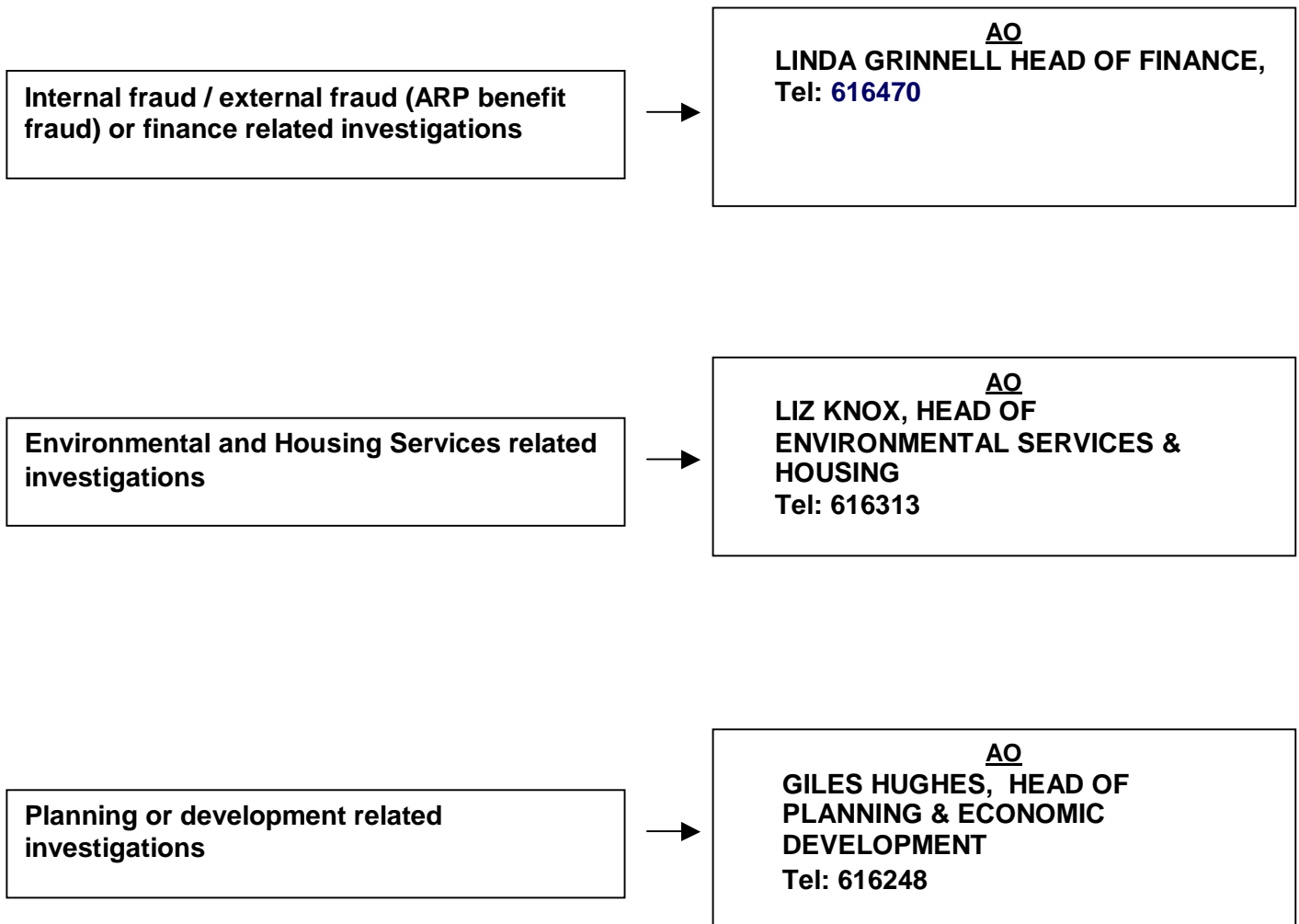
### **Traffic data**

(RIPA s21 (4) (b) ). This is data about communications. It relates to data generated or acquired by the Service Provider (**SP**) in delivering / fulfilling services to its customers. Local Authorities are not entitled to access this information. The information includes:

- Information identifying the sender and recipient (including copy recipients) of a communication.
- Routing information identifying or selecting any apparatus, such as equipment, machinery or device, or any wire or cable) through which a communication is transmitted e.g. dynamic IP address allocation, web postings and email headers (to the extent that the content of the communication is not disclosed-the subject line of an email is considered content).
- Information identifying any location of a communication, such as mobile phone cell site location.

- Call detail records for specific phone calls i.e. Call Line Identity (CLI).
- Web browsing information (to the extent that only the host machine or domain name (website name) is disclosed.
- Information written on the outside of a postal item.
- Online tracking of communications (including postal items).

**ECDC List of Authorised Officers- RIPA applications**



Generally Applicant Officers will apply for RIPA authorisations to the relevant AO that covers their service area. However, each of the above AO's can authorise Applications, Renewals, and undertake Reviews and Cancellations for any other ECDC service area investigation, if the Service area AO is unable to do so.

## LEGISLATION

- 15.1 There have been a number of Acts passed by Parliament, which will affect the way that CCTV systems are operated. In particular the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 and the Freedom of Information act 2000 and Acts relevant to other agencies.
- 15.1.1 Section 15 of this manual lays down Cambridge City Council's CCTV system's approach to complying with these Acts. Whilst at the same time recognizing that, as these Acts develop, so will this section of the manual.
- 15.1.2 Cambridge City Council will not monitor any external CCTV cameras unless the owners of those cameras agree to abide by the rules laid out in the Council's Codes of Practice and this Operational Manual.
- 15.1.3 The key objectives of Cambridge City Council's CCTV system are to:
- Protect areas and premises used by the public.
  - Deter and detect crime.
  - Help to identify offenders, leading to their arrest and prosecution.
  - Reduce anti-social behavior and aggressive begging.
  - Reduce fear of crime.
  - Encourage better use of city facilities and attractions.
  - Maintain and enhance the commercial viability of the city and encourage continued investment.
- 15.2 The Data Protection Act 1998 (DPA)**
- 15.2.1 The Data Protection Act 1998 came into force on 1<sup>st</sup> March 2000. The Act relates to data processing of all types. Under the Act, data is defined as 'information', which is being processed by equipment operating automatically in response to instructions; or is recorded with the intention that it should be processed'.
- 15.2.2 Cambridge City Council's CCTV system falls into the second definition, in that we record images for release to enforcement agencies for processing, and has therefore been registered with the Information Commissioner.
- 15.2.3 Cambridge City Council's CCTV arc of observation is clearly marked with signs that inform people that they are within an area observed by CCTV cameras. The signs show the recognized CCTV symbol, have a contact telephone number and indicate that Cambridge City Council operates the system. No 'covert' cameras are used by the Cambridge City Council CCTV system.
- 15.2.4 The Information Commissioner has set out eight principles to ensure that CCTV systems meet the requirements of the DPA. These are:

- All personal data will be obtained and processed fairly and lawfully.
- Personal data will be held only for the purposes specified.
- Personal data will be used only for the purposes, and disclosed only to the people, shown within the Council's Code of Practice and Operational Manual.
- Only personal data will be held which are adequate, relevant and not excessive in relation to which the data is held.
- Steps will be taken to ensure that personal data are accurate and where necessary, kept up to date.
- Personal data will be held for no longer than is necessary.
- Individuals will be allowed access to the information held about them and, where appropriate, permitted to correct or erase it.
- Procedures will be implemented to put in place security measures to prevent unauthorized or accidental access to, alteration, disclosure, or loss and destruction of, information.

15.2.5 All Cambridge City Council staff who have access to the CCTV system have signed a confidentiality agreement and have been fully trained in their responsibilities with regard to the recording, control, security and issuing of data produced within the CCTV Control Room and their responsibilities and tasks are covered in detail in the sections of the this manual.

15.2.6 To ensure compliance with the Data Protection Act, Cambridge City Council's CCTV system will ensure that the following rules are maintained:

- All recorded images will be of good quality and factually correct
- Only DVD-R or CD-R's will be used. All discs will be marked with a unique serial number.
- Only authorised personnel will be permitted to view images within the CCTV Control Center.
- Only CCTV personnel and the Police Liaison Officer will be permitted to operate the equipment within the CCTV Control Center.
- Browsing of tapes for potential incidents will not be permitted.
- The investigating officer will be required to sign a release certificate for any images removed from the Control Center so that a clear audit trail of evidence is maintained.
- The 'master disc' containing the original copy of the evidence will be sealed and secured in the evidence locker.
- All images recorded within the Control Center not required for investigation of, or prosecution of an offence, will be destroyed after 28 days.
- Images may be retained longer than 28 days but only at the request of an enforcement agency to continue an inquiry or for a prosecution.

- Any investigating officer who signs out a copy disc or still image will receive a chaser letter at regular intervals requesting the image's return.
- All discs will be kept secured at all times.
- The duty Operator will be responsible for the security of the images held within the Control Center.
- The location of all discs must be known at all times.
- All discs will be destroyed within the CCTV Control Center at the end of their working life.
- Recording quality will be audited monthly.
- All images recorded by the CCTV cameras will have the date, time and the location of the camera providing the images clearly superimposed on them.
- All equipment within the Control Center including cameras, DVR recorders and time generators will be checked daily and faults reported and repaired as quickly as possible.
- CCTV Operators will not view private areas except under the conditions laid down in paragraph 4.3 in section 4 of this Operational Manual.
- Operators will only monitor individuals whom they believe have committed or are about to commit an offence.
- Operators will not use the cameras to follow individuals because of their sex, colour, race, dress or appearance. Nor will they stereotype members of the public.
- No images of any kind produced by Cambridge City Council's CCTV Control Center will be released for commercial or entertainment purposes.
- No recordings or still images will be produced for any other purpose than the achievement of the aims and objectives set out in paragraph 15.1.3 above.

15.2.7 A person may request a viewing of images they believe the CCTV Control Room has of them or a copy of the images by contacting Cambridge City Council's Information Management Officer on 01223-457000. They will then be supplied with a Data Access Request Form, which must be filled in, in all parts, and returned to the Information Management Officer.

15.2.8 The CCTV Manager may not comply with the request in the following circumstances:

- If images of third parties are also in the frame and their permission for disclosure cannot be obtained.
- If the request is considered to be unreasonable or vexatious.
- If the images are in connection with evidence of an incident under investigation by an enforcement agency. The responsibility for disclosure of

that evidence rests with the enforcement agency and not with the CCTV Control Center.

15.2.10 The Information Commissionaires contact details are shown on the last page of Part II (The Code of Practice) of these manuals.

### 15.3 **The Human Rights Act 1998 (HRA)**

15.3.1 The Human Rights Act into force in 2000. The Act gives “further effect to the rights and freedoms guaranteed under the European Convention on Human Rights”.

15.3.2 The HRA does not bring any new rights or criminal offences, but the Act does bring existing rights into force as part of UK domestic law, which will enable people in the UK to have cases dealt with in UK courts rather than having to take them to Strasbourg for a ruling as was the case before this Act was passed. The Act also gives public authorities (Cambridge City Council) a legal duty to act compatibly with the Convention rights.

15.3.3 There are a total of 18 Articles in Part 1 of the HRA, some which are absolute rights as in ‘The Right to Life’ and others which are qualified rights as in Articles 8 to 11 below.

Qualified rights are rights that may be interfered with or restricted by the state if the activity threatens national security, public safety or health or to deter or detect crime etc. However these rights can only be restricted if the need for that restriction can be shown to be Proportionate, Legal, has a clear Aim and is Necessary (PLAN).

15.3.4 The CCTV Manager is responsible for ensuring that the CCTV system does not infringe individual’s rights under the HRA. He along with other Cambridge City Council Managers will be responsible for challenging any infringements it is being asked to assist in imposing by other agencies (through surveillance under RIPA, see paragraph 15.4 below), by challenging any request it receives by applying PLAN to any such restriction and obtaining satisfactory justifications to any such requests.

15.3.5 All 18 Articles in the HRA are important but the Articles, which will have a direct impact on the operation of Cambridge City Council’s CCTV system, are:

a **Article 6: RIGHT TO A FAIR TRIAL.** When producing evidence, CCTV Operators must bear in mind that the evidence being produced can be used to prove innocence as well as guilt. Although it is a Police responsibility for disclosure of evidence under the PACE Act, Operators must ensure that Police Officers or other enforcement agencies are made aware of all the cameras used whilst monitoring an incident. It is for the enforcement agencies to decide what is or is not relevant evidence and not the CCTV Operator.

The Operator must, if requested, ensure that all relevant evidence is secured in the evidence locker and that all details concerning the production of any evidence are accurately recorded.

.b. **Article 8: RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE.** It is recognized that everyone has the right to respect for their

private and family life, their home and their correspondence. Except for the prevention of disorder or crime and for the protection of the rights and freedoms of others. Cambridge City Council's CCTV system has been set up with clearly defined aims, which are shown in full on page 2 of Cambridge City Council's 'Code of Practice'. The aims of the system are also shown at paragraph 15.1.3 above.

The system clearly recognizes people's 'right to privacy' by ensuring all its Operators are properly trained, that there are clear guidelines in the CCTV Operational Manual and Code of Practice, that technical safe guards such as 'no dwell zones' are entered into the CCTV system and that regular audits of the system are carried out.

Although general observation will be maintained within the cameras' arcs of observation (the cameras cover public areas and can see what a member of the public could see with the naked eye, albeit from a different angle), CCTV Operators will not follow individual members of the public except when an offence has been committed or in the judgment of the Operator is about to be committed.

Any images captured by CCTV will be held for a maximum of 28 days and then destroyed except when an enforcement agency requires the evidence to be retained for investigation or prosecution. No CCTV images will be released for commercial or entertainment purposes.

- c. **Article 10: FREEDOM OF EXPRESSION.** This article carries with it duties and responsibilities by the people who wish to exercise these freedoms. Therefore CCTV will only monitor such events in the interest of public safety, the prevention of disorder or crime, to protect the rights of others and to assist in enforcing any lawful restrictions placed on any such activity.
- d. **Article 11: FREEDOM OF ASSEMBLY AND ASSOCIATION.** Everyone has the right to peaceful assembly and freedom of association. CCTV will only monitor these events in the interest of public safety, the prevention of disorder or crime, the protection of the rights and freedoms of others and to assist in enforcing the lawful restrictions placed on any such event.
- e. **Article 14: PROHIBITION OF DISCRIMINATION.** Cambridge City Council has very clear policies on discrimination. All CCTV Operators are aware of the Council's policies. In addition, all Operators will attend extra anti-discrimination training. No Operator will monitor an individual because of their sex, race, colour, dress, appearance or monitor individuals by stereo typing them in any way.

15.3.6 All Operators must understand that they have a clear responsibility as the operators of the system to assist Cambridge City Council in its duty to uphold the HRA. Operators should do nothing that is likely to breach the HRA. If any Operators find themselves in a position where they are unclear as to how they should respond, they are to contact the CCTV Manager for guidance.

#### 15.4 **The Regulation of Investigatory Powers Act 2000 (RIPA)**

- 15.4.1 The Regulation of Investigatory Powers Act received Royal Assent in July 2000. The aim of the Act is to ensure that the investigatory powers of the intelligence service, police and the military etc are used in accordance with human rights. The Act provides a basis for authorisation and use by organisations of 'surveillance' (including CCTV) and regulates the techniques employed and safeguards the public from invasions of privacy.
- 15.4.2 This Act can be used for surveillance in the following categories:
- a. In the interests of national security.
  - b. To prevent or detect crime or prevent disorder.
  - c. For the economic well being of the United Kingdom.
  - d. In the interest of public safety.
  - e. For the purpose protecting public health.
  - f. Assessing or collecting of any tax, duty or levy.
  - g. For any other purpose ordered by the Secretary of State.
- 15.4.3 The Act does not cover the use of overt public CCTV systems, as members of the public are aware that such systems exist and are a means of detecting and deterring crime. General CCTV operations to observe public demonstrations or responses to immediate police requests for observation do not need to be authorized under RIPA. However, pre-planned, covert operations to follow known individuals, target premises or specific vehicles, which involve the use of CCTV, will need authorization.
- 15.4.4 The Act deals with 'covert surveillance', which is defined as: Observations, which are carried out by, or with, surveillance devices. Surveillance will be covert where it is carried out in a manner calculated to ensure that the person or persons subject to the surveillance are unaware that it is, or may be, taking place. Covert surveillance is divided into two types, 'direct' and 'intrusive'
- a. **Direct Surveillance** is covert but not intrusive and is undertaken:
    - (i). For a specific investigate or a specific operation;
    - (ii). In such a manner as is likely to result in obtaining private information about a person; and
    - (iii). Otherwise than by way of an immediate response to events or circumstances, which would not allow time for authorization to be obtained under this section (26) to carry out surveillance.
  - b. **Intrusive Surveillance** is covert surveillance that:
    - (i). Is carried out in any residential premises or any private vehicle and
    - (ii). Involves the presence of an individual or a surveillance device on the premises or in the vehicle.

- 15.4.5 No 'covert' cameras are used by Cambridge City Council's CCTV system. However, the CCTV Control Center may receive a request to mount observation on a known subject without their knowledge as part of a pre-planned operation, to watch the outside of a specific premises or to observe disruptive neighbors. These actions would be considered to be 'covert' surveillance. If a request is received, the agency requesting such assistance will be required to confirm the correct authorization has been obtained to ensure that the surveillance is lawful.
- 15.4.6 If authorization is obtained then a 'covert' surveillance operation becomes lawful under the RIPA. If however 'covert' surveillance is conducted without authorisation, then it is unlawful under Article 6 of the HRA.
- 15.4.7 No 'covert' operation will be undertaken by Cambridge City Council's CCTV system unless details of the serial number of the authorization certificate have been received along with the name of the authorizing officer, and the duration of the operation. All requests for pre-planned surveillance operations are to be directed to the CCTV Manager (or in his absence the Director of City Services or the Head of Parking Services) in advance of the operation. CCTV Operators are not permitted to authorise or take part in such operations without the expressed permission of the CCTV Manager (or, in his absence, the Director of City Services or the Head of Parking Services).
- 15.4.8 Authorizing Officers from the police will normally be a Superintendent or above and they may authorize operations for up to three months. In an emergency, the surveillance request may be authorized by and Inspector but the operation may only last for seventy-two hours unless written counter-authorization is received from a Superintendent or above. Authorizing Officers from other organizations will be at the level stipulated in the Act.
- 15.4.9 Authorization by agencies requesting assistance in 'covert' operations of any kind may be challenged by the CCTV Manager (or the Director of City Services or the Head of Parking Services). If in doubt, advice will be requested from Cambridge City Council's Legal Section.

## **15.5 The Freedom of Information Act 2000 (FOI)**

- 15.5.1 The Freedom of Information Act (FOI) was passed in 2000 and was fully implemented in 2005. The Act provides a general right of access to all recorded information held by public authorities without significant formality or inquiry into the motives of the applicant and at subsidised cost.
- 15.5.2 Rights granted under the Act provides that any person making a request for information to a public authority is entitled to be informed in writing by the public authority whether it holds information of the description specified in the request and if that is the case, to have that information communicated to them.
- 15.5.3 Under the Act the definition of 'information' means information recorded in any form and is fully retrospective. It includes personal and non-personal information.
- 15.5.4 Under the FOI Act it is a criminal offence to alter, deface, erase, destroy or conceal any record held by the council, with the intention of preventing

the disclosure of all, or part, of the information to which the applicant would have been entitled.

- 15.5.5 Applications for information may come from individuals or legal entities such as a company. Applicants do not have to mention any Acts nor do they have to give a reason for their application when applying for information but requests for information must be in writing.
- 15.5.6 The FOI Act should not unduly affect CCTV Operators. Their current dealings with and passage of information between partners will continue. However any requests for information from applicants outside these partnerships should not be dealt with by CCTV Operators but must be passed onto the CCTV Manager. He will then, were appropriate, arrange to liase with the City Council's Information Management Officer.
- 15.5.7 If an applicant is not satisfied with the way their application has been dealt with, they may make a complaint using the Council's complaints procedure or they may contact the Information Commissioner direct.

|   |
|---|
| <b>THIS MANUAL WAS LAST REVISED ON 13<sup>th</sup> MARCH 2007</b> |
|---|

**Particulars to be contained in records (Regulation 3 SI 2000/2725)**

The following matters are specified for the purposes of paragraph (d) of section 29(5) of the 2000 Act (as being matters particulars of which must be included in the records relating to each source):

(a) the identity of the source:

(b) the identity, where known, used by the source:

(c) any relevant investigating authority other than the authority maintaining the records:

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

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

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

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

(h) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c): (i.e. Handler and Controller details):

(i) the periods during which those persons (in "h" above) have discharged those responsibilities:

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

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

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

(m) any dissemination by that authority of information obtained in that way:

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

# A CODE OF PRACTICE FOR THE CAMBRIDGE CITY COUNCIL'S PUBLIC CCTV SCHEME

---



---

This Code of Practice has been the subject of extensive public consultation. Its aim is to ensure that the principles, which will govern the regulation and operation of the Cambridge CCTV system, are known to and approved by Cambridge residents.

For all enquiries about the Code of Practice, please telephone Martin Beaumont on (01223) 457390

## CODE OF PRACTICE

### INTRODUCTION

The Cambridge CCTV System has been developed in response to the growth of crime and fear of crime in the city. The sole purpose of the Cambridge CCTV System is to make the city a safer and more welcoming place at any time of the day or night, allowing all citizens and visitors, regardless of age, gender or race, the opportunity to participate fully and without fear in the life of the City.

Cambridge City Council, The Guildhall, Market Square, Cambridge, CB2 3QJ, operate the CCTV cameras, which is responsible for the fair and effective operation of all aspects of the CCTV service. A monitor screen has been installed at Police Headquarters at Hinchingsbrooke, which will allow the Council Control Room to relay pictures through to the Police.

The Code is also supported by an Operational Manual for staff operating the system. Only CCTV Staff, the Director of City Services, the Head of Parking Services and the Police Liaison Officer have authorised routine access to the CCTV Control Centre.

The System comprises of a number of colour and monochrome cameras and is operated from a Control Centre located at the Guildhall, Market Square, Cambridge, CB2 3QJ. The images from these cameras are recorded and monitored 24 hours a day, 365 days a year. All recorded material is the property of Cambridge City Council, which retains copyright.

This Code of Practice sets out the aims of the CCTV system and how it will be used. The system will not be used for any other purpose than those set out in this document. The operation of the System will be made accountable to the citizens of Cambridge via Cambridge City Council's Strategy-Scrutiny Committee, which will monitor its performance and review its effectiveness. The day-to-day management of the system will be the responsibility of Martin Beaumont, CCTV Manager.

### 1. PURPOSE STATEMENT

1.1 It is important that all those who will be affected by the Cambridge CCTV Scheme and all those charged with operating the service understand exactly why the system has been introduced and what it will and will not be used for. The key objectives of the Cambridge CCTV System are:

- . Protecting areas and premises used by the public;
- . Deterring and detecting crime;

Assisting in the identification of offenders leading to their arrest and successful prosecution;

Reducing anti-social behaviour and aggressive begging;

Reducing fear of crime;

Encouraging better use of city facilities and attractions;

Maintaining and enhancing the commercial viability of the city and encouraging continued investment.

## 1.2 Privacy

We respect and support the individual's entitlement to go about their lawful business and this is a primary consideration in the operation of the System. Although there is inevitably some loss of privacy when CCTV cameras are installed, cameras will not be used to monitor the progress of individuals in the ordinary course of lawful business in the areas under surveillance. Individuals will only be monitored if there is reasonable cause to suspect that an offence has been or may be about to be committed, as defined by the Operational Manual given to staff.

The Control Centre Operators must only use the cameras to view public areas and not to look into the interior of any private premises or any other area where an infringement of privacy of individuals may occur. The only exceptions to this rule are first, if an authorised operation is mounted under the Regulation of Investigatory Powers Act (see paragraph 1.6) or response to a police or other enforcement agencies' request for assistance following a crime being committed, or if an Operator, whilst operating the cameras in accordance with this Code of Practice, nevertheless happens to observe something which s/he believes indicates that a serious crime is being, or is about to be committed in a non-public area. Any event where an Operator takes a decision positively to view or continue viewing a private area must be entered into the Incident Log. The details must include location, time, date, camera number and the reason for the observation. Operators will be required to justify their actions. Any breach of this condition of employment will result in disciplinary proceedings and may lead to the dismissal of the Operator.

## 1.3 Cameras

All cameras are sited so that they are clearly visible, except for cameras used in Ely, Soham, as part of the Re-deployable CCTV system and in car parks, where cameras are mounted within protective domes. No hidden cameras will be used, nor will the Scheme utilise any non-functioning or 'dummy cameras'.

Publicity will be given to the system by clear signing within the monitored area. This will ensure that both the maximum deterrent value is achieved and that the public are clearly aware when they are in a monitored area. The System will not record sound in public places.

The Re-deployable CCTV cameras are designed to be deployed into other areas of the city for short periods of time. They are normally mounted on lampposts or buildings and send their images back to the CCTV Control Room via an encrypted radio signal. The use of these cameras is governed in exactly the same way as the fixed position cameras and they will be operated in accordance with this Code of Practice.

## 1.4 Provision of Evidence

Arrangements will be made to provide recorded images to the Police and other enforcement agencies including local authority departments. These images may be used to conduct investigations into potential criminal offences (e.g. racial

harassment). Images will only be released in connection with law enforcement processes.

### **1.5 Breaches of the Code**

Any breach of the Code of Practice is a serious matter. Officers or Control Centre staff who are in breach of the Code will be dealt with according to the disciplinary procedures of the City Council, a process that could ultimately result in their dismissal. If an employee/contractor were to misuse the images to make a profit for him/herself, the Council would take all possible steps to recover the profit made.

The responsibility for guaranteeing the security of the System will rest with the CCTV Manager, Martin Beaumont, who will in the first instance investigate all breaches or allegations of breaches of security and report findings to the Director of City Services and the Council's Internal Ombudsman who will jointly agree a response. If no agreement is reached, the matter will be referred directly to Committee.

In the event of a serious breach Cambridge City Council will request that a person with relevant professional qualifications who is independent of the Scheme undertake an investigation and make recommendations to the Council on how the breach can be remedied.

### **1.6 Legislation**

The Cambridge CCTV Scheme has been registered with the Information Commissioner's Office and will follow the guidelines of the Data Protection Act 1998 and the principles of good practice identified by the Information Commissioner (address on last page of this document).

In addition, Cambridge City Council's CCTV system will comply with the Human Rights Act 1998, the Freedom of Information Act 2000 and the Regulation of Investigatory Powers Act 2000.

The Regulation of Investigatory Powers Act is to ensure that investigatory powers of the intelligence services, the police and other enforcement agencies are used in accordance with the Human Rights Act and Cambridge City Council will ensure that all requests for assistance from the Council's CCTV system under this Act are examined in detail to ensure that they are proportionate, legal, appropriate and necessary. Where any doubts exist, legal advice or advice from the Surveillance Commissioner's Office (address on last page of this document) will be sought before the Council agrees to undertake action under this Act.

### **1.7 Changes to the Code**

Revision and change to the Code of Practice will inevitably occur during the life of the CCTV Scheme, due to evaluation of the Code and developments in the technology used in the Scheme. Cambridge City Council's Leader will approve all major changes to the Code of Practice after consideration by the Strategy Scrutiny Committee. If agreed, a new Code of Practice will be produced containing any newly agreed provisions and this New Code will replace all existing old codes which will be withdrawn from public circulation. The Director of City Services has authority to make minor amendments to the Code of Practice.

## **2. ACCOUNTABILITY**

There is a need for a well-defined structure of responsibility to the public to maintain public support and confidence in the CCTV System. The Cambridge CCTV Scheme will address this issue in the following way:

- Copies of the Code of Practice as agreed following public consultation will be

made available for public inspection at all Council reception points, public libraries and on the City Council's Website;

- The Council's formal complaints procedure covers complaints concerning the operation of CCTV.

### **3. EVALUATION**

Cambridge City Council will be responsible for the evaluation of the Scheme, which will be conducted at regular intervals following its introduction. This evaluation will be conducted both internally (Police and City Council staff) and independently by a body appointed by the Council. The following areas will be examined as part of the evaluation process:

- Assessment of the impact on crime;
- Assessment of neighbouring areas without CCTV (Displacement);
- The views of the public;
- Operation of the Code of Practice.

The costs of the evaluation programme will be built in to the annual running costs of the Scheme and the results of the evaluation, where appropriate, will be published.

### **4. CONTROL CENTRE OPERATION AND ADMINISTRATION**

#### **4.1 Staff**

The Control Centre will be operated on a 24-hour basis. Staff are employed by Cambridge City Council and are appointed subject to approved vetting procedures, to ensure their suitability for the work.

Cambridge City Council will ensure that all Operators are trained to a proficient level and are licensed by the Security Industry Authority before they are allowed to take up an operational position in the Control Room. Training will include:

- Use of equipment;
- Observation techniques;
- City Council procedures and record keeping;
- Report procedures and action on incidents;
- Evidence handling;
- Actions in the event of an emergency;
- Legislation and crime prevention;
- Operational exercises.

A suitably qualified member of the CCTV staff will supervise all training at all times. The Council will also ensure that all Control Room Operators are provided with annual "Refresher Training" to ensure that the highest operating and management standards are maintained. The Council will ensure that training records are maintained for each member of staff employed in the Control Centre. The conditions of employment will require a "Confidentiality Clause" which prohibits public and private disclosure of information obtained during monitoring. This clause will be effective both during and after staff service on the scheme.

The Council also reserves the right to exclude permanently from the Control Centre, and/or require the dismissal of, any Operator who is in breach of this Code. Staff will be required to provide the Police from time to time with statements required for evidential purposes.

Health and Safety issues regarding the CCTV Control Centre, its staff and visitors are covered in detail in Parts 1 and III of these documents.

## 4.2. **Operating Efficiency**

The Control Centre Duty Operators will daily confirm the operational efficiency of the system and the link to the Police. Any defects will be reported to the CCTV Manager Martin Beaumont. They will be logged and remedial action will be taken immediately.

At all times there will be at least one person remaining in the Control Centre. All use of the cameras shall accord with the purposes and key objectives of the Scheme as developed in training and specific operating instructions to staff, and shall comply with the Code of Practice.

Images and records will be reviewed periodically, and without prior notice to staff, by the CCTV Manager to ensure that this is happening. Staff will be aware that they will be subject to this audit of their recordings and will be required to justify their interest in a member of the public or particular premises. In the event of an emergency requiring evacuation of the Control Centre, procedures will be put into operation to ensure the continued operation and security of the system.

## 4.3 **Access**

The Control Centre door has an access control system and will remain secured at all times. Routine access to the Control Centre will be limited to:

- Duty CCTV staff;
- Designated officers of the Council;
- Designated police officers;
- Police officers who have been authorised by the Police Duty Officer and by prior arrangement with the CCTV Manager or duty CCTV staff;
- Particular arrangements will apply to visitors and contractors as outlined in 4.4 and 4.5 below.

## 4.4 **Visitors**

Organised visits for viewing the operation of the system will be arranged from time to time, but these may be subject to change or termination at short notice to meet operational requirements. Operation of equipment will only be carried out by the duty staff. All other persons wishing to visit the Control Centre must make their request to the CCTV Manager or in his absence the Head of Parking Services or the Director of City Services. Visitors may be asked to make their request in writing specifying the reasons for that request.

It is important that operations are managed with the minimum of disruption. Casual visits will not be permitted. All visitors will sign a log detailing their name, company, organisation, and their arrival and departure times. This log will be subject to regular audit and assessed to ensure compliance with the Code of Practice and operating procedures.

## 4.5 **Contractors**

Access for contractors will be necessary from time to time for the purpose of maintaining the Control Centre and its equipment. This will be limited to that strictly necessary for the work. At no time will contractors be left unattended in the Control Centre. All contractors' visits will be logged.

## 4.6 **Police**

The Police should not require access to the Control Centre unless specifically designated or authorised. Police officers attending unexpectedly shall only be admitted after the purpose of the visit has been approved by contact with the Duty

Officer at the City Police Station or the CCTV Manager. Their attendance will be logged.

#### **4.7 Control Centre Operation**

There must always be at least one Operator present within the Control Centre. An Incident Log will be maintained on the basis of date and time of day throughout operation. It will give brief details of all incidents monitored and show all relevant actions taken by Operators.

A Visitor Log will be maintained in the Control Centre, which all visitors will be required to complete. The entry will show the time, duration, date and intended purpose of the visit. A Media Movement Log and a Log of all Video (Still Image) Prints will be maintained.

#### **4.8 Communications and Control**

A monitor is installed in the Control Room at Police Headquarters at Hinchingsbrooke. Pictures from any of the cameras may be relayed to this monitor at the instigation of the CCTV Operator or at the request of the Duty Police Operator. The Police have no direct control of any cameras nor images relayed to their monitor. A dedicated radio and IP link with the Police Control Room is provided for communication. The link will only be used for official purposes. Emergency procedures will be used in appropriate cases to call or liaise with fire, ambulance or other emergency services.

### **5. DIRECTION AND CONTROL OF THE SYSTEM**

#### **5.1 Direction**

Operation of the system is the responsibility of the Director of City Services. The system is directed towards providing a safer environment for the community. The Council will use the system for:

- Day to day monitoring of the surveillance areas;
- The security of Council premises, land and street furniture;
- Monitoring premises using cameras and alarms owned by third parties under appropriate agreements.

#### **5.2 Police Role**

The control of the cameras and monitoring is in the hands of the Control Centre staff only. The Police may request assistance in order to:

- Assist with the deployment of resources;
- Monitor potential public disorder or other major security situations;
- Assist in the detection of crime;
- Facilitate the apprehension and prosecution of offenders in relation to crime and public order;
- Assist with the detection of moving traffic offences where it is considered that the public safety is at risk.

Such requests will usually arise after the Police have been contacted by the Duty Operator. In these circumstances the Police Duty Operator may request the Duty Operator to take further action. In circumstances when problems are anticipated, arrangements may be made for a Police Officer to be present within the CCTV Control Centre for liaison purposes. This will normally apply for the duration of the incident and will be subject to the arrangements made by the Police Duty Officer. On each occasion a record must be made in the Incident Log.

### **5.3 Major Incidents**

Use of the CCTV System will be integrated into the Council's Emergency Planning Procedures during major civil emergencies. If required, the Chief Executive or his designated deputy will authorise the deployment of a Liaison Officer from the major civil emergencies team into the CCTV Control Centre.

The Duty Operator(s) will give assistance and technical advice as required in all matters concerning the deployment and use of the facilities within the CCTV Control Centre.

### **5.4 Third Party Equipment**

The Council may monitor pictures from cameras installed by third parties subject to the making of the necessary formal agreements and the acceptance by third parties of this Code of Practice. Designated persons will have access to the Control Centre by prior appointment only and such visits will be strictly for the purpose of reviewing the operation of their own equipment. Attendance will be closely supervised at all times and equipment will continue to be operated by the Duty Operators. Access to images is detailed in the following section.

## **6. CONTROL OF IMAGE, RECORDING MEDIA AND VIDEO PRINTS**

### **6.1 DVD/CD Recording**

Recorded materials may need to be submitted as evidence in criminal proceedings and therefore must be of good quality, and be accurate in content. All such material will be treated in accordance with strictly defined procedures to provide continuity of evidence and to avoid contamination of the evidence. The Control Centre system is supported by permanent digital recording for all cameras. Recorded material will not be sold or used for commercial purposes or the provision of entertainment.

The showing of recorded material to the public will only be allowed in accordance with the law; either in compliance with the needs of Police in connection with the investigation of a crime, which will be conducted in accordance with the provisions of this Code of Practice, or in any other circumstances provided by law.

In certain circumstances images may be retained or copied for training, demonstration or evidential purposes. All other routine recordings will be retained for 28 days and then erased in accordance with defined operating procedures. Details of all reviewing of images will be recorded in the Third Party Viewing Log.

The Council retains copyright of all images and would use this to restrain unauthorised use of them. This would remain the case even if the monitoring were being carried out by contractors.

### **6.2 Control of DVD/CD Media**

All images on disc media will remain the property of the Council. Each new disc must be clearly and uniquely marked before it is brought into operation.

At each use the identification number of the disc, date, time of insertion and time of removal shall be noted in the Media Movement Log.

Except for evidential, training and demonstration purposes discs containing recordings must not be removed from the Control Centre under any circumstances. All discs will be erased prior to disposal.

### **6.3 Access to Images**

The principal external source of requests for access to images is expected to be from the Police or other enforcement agencies. The Duty Operators may deal with these requests. Other requests for access, such as for monitoring traffic flows, must be made in writing to the CCTV Manager, specifying the reasons for the request. Such reviewing must be directly supervised at all times.

Access to images by third parties will not normally be allowed except where a formal agreement is in force relating to monitoring of third party cameras. There may be circumstances in which the Council is subject to a court order to release images in connection with civil disputes. These cases are likely to be unusual, but the Council would be unable to refuse to release material in these circumstances. Access to disc containing the images or video print image evidence for lawyers acting for defendants or victims in connection with criminal proceedings will be provided under the Disclosure of Evidence Act by either the Police, Crown Prosecution Service or enforcement agency dealing with the case.

There may be a request under the Data Protection Act or the Freedom of Information Act to allow individuals to see or be informed about any data held about them. Since data is only stored for a maximum of 28 days, it is vital that such requests are made in writing to the City Council's Information Management Officer (address on the last page of this document) as quickly as possible, but in any event within 21 days to allow the relevant data to be held. The applicant will then be sent the necessary form to be filled in and returned so that their request can be met.

No other access will be allowed unless approved by the CCTV Manager for reasons, which fall within the purposes and objectives of the Scheme and in accordance with the Code of Practice.

#### **6.4 Images from Third Party Cameras**

Where a formal agreement for third party monitoring is in force, routine access to images will not be allowed. Applications to review images must be made in writing to the CCTV Manager specifying the reasons for the request. Third party viewings and production of recordings will be dealt with in the same way as all other agencies.

#### **6.5 Copying of Images**

Except for training, demonstration and evidential purposes images may not be copied in whole or in part.

#### **6.6 Evidential DVD or CD Discs**

Discs required for evidence will be dealt with in accordance with The Police and Criminal Evidence Act 1984 (PACE). A record will be made in the Third Party Viewing Log of the production of a master discs and its release to the Police or to other authorised agencies. An authorised officer may only remove these master discs from the Control Centre to a secure store.

Discs provided to the Police or other agencies shall at no time be used for anything other than the purposes for which they were originally released.

#### **6.7 Photographs**

The use of photographs for briefing camera operators should be conducted strictly in accordance with advice from the Police to avoid contamination of evidence. Unless otherwise advised by the Police, photographs:

- Should not be on display;
- Should only be retained if provided by the Police for this purpose;
- Should be seen only by individuals stipulated by the Police.

## **7. REVIEW AND EVALUATION**

### **7.1 Review**

CCTV Operations will be subject to regular review against the objectives of the Scheme. A core set of criteria has been agreed, and information will be collected at regular intervals measuring progress against them. Improvements to operating procedures will be made as soon as they are identified.

## **8. COMMENTS AND COMPLAINTS**

### **8.1 Comments**

Comments on the scheme may be addressed to the Director of City Services who has operational responsibility for the scheme.

### **8.2 Complaints**

Formal complaints about the operation of the system should be addressed to the Director of City Services (her address is on the last page of this document) as soon as possible after the incident or the CCTV action causing the complaint. They will be dealt with in accordance with the City Council's formal complaints procedure.

### **8.3 Addresses**

Contact addresses are:

Toni Ainley  
Director of City Services  
Cambridge City Council  
Mill Road Depot  
Cambridge CB1 2AZ  
Tel: 01223 458201  
Fax: 01223 458249  
E-mail: [toni.ainley@cambridge.gov.uk](mailto:toni.ainley@cambridge.gov.uk)

Paul Necus  
Head of Parking Services  
Cambridge City Council  
Mill Road Depot  
Cambridge CB1 2AZ  
Tel: 01223 458510  
Fax: 01223 457509  
E-mail: [paul.necus@cambridge.gov.uk](mailto:paul.necus@cambridge.gov.uk)

The Divisional Commander  
Southern Divisional  
Cambridgeshire Constabulary  
Parkside Police Station  
Parkside  
Cambridge CB1 1JG  
Tel: 01223 358966  
Fax: 01223 300380

Information Management Officer  
Cambridge City Council  
The Guildhall  
Cambridge CB2 3QJ  
Tel: 01223 457000  
Fax: 01223 457039

Information Commissioner  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire SK9 5AF  
Tel: 01625 545700  
Fax: 01625 524510

Surveillance Commissioner  
PO Box 29105  
London  
SWIV 1ZU  
Tel: 0171 825 3421  
Fax: 0171 828 3434

Martin Beaumont  
CCTV Manager  
Cambridge City Council  
The Guildhall  
Cambridge CB2 3QJ

Tel: 01223 457390  
Fax: 01223-457149  
E-mail: [martin.beaumont@cambridge.gov.uk](mailto:martin.beaumont@cambridge.gov.uk)

CCTV Website: [www.cambridge.gov.uk](http://www.cambridge.gov.uk) then select CCTV from the A to Z listings.

**THIS CODE WAS LAST REVISED IN JUNE 2009**