

WIRRAL COUNCIL

AUDIT & RISK MANAGEMENT COMMITTEE – 23 SEPTEMBER 2009

REPORT OF THE DIRECTOR OF LAW, HR AND ASSET MANAGEMENT

**OFFICE OF SURVEILLANCE COMMISSIONERS INSPECTION REPORT –
22 JULY 2009**

1. BACKGROUND

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) governs how public bodies use surveillance methods: The Council may use covert surveillance for the purpose of preventing or detecting crime or preventing disorder.

1.2 The origin of RIPA lies in the Human Rights Act 1998 which places restrictions on the extent to which public bodies may interfere with a person's right to respect for his or her home and private life and correspondence during the course of an investigation into suspected criminal activities. The provisions of RIPA ensure (in summary) that any such interferences are in accordance with the law and are necessary and proportionate (i.e. the seriousness of the suspected crime or disorder must outweigh any possible interferences with the personal privacy of the persons being investigated and of persons who associate with them).

1.3 The Council's Constitution authorises the Directors of Regeneration, Technical Services and Finance to designate Heads of Service and Service Managers to authorise the use of covert surveillance in accordance with the procedures prescribed by RIPA.

1.4 The Office of Surveillance Commissioners (OSC) is responsible for overseeing the operation of RIPA. The OSC inspects the Council regularly. It has done so in July 2003, 2007 and 2009.

1.5 This report summarises the findings of the OSC following its most recent inspection on 1st July 2009 and the action being taken to implement its recommendations.

2. THE USE OF RIPA BY THE COUNCIL

2.1 Between 1st July 2007 and 30 June 2009 the Council granted 58 authorisations for covert surveillance (an average of 29 annually).

2.2 Of those authorisations, 44 were for covert surveillance by the Wirral Anti-Social Behaviour Team to gather evidence of serious anti-social behaviour (mainly on housing estates) for use in proceedings for possession

injunctions and anti-social behaviour orders. The use of covert surveillance by the installation of cameras and sound recording equipment is a valuable means of overcoming the barriers raised by witness intimidation to evidence obtained by other means. It also is potentially more reliable evidence than the recollection of a witness whose memory may be fallible and whose evidence may be perceived as biased against the defendant.

2.3 Eleven authorisations were for covert surveillance by Wirral Trading Standards officers for use in investigations into offences such as the sale of counterfeit goods and of cigarettes, alcohol or fireworks to under-age children. They often take the form of "test purchases" in a shop from a retailer suspected of committing offences and the intrusion into personal privacy is minimal.

2.4 Three authorisations were granted by the Director of Technical Services for investigations into fly-tipping, unlawful street trading and the illegal deposit of skips on the highway. The high standard of those authorisations was particularly commended by the Surveillance Inspector when he examined them on 1st July 2009.

3. OSC REPORT

3.1 The report of the Surveillance Commissioner dated 22 July 2009 is contained in Appendix 1.

3.2 His Surveillance Inspector found that all four of the recommendations made by the previous Inspector had been carried out – namely;

3.2.1 Home Office model forms were being used;

3.2.2 A central record of authorisations had been compiled;

3.2.3 The training needs of applying and authorising officers had been analysed and training events organised;

3.2.4 Training events had covered the defects found by the previous inspector in the content of authorisations for covert surveillance.

3.3 The OSC made the following recommendations to improve the Council's implementation of RIPA:

Policy and Guidance Document

3.3.1 The Council's Policy and Guidance document should include practical advice for those seeking or granting authorisations for covert surveillance; it should cover the use of CCTV for covert surveillance and contain more detail about the use of covert human intelligence sources (CHIS).

The Council's Response

Additional paragraphs in Appendix 2 will be inserted into the Policy Document (Appendix 3) to include practical advice (paras 3.13 and 3.19), the use of CCTV (para 3.19) and more information on CHIS (para 4.5). The current Code of Practice for CCTV is attached in Appendix 4 and will be revised by the Department of Regeneration and the Police to reflect changes since its introduction and to ensure compliance with RIPA.

Central Oversight

3.3.2 There should be a single person with responsibility for maintaining the Central Record of Authorisations and for overseeing the use of authorisations for covert surveillance.

The Council's Response

Whenever an Authorising Officer grants an authorisation he or she should telephone the Central Services Manager in the Department of Law, HR and Asset Management and obtain a unique reference number. The Authorisations should then be immediately sent electronically to the Central Services Manager for inclusion in the relevant department's electronic folder and for inclusion on the Central Record. The contents of that Central Record are described in a new paragraph, 3.20 in the Policy Document (Appendix 2). A Group Solicitor has now been assigned to monitor proactively the use of RIPA. He will be the solicitor assigned to give advice to the anti-Social Behaviour Team (the main user of RIPA). He will hold quarterly meetings with the Co-ordinators in the Regeneration, Finance and Technical Services Departments to assess compliance with RIPA and the Policy Document using the information obtained from the electronic folder of authorisations and the Central Record of Authorisations. The first of such meetings since the inspection took place on 28 August 2009.

Defects in Authorisations

3.3.3 The Inspector noted certain weaknesses in the content of authorisations which are discussed in paragraphs 7.4 and 7.5 of his report. These imperfections must be remedied but it is important to note that the Inspector did not find that any authorisations (other than one retrospective authorisation) were unlawful or had been granted unnecessarily or were disproportionate or had involved too great an intrusion into a person's privacy. The defects were imperfections rather than fundamental flaws.

The Councils Response

Further guidance on the completion of an authorisation has been added to paragraph 3.13 of the Policy Document. There will be more central oversight of the standard of the content of authorisations by the Group Solicitor assigned for that purpose by the Head of Legal and Member Services. Efforts

will be made to organise future training which is more orientated towards practical advice on how to complete properly applications for authorisations.

4. FINANCIAL, STAFFING, LOCAL AGENDA 21, PLANNING, SOCIAL INCLUSION AND LOCAL MEMBER IMPLICATIONS

There are none.

5. EQUAL OPPORTUNITIES IMPLICATIONS

The purpose of RIPA is to strike a fair balance between the rights of individuals to privacy and the rights of public bodies to act in the public interest to detect and prevent criminal behaviour.

6. COMMUNITY SAFETY IMPLICATIONS

The use of RIPA enables the Council to use covert surveillance to tackle the problem of anti-social behaviour and disorder.

7. BACKGROUND PAPERS

There are none.

8. RECOMMENDATIONS

8.1 Members note the report of the OSC and approve the proposed response to his recommendations.

Bill Norman
Director of Law, H.R. and Asset Management

APPENDIX 1

The Rt Hon. Sir Christopher Rose



Office of Surveillance
Commissioners

400
050
CHIEF EXECUTIVE

24 JUL 2009

EXECUTIVE

24 JUL 2009
COPY BN 24.7.09



Chief
Surveillance
Commissioner

Restricted

22nd July 2009

Dear Mr. Maddox,

Covert Surveillance

On 1st July 2009, one of my inspectors, Mr Graham Wright, accompanied by Mr Kevin Davis, visited your Council on my behalf to review your management of covert activities. I am grateful to you for the facilities afforded for the inspection.

I enclose a copy of Mr Wright's report which I endorse. I am pleased to see that the recommendations made following the last inspection 2 years ago have all been discharged. But the present fragmented system and lack of clear, consistent, management is not explained by this recent change in personnel with responsibility for RIPA oversight. The weaknesses identified can readily be remedied if the recommendations are followed.

The recommendations are that your Policy document be amended to reflect the comments made in paras 6.2 and 6.3 of the report, that maintenance of the Central Record be rationalised and a more robust, consistent regime of quality assurance introduced and that the defects in authorisations identified in paras 7.4 and 7.5 remedied by applicants, authorising officers and those responsible for corporate oversight.

I shall be glad to learn that your Council accepts the recommendations and will see that they are implemented.

One of the main functions of review is to enable public authorities to improve their understanding and conduct of covert activities. I hope your Council finds this process constructive. Please let this Office know if it can help at any time.

Yours sincerely
Christy-Ann Rose

Mr Stephen Maddox
Chief Executive
Wirral Metropolitan Borough Council
Town Hall, Brighton Street
Wallasey
Wirral
Merseyside, CH44 8ED

Restricted

RESTRICTED



Office of Surveillance
Commissioners

OFFICE OF SURVEILLANCE COMMISSIONERS

INSPECTION REPORT

WIRRAL METROPOLITAN BOROUGH COUNCIL

1 July 2009

**Surveillance Inspector:
Graham Wright**

RESTRICTED

RESTRICTED

DISCLAIMER

This report contains the observations and recommendations identified by an individual surveillance inspector, or team of surveillance inspectors, during an inspection of the specified public authority conducted on behalf of the Chief Surveillance Commissioner.

The inspection was limited by time and could only sample a small proportion of covert activity in order to make a subjective assessment of compliance. Failure to raise issues in this report should not automatically be construed as endorsement of the unreported practices.

The advice and guidance provided by the inspector(s) during the inspection could only reflect the inspectors' subjective opinion and does not constitute an endorsed judicial interpretation of the legislation. Fundamental changes to practices or procedures should not be implemented unless and until the recommendations in this report are endorsed by the Chief Surveillance Commissioner.

The report is sent only to the recipient of the Chief Surveillance Commissioner's letter (normally the Chief Officer of the authority inspected). Copies of the report, or extracts of it, may be distributed at the recipient's discretion but the version received under the covering letter should remain intact as the master version. Distribution beyond the recipient's own authority is permissible but it is requested that the 'Secretary to OSC', Office of Surveillance Commissioners, is informed of the named individuals to whom copies or extracts have been sent. Any references to it, or extracts from it, must be placed in the correct context.

The Office of Surveillance Commissioners (OSC) is not a public body listed under the FOI Act 2000, however, requests for the disclosure to a third party of any information contained within this report should be notified to the Secretary to OSC."

RESTRICTED



Office of Surveillance
Commissioners

OSC/INSP/075

The Rt. Hon Sir Christopher Rose
Chief Surveillance Commissioner
Office of Surveillance Commissioners
PO Box 29105
London SW1V 1ZU

10th July 2009

OSC INSPECTION REPORT – Wirral Metropolitan Borough Council

1 Date of Inspection

The inspection took place on Wednesday 1st July 2009.

2 Inspector

Graham Wright conducted the inspection and was accompanied by Kevin Davis.

3 Introduction

3.1 Wirral Metropolitan Borough Council (MBC) is one the five constituent authorities of Merseyside. It employs approximately 12,500 staff (including teaching staff) serving a population of approximately 313,000. It was last inspected by the OSC in July 2007. In the period since the previous inspection the council has authorised 42 Directed Surveillance and no Covert Human Intelligence Sources (CHIS).

3.2 None of the above mentioned authorisations involved the acquisition of confidential information and I was not informed of any breaches.

3.4 There has been one change in the Directorate structure of the council with the creation of a Directorate of Law, Human Resources and Asset Management.

3.5 The Chief Executive is Mr. Stephen Maddox and the address for correspondence is Wirral Metropolitan Borough Council, Town Hall, Brighton Street, Wallasey, Wirral CH44 8ED.

4 Inspection Approach

4.1 This one day inspection commenced by meeting with the Chief Executive. He welcomed the inspection process and demonstrated a genuine interest in the council's usage and governance of RIPA.

RESTRICTED

RESTRICTED

- 4.2 We then met with Rosemary Lyon (Interim Head of Legal and Member Services) and Colin Hughes (Group Solicitor) who currently is overseeing RIPA processes following the departure of the previous Head of Legal and Member Services. They informed us of the council's response to the recommendations of the previous inspection, the council's authorisation and oversight arrangements and details of training provided.
- 4.3 There was also a meeting with the following Authorising Officers and enforcement officers. We discussed the activities of their departments and provided feed-back on the authorisations that had been examined:
- Mike O'Brien – Anti Social Behaviour Team
 - Lucy Pritchard – Enforcement Coordinator ASB
 - Simon Hutchinson – Risk and Insurance
 - John Sebborn – Anti Social Behaviour Team
 - John Kenny – Community Safety (CCTV)
 - John Malone – Trading Standards Manager
 - Abdul Bari – Trading Standards
 - David Green – Director, Technical Services
 - Sue Bannister – Environmental Enforcement
 - Phil Black – Enforcement Manager, Technical Services
 - Malcolm Flanagan – Revenue, Benefits and Customer Services
 - Kris NG – Housing Benefits
- 4.4 We also met with Drew Rai (Central Services Manager) who devised and maintains the Central Record of authorisations. Prior to the visit I had examined the council's policy document and training presentation and feed-back on them was provided on the day. We also examined 24 authorisations for Directed Surveillance on the day of the visit.
- 4.5 At the conclusion of the inspection feed-back was given to Bill Norman (Director of Law, Human Resources and Asset Management), Rosemary Lyon and Colin Hughes regarding the main findings of the inspection.
- 5 Review of Progress Against Previous Recommendations**
- 5.1 The 2007 inspection made four recommendations, all of which were accepted by the council.
- 5.2 *The Head of Legal and Member Services, in his RIPA monitoring role should ensure that the latest version of the Home Office model forms are used for authorising all future Directed Surveillance applications and that through the use of such forms, the imperfections found in the earlier applications and authorisations are not repeated.*

The most recent Home Office templates have now been taken into use and are available electronically to practitioners. Whilst some shortcomings remain in

RESTRICTED

authorisations and allocations, **this recommendation can be considered as discharged.**

- 5.3 *The central record should be regularly updated and capture all the information required by the Codes of Practice. It should be used more effectively in order to provide central oversight and monitoring of all authorisations.*

The Central Record of authorisations now complies with the requirements of the Code of Practise in that all the information required is contained in it and to that extent **this recommendation can be considered as discharged.** However, the maintenance and use of the record is the subject of a recommendation in this report.

- 5.4 *A training needs analysis should be undertaken to identify knowledge gaps and thereafter a corporate RIPA training event held to educate and inform all potential applicants and authorising Officers.*

The training needs analysis has been done and three events held since the previous inspection. **This recommendation can be considered as discharged.**

- 5.5 *The issues and imperfections discovered during this inspection should be included in the curriculum of any future corporate RIPA training event.*

This was done during the above mentioned training events. Therefore, notwithstanding the fact that weaknesses are still evident, **this recommendation can be considered as discharged.**

6 Policies and Procedures

- 6.1 As mentioned previously, the council's policy and guidance document had been examined prior to the inspection visit. It is the *Policy and Procedure on the Use of Powers Under RIPA (2008)*. The document contains the Human Rights background and context of RIPA and all the relevant definitions. There is also a description of the internal processes for authorisation.
- 6.2 Whilst the document does not contain any inaccurate information and guidance, it lacks practical advice to those who may seek or grant authorisation, concentrating more of the legal aspects of RIPA. There is also very little explanation regarding the provisions and actions action to be taken in respect of CHIS.
- 6.3 There is no CCTV protocol or guidance regarding the use (by council staff or other agencies) of such systems in circumstances regarding authorisation under RIPA.
- 6.4 The process for applying for and obtaining authorisation is that applicants will usually complete the relevant forms and forward them electronically to an

RESTRICTED

Authorising Officer. This officer should then ring a legal secretary to obtain a URN from the Central Record. When this has been obtained and the authorisation granted the relevant file will be electronically stored in the relevant department's folder and the Central Services Manager informed of this fact in order that the authorisation can be accessed and a full Central Record entry completed. A hard copy of the authorisation is securely retained in Legal Department.

- 6.5 Subsequent submissions are similarly dealt with.

7 Inspection Findings

Central Record and Oversight

- 7.1 Whilst the Central Record of authorisations complies with the Code of Practice in terms of its content, it is not used to have oversight, or conduct any management, of authorisations granted by the council. It is also the case that several authorisations had not been entered on the Central Record and only came to light as part of the preparation for this inspection.
- 7.2 There is currently no corporate quality assurance of authorisations and compliance audit as there is no single person with clear responsibility for this and the maintenance of the Central Record. This is fragmented and is failing to address the poor quality of some authorisations and lack of compliance with laid down processes.

Directed Surveillance

- 7.3 This is the only form of covert activity undertaken by the council and is predominantly used for investigations into Anti Social Behaviour, Trading Standards matters, Benefit Fraud and waste tipping.
- 7.4 The standard of applications and authorisations varied considerably. Those from Technical Services in particular were of a good standard. Others had failings in some aspects and several from Trading Standards were authorised retrospectively by the Authorising Officer. This had been done in a transparent fashion, with the authorisations having been clearly marked to this effect and had occurred due to the fact that the Authorising Officer from the applicant's department was absent and therefore the activity was not authorised until after it had been conducted. I am satisfied that this was done as a result of lack of understanding by the applicant but is clear evidence of the need for some form of oversight that can pick up on such mistakes and ensure that they do not recur - rather than waiting for the issue to be highlighted at the next OSC inspection.
- 7.5 Whilst the above mentioned matter was the most serious defect, others could render authorisations vulnerable to challenge. The following weaknesses were discovered during our examination:

RESTRICTED

- It was not always clear as to what the information/intelligence was that an investigation was based upon
- Applicants failed to properly answer why the covert activity was necessary and proportionate
- Authorising Officers failed to evidence their considerations regarding the key principles of necessity and proportionality
- Authorising Officers failed to set down an accurate description of all the covert activity they were authorising
- Cancellations were late and contained very little detail regarding what activity had been conducted under the authorisation, what surveillance product had been obtained and how that product was being stored, retained, or destroyed
- Where a technical feasibility study has been completed this should be included in the documentation considered by the Authorising Officer and officers carrying out technical installations should have sight of the relevant authorisation prior to the installation being carried out
- Review dates should be stipulated by the Authorising Officer at the time of authorisation

Training

- 7.6 The council has held several training events since the previous OSC inspection and these have been attended by the vast majority of staff who may be an applicant or Authorising Officer.
- 7.7 I examined the content of those events and found it to be an accurate and relevant description of the law. What was lacking was a more practical application of the provisions of RIPA and guidance regarding the completion of applications and authorisations.

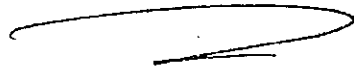
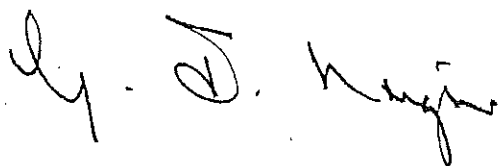
8 Conclusion

- 8.1 Wirral MBC uses the powers vested under the Regulation of Investigatory Powers Act 2000 in appropriate investigations. There has been a recent change in personnel with responsibility for RIPA oversight but even this does not account for the fragmented system and total lack of clear and consistent management.
- 8.2 The solution is simple and will result in greater levels of compliance and an improvement in standards.
- 8.3 I would like to pass on my thanks to all the staff we met for their co-operation and courtesy. Particular thanks should be passed to Colin Hughes who made all the arrangements for the day and provided me with the pre-read material.

RESTRICTED

9 Recommendations

- 9.1 The council policy document should be amended to address the failings found and there should be a policy/protocol regarding the use of council CCTV – paragraphs 6.1 to 6.3
- 9.2 The maintenance of the Central Record of authorisations should be rationalised and a more robust, consistent quality assurance regime introduced – paragraphs 7.1 and 7.2
- 9.3 The listed failings in Directed Surveillance authorisations should be borne in mind by applicants, Authorising Officers and those with responsibility for corporate oversight – paragraphs 7.4 and 7.5



Surveillance Inspector

APPENDIX 2

POLICY AND PROCEDURE GUIDANCE ON RIPA – PROPOSED ADDITIONS

3.13 **Add** the following sentences

Officers should ensure that when they complete the authorisation forms they comply with the following requirements:

- (a) the information on which an investigation is based must be clearly identified
- (b) applications should state clearly why the covert activity is believed to be necessary and proportionate.
- (c) Authorising Officers should clearly state why they consider the covert activity is necessary and proportionate (including the steps to be taken to minimise intrusions into privacy, particularly of those persons not suspected of crime or disorder). They must never be granted retrospectively.
- (d) Authorising Officers must describe accurately all the covert activity which they are authorising so as to ensure that the limits are not infringed.
- (e) Technical feasibility studies should be presented to the Authorising Officer along with the application for authorisation. They should be attached to the authorisation. If the authorisation is granted, the person carrying out technical installations (e.g. of cameras and sound recording equipment) must see the relevant parts of the authorisation prior to the installation of any surveillance equipment.
- (f) Review dates should be stipulated by Authorising Officers at the time they authorise the covert surveillance for any extended period. This is to ensure that the need for continuation of the surveillance is regularly assessed and recorded on Form RIPAD52 and that (where appropriate) authorisations are

either renewed (before they expire) on Form RIPAD54 or cancelled on Form RIPAD53.

- (g) Cancellations of authorisations should be made promptly when the need for covert surveillance has ceased. The cancellation should contain a full description of the activity which has been authorised, what the results of the surveillance were, and how and when any products of the surveillance will be stored, retained or destroyed.

ADD

3.19 The following examples illustrate the circumstances in which it is necessary and appropriate to obtain authorisation for covert surveillance:

- 3.19.1 Residents report to the Anti-social Behaviour Team that the occupants of a neighbouring property are disturbing them at night by engaging in noisy parties or quarrels fuelled by the consumption of alcohol and threaten them with violence when they protest.

In such circumstances covert surveillance (e.g. by means of a camera and sound recording devices unobtrusively fitted to an adjoining property) would be necessary to prevent crime and disorder (because witnesses are likely to be intimidated) and proportionate (the disturbance is frequent and at a high level). The recording device should not normally be capable of picking up conversations at a normal level within the home targeted (and consequently is not intrusive). The Authorising Officer must therefore have available a technical feasibility study .

The amount of collateral intrusion on the privacy of the persons should be low (if the device is directed only at the targeted property) and if the need for continual surveillance is regularly reviewed by the Authorising Officer to

ensure that the recording device is removed (when, for example it becomes apparent that the antisocial behaviour has ceased or significantly diminished) Those fitting the recording device must be shown that part of the authorisation which defines the permitted coverage of the camera so that the limits of the authorisation are not infringed.

3.19.2 The police approach the operators of the Council's CCTV cameras and ask them to train their cameras on a particular part of a public place where they suspect drug dealers are doing business. Council staff may only comply with the request of the police if they are satisfied that the police officers have obtained the necessary authorisation for directed surveillance from their superiors. Whilst the cameras are overt, they would be used for the purposes of a specific investigation or specific operation and therefore that use would require authorisation. Members of the public would not normally expect public cameras to be trained on specific individuals or on specific public places for protracted periods and therefore their use in that instance would be covert. The same principles would apply if Trading Standards Officers requested the use of CCTV cameras to monitor the activities of suspected illegal traders in a prohibited street. Authorisation for directed surveillance would be required before the CCTV cameras could be used for that purpose.

ADD

3.20 The Head of Legal and Member Services will compile and maintain electronically a central record of authorisations granted by authorising

Officers. That central record shall contain the following information about the authorisation:

- (a) Whether it is for Directed Surveillance or Covert use of Human Intelligence Source.
- (b) Its unique reference number.
- (c) Applicant's name and title.
- (d) Department and Section.
- (e) Identity of Target and the title of the investigation.
- (f) Date of authorisation.
- (g) Renewal Date and name and/or title of Authorising Officer.
- (h) Review Date.
- (i) Whether the urgency provisions were used and, if so, why?
- (j) Whether the investigation is likely to result in obtaining confidential information.
- (k) Cancellation Date.

The information contained in the Central Record will be used by the Head of Legal and Member Services to monitor the use by departments of RIPA. It will be a standing item on the agenda of the quarterly meetings of the Coordinators Group referred to in paragraph 7.1.

ADD

- 4.5 The following examples illustrate the circumstances in which it is necessary and proportionate to obtain authorisation for the use of a CHIS (Covert Human Intelligence Source).

4.5.1 The Anti-Social Behaviour Team engage a private detective to pose as a tenant of Wirral Partnership Homes in order to form a relationship with a group of tenants suspected of committing acts of serious anti-social behaviour, including criminal damage to property, drug dealing and intimidation of other tenants. The purpose of establishing a relationship is to obtain information admissible in possession proceedings (e.g. by covert tape recordings of conversations) or to assist the police or the Anti-Social Behaviour Team to anticipate the future criminal behaviour of the tenants under suspicion. No potential witnesses are willing to co-operate with the Anti-Social Behaviour Team by installing cameras in the properties. Authorisation would be required in such circumstances since the private detective will be establishing a personal relationship with the subjects to obtain and disclose information to the Anti-Social Behaviour Team in a manner that is calculated to ensure that the subjects are unaware of the purpose of the personal relationship. This example also illustrates the difficulties, dangers (and expense) of using a CHIS in the circumstances where evidence cannot be obtained by other methods.

4.5.2 A trading standards officer enters a shop and makes a "test purchase" from a retailer suspected of selling "counterfeit goods". No authorisation would be required for a CHIS because he would not be establishing a personal relationship with the retailer (although if he had attached to his person a concealed camera it would be necessary for him to obtain authorisation for directed surveillance). If on the other hand, the trading standards officer struck up a conversation with the retailer whilst posing as a member of the public in order to ascertain whether the retailer (without any encouragement

from the Trading Standards Officer) would offer to sell him (or another customer) counterfeit goods, then he would be acting as a CHIS and authorisation would be required. The essence of a CHIS is that he obtained information by winning someone's confidence on a false basis

APPENDIX 3



POLICY AND PROCEDURE ON THE USE OF POWERS UNDER THE REGULATION OF INVESTIGATORY POWERS ACT

1. INTRODUCTION

- 1.1 *"Surveillance plays a necessary part in modern life. It is used not just in the ~ targeting of criminals but as a means of protecting the public from harm and ~ preventing crime."*

From the Foreword to the Home Office's Code of Practice on Covert Surveillance

- 1.2 The use of covert surveillance by public authorities, particularly local authorities has been the subject of much recent debate. The use of covert surveillance is properly a matter of public concern. The purpose of this policy is to set out exactly how the Council will use its surveillance powers and comply with best practice.
- 1.3 **Councils may only use covert surveillance for the purpose of preventing or detecting crime or preventing disorder and where doing so is in the public interest.** The Council uses covert surveillance to support its enforcement activities. It has been used principally by the Regeneration Department in dealing with anti-social behaviour and trading standards cases. This has resulted in many successful cases being brought which might otherwise not have been possible bringing rogue traders to account and improving the lives of Wirral residents suffering from severe anti-social behaviour. In 2007/8 the Council used directed surveillance on 45 occasions; 36 in anti-social behaviour cases and nine in cases investigated by Trading Standards.
- 1.4 The Council approved a policy and procedure for the use of covert surveillance in 2004. The Council has been inspected twice by the Office of the Surveillance Commissioner in 2003 and 2007. The use of surveillance was also the subject of a review by the Council's Internal Audit Team in 2008. The need to revise and update the Council's Policy and Procedure was identified as part of that review.

2. RELEVANT LEGISLATION

2.1 The Human Rights Act 1998 (HRA)

2.1.2 The HRA gives effect to the rights and freedoms guaranteed under the European Convention on Human Rights and Fundamental Freedoms ("the Convention"). 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. It is now clear from decided cases that this right extends to activities of a professional or business nature and so includes employees. 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.

2.1.3 Consequently, there is to be no interference with the exercise of these rights by any public authority, except where:

Such interference is in accordance with the law and is necessary in a democratic society in the interests of:

- national security
- public safety
- the economic well-being of the country
- for the prevention of disorder or crime
- for the protection of health or morals
- the protection of the rights and freedoms of others.

The Council is a public authority. However, as mentioned above (and explained in more detail in section 3 below), local authorities may **only** undertake covert surveillance for the purpose of preventing or detecting crime or preventing disorder.

2.1.4 The HRA can be found at:

www.opsi.gov.uk/ACTS/acts1998/19980042.htm

2.2 **The Regulation of Investigatory Powers Act 2000 ("RIPA")** (and associated Regulations)

2.2.1 RIPA was introduced shortly after the HRA to ensure that the use by public bodies of surveillance was codified. Prior to RIPA there was only limited regulation of the use by public bodies of surveillance. RIPA was passed to ensure a consistency of approach and to set in place safeguards to ensure that the use of surveillance is proportionate.

2.2.2 RIPA was passed well before the terrorism attacks on September 11 and was not introduced to deal with terrorism. RIPA and its associated regulations also follow the philosophy of recent legislation in trying to strike a balance between community responsibilities, including effective law enforcement, and individual rights and freedoms.

3.0 COVERT SURVEILLANCE

3.1 The term surveillance includes

- Monitoring, observing or listening to people, their movements, their conversations or their other activity or communication;
- Recording anything monitored, observed or listened to in the course of surveillance;
- Surveillance by or with the assistance of a surveillance device.

3.2 **Covert** surveillance is surveillance that is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. This needs to be contrasted with the deployment of **overt** surveillance. The use of such surveillance in places to which the public has access is increasingly commonplace. The Council has employed it in the form of CCTV monitoring of its offices, car parks and the town centres. CCTV monitoring is undertaken in accordance with the Council's Code of Practice for the operation of CCTV. CCTV is usually clearly marked through the use of signage.

3.3 RIPA applies where any covert surveillance of an identifiable or named person is carried out by a public authority carrying out an investigatory function. RIPA includes a local authority within the description of public authority.

3.4 Covert surveillance can be either

- (a) **intrusive**, that is, carried out in relation to anything that is taking place on any residential premises or in any private vehicle by an individual or a surveillance device on the premises or in the vehicle; or
- (b) **directed**, that is, undertaken for the purposes of a specific investigation or operation and involving the observation of a person or persons in order to gather information about them.

3.5 **Local authorities are not authorised to conduct intrusive surveillance.**

3.6 **Directed** covert surveillance that is likely to result in obtaining private information about a person is permitted by RIPA and its associated regulations if such surveillance has been authorised in the manner provided by the Act, the Home Office Code of Practice and the prescribed standard forms. Private information is any information relating to a person's private or family life.

- 3.7 An authorising officer for a public authority may only grant authorisation to carry out directed surveillance if it is necessary in the interests of:
- national security (not applicable to local authorities);
 - preventing or detecting crime or of preventing disorder;
 - public safety (not applicable to local authorities);
 - protecting public health (not applicable to local authorities);
 - assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department (not applicable to local authorities); or
 - is specified by regulations.
- 3.8 Local authorities may only authorise use of covert directed surveillance on the ground that it is necessary in the interests of preventing or detecting crime or of preventing disorder. The use of surveillance must also be proportionate to what is being sought to achieve.
- 3.9 Authorisation is not required to record things which are not planned but arise in the course of an investigation. For example if an enforcement officer is attending a property to visit a witness and observes a neighbour causing criminal damage he/she can record what they saw without authorisation.
- 3.10 Particular care needs to be taken when the surveillance may give rise to the obtaining of **confidential information**. In this context confidential information means:
- Where legal professional privilege applies;
 - Confidential personal information; or
 - Confidential journalistic material

Legal professional privilege will apply to oral and written communications between a professional legal adviser and his/her client made in connection with the giving of legal advice or in connection with or contemplation of legal proceedings.

Confidential personal information is information held in confidence about a person's physical or mental health or to spiritual counselling or assistance. The information must have been created or acquired in the course of a trade, business or profession or for the purpose of any paid or unpaid office.

Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

If the purpose of the surveillance is to obtain confidential information then this will need to be approved by the Head of Legal and Member Services and the Chief Executive. If in the course of an operation confidential material is obtained through surveillance this must be notified immediately to the Head of Legal and Member services. It must be retained and provided to the inspector from the Office of the Surveillance Commissioner at the next inspection.

- 3.11 An applying officer wishing to use directed surveillance must complete **FORM RIPADS1** (all forms are attached to this policy). The applying officer must fully complete all parts of the form. The officer should refer as necessary to the Home Office Code of Practice, available as set out in paragraph 3.18 below.
- 3.12 The applying officer must consider the proportionality of the use of surveillance. The officer must consider the seriousness of the matter being investigated, the impact that any evidence obtained through the surveillance will have on the investigation and the level of intrusion which will be caused. The officer must take steps to ensure that any intrusion is kept to the minimum level necessary. Any intrusion in to the private life of persons not the subject of the investigation (e.g. family or visitors) should be minimised.
- 3.13 The completed form should be referred to an **authorising officer**. All Chief Officers may designate officers within their department as authorising officers for the purposes of RIPA. On receipt of the form the authorising officer will contact the Head of Legal and Member Services to obtain a unique reference number. The authorising officer must be a Head of Service or Service Manager. The authorising officer will place the form on the central register. The register is an electronic folder with access rights limited to authorising officers (for their area only) and the Head of Legal and Member Services or his/her nominated representatives (to all contents). When an authorising officer places a form on the register he/she will also separately notify the Head of Legal and Member Services by e-mail that this has been done. If the authorising officer does not have access to the register he or she will e-mail the form to the Head of Legal and Member Services who will arrange for it to be placed on the register. All forms for authorised applications shall be placed on the register immediately. All applications shall remain on the register for at least 3 years.
- 3.14 **Urgent Oral Applications**
- 3.14.1 It is possible to grant urgent oral authorisations. It is envisaged that this will be done very rarely, if ever. No authorisations have been granted in this way in the past 3 years. The Code of Practice states that this should not be done:
- unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the authorising officer's own making.*

3.14.2 Where an urgent authorisation is granted the authorising officer must record as soon as is practicable the reasons for granting the authorisation urgently. An urgent authorisation will lapse after **seventy two hours**.

3.14 Review/Cancellation

3.15.1 Written authorisations will lapse automatically unless they are renewed after **3 months**. However, authorisations should be reviewed on a regular basis and cancelled when they are no longer required for the purpose for which they were granted. In each case the authorising officer within each public authority should determine how often a review should take place. This should be as frequently as is considered necessary and practicable. On carrying out a review the authorising officer should complete a **Form RIPADS2**. Once completed the form should be placed on the central register immediately either by the authorising officer directly or via the Head of Legal and Member services. If the form is placed directly on the register the authorising officer must notify the Head of Legal and Member Services that this has been done by e-mail.

3.15.2 If upon review the need for directed surveillance no longer exists then the authorisation will be cancelled immediately. On cancellation the authorising officer shall complete **Form RIPADS3**. The completed form shall be placed on the central register either by the authorising officer directly or via the Head of Legal and Member services. If the form is placed directly on the register the authorising officer must notify the Head of Legal and Member Services that this has been done by e-mail.

3.16 Renewal

If the authorisation is due to lapse it may be renewed for a period of a further 3 months provided the need for the surveillance continues. If a renewal is required a **Form RIPADS4** shall be completed. If an authorisation is renewed for a further period of 3 months it should be reviewed during that period.

3.17 Audit Checks

The Head of Legal and Member Services shall carry out a regular audit of authorisations contained on the central register at least once every 3 months.

3.18 Code of Practice

The Home Office Code of Practice on the Use of Covert Surveillance can be viewed at: <http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/>

4.0 COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

- 4.1 The use of CHISs is also regulated by RIPA. A CHIS is a person who establishes or maintains a relationship with someone in order to obtain information, to provide another person with access to information or to disclose information as a consequence of that relationship. Should an officer consider the use of a CHIS as necessary, they must liaise with the Head of Legal and Member Services. If the use of a CHIS is deemed necessary, special arrangements will be made for their use in accordance with the Home Office Code of Guidance on Covert Human Intelligence Sources (see paragraph 4.5 below). It is not anticipated that CHISs will be used often by the Council. However, if professional witnesses are used they may fall within the definition of CHISs.
- 4.2 If an investigating officer does believe that the use of a CHIS is necessary in the course of an investigation he/she should complete **FORM RIPACHIS1**. The officer must consider the safety and welfare of a person acting as a source and must carry out a risk assessment before authorisation is granted. The use must be proportionate to what is intended to be achieved. The authorisation will lapse automatically if not renewed after a period of **12 months**.
- 4.3 Special considerations apply if the person to be used as a source is **vulnerable** or a **juvenile**. In such circumstances advice should be sought from the Head of Legal and Member Services. Authorisation may only be granted by the Chief Executive, as Head of Paid Service, or in his/her absence a Chief Officer.
- 4.4 The same procedures outlined above in respect of directed surveillance of:
- Maintenance of a central register
 - Confidential information
 - Review
 - Cancellation
 - Renewal; and
 - Audit checks

Shall also apply to the use of CHISs. The following forms shall be used **FORM RIPACHIS2** (review), **FORM RIPACHIS3** (cancellation) and **FORM RIPACHIS4** (renewal)

4.5 Code of Practice

The Code of Practice relating to the use of CHISs can be found at:
<http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/>

5.0 COMMUNICATIONS DATA

- 5.1 Requests for communications data will be dealt with by **designated persons**. Those persons who are authorising officers for the purposes of directed surveillance and CHISs shall also be designated persons for the purposes of obtaining communications data. Each local authority must have its own **Single Point of Contact (SPOC)**, to whom applicants can submit their requests for communications data. This is to ensure there is a specific point of accountability in each authority requesting data for reasons connected with RIPA and the HRA etc. The SPOC for Wirral Council is the Trading Standards Manager
- 5.2 It is important to note that we are not referring here to the interception of communications or the **content** of communications. The Council does not have power to intercept communications or acquire content.
- 5.3 There are 3 types of communications data;
- traffic data;
 - service use data; and
 - subscriber data.
- 5.4 More information on what constitutes these types of communication data is set out in the Home Office Code of Practice (see paragraph 5.9 below). Advice can also be sought from the Head of Legal and Member Services. Local authorities are only able to seek disclosure under RIPA of service use data and subscriber data not of traffic data.
- 5.5 Applications may be made for service use data e.g. itemised bills or subscriber data e.g. whether a person uses a particular network, who is the user of a particular number. A request for such information can only be made where it is necessary for the purpose of preventing or detecting crime or preventing disorder. The request must be proportionate. The form for completion for disclosure of communications data including guidance on completion is attached as **FORM RIPACD 1**. An authorisation or notice remains valid for **one month**. A valid authorisation or notice may be renewed for a further period of one month.
- 5.6 An authorisation or notice must be cancelled as soon as it is no longer necessary for the service provider to comply with the notice or the conduct required by the notice is no longer proportionate to what was sought to be achieved.
- 5.7 The **Senior Responsible Officer** must be responsible for:
- the integrity of the process in place within the public authority to acquire communications data;
 - compliance with Chapter II of Part I of the Act and with this code;

- oversight of the reporting of errors to the Interception of Communications Commissioners Office (IOCCO) and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with the IOCCO inspectors when they conduct their inspections; and
- where necessary, overseeing the implementation of post-inspection action plans approved by the Commissioner.

In Wirral the Senior Responsible Officer is the Head of Legal and Member Services.

5.8 In Wirral there has been very limited use of these powers. In the year 01/01/08 – 31/12/08 there were only 2 requests made for subscriber data by the Council.

5.9 The Home Office Code of Practice on the use of Communications Data can be viewed at: <http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/acquisition-disclosure-cop.pdf>

6.0 REPORTING AND REVIEW

5.1 The Council recognises the public interest in the use by it of these powers. It is essential that it regularly monitors and reviews the use of these powers. Therefore, this policy and procedure shall be subject to a review on at least an annual basis. The Head of Legal and Member Services shall report annually to the Chief Officers Management Team on the use of these powers and the Director of Law, HR and Asset Management shall report annually to the Cabinet and the Audit and Risk Management Committee.

7.0 COORDINATION AND TRAINING

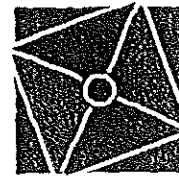
7.1 All Departments that use or may use the Council's powers under RIPA shall nominate a Departmental Coordinator under this Policy. The Departmental Coordinators shall meet at least once a quarter to review the operation of this policy, share best practice and consider training needs. Those meetings shall be chaired by the Head of Legal and Member Services or his/her nominated representative. Appendix 1 shows the list of Departmental coordinators.

7.2 The Council shall ensure that adequate training is provided to officers in the use of the powers. A training register shall be maintained and all authorising/designated officers will receive training at least every 2 years. A copy of the register is attached as Appendix 2. If an authorising/designated officer has not attended any training for a period of 2 years they shall **automatically cease** to be a responsible/authorised officer.

This page is intentionally left blank

APPENDIX 4

**CODE OF
PRACTICE FOR
CLOSED CIRCUIT
TELEVISION**



CODE OF PRACTICE

1.00 INTRODUCTION

1.01 This Code of Practice covers the purpose, use, accountability, management and monitoring of the Hamilton Quarter Closed Circuit Television (CCTV) system.

1.02 The system is owned by:

Metropolitan Borough of Wirral
Wallasey Town Hall
Brighton Street
Wallasey
Wirral
Merseyside
L44 5AA

1.03 The principles of Town Centre CCTV surveillance were approved by the Council's Policy and Resources General Panel on the 8th August 1996, following full consultation with the Merseyside Police.

1.04 The **system** enables video/data transmissions to be relayed from remote cameras at the sites listed in paragraph 1.07 back to the central control room via optical fibre.

1.05 All video circuits are fed into a central switching matrix located at the Council's control room. The local police control room is able to observe the system from remote facilities on a monitor. The Council control room has full telemetry control over the cameras. Time-lapse video recording of all circuits is undertaken by the Council. Real time recording may occur from time to time to assist police operations or responses to civil emergencies.

1.06 The camera control system provides all video switching and telemetry facilities.

1.07 The **cameras cover** the areas in and around:-
Hamilton Square, Argyle Street, Cleveland Street, Conway Street,
Hamilton Street, Market Street, Price Street and nearby car parking areas.
The precise area of camera coverage in each location is not stated for operational reasons.

1.08 . All **recorded material** on video tapes is the property of the Metropolitan Borough of Wirral and the copyright of the material recorded thereon remains with the Council at all times.

2.00 PURPOSE

2.01 The **purpose** of the scheme is to reduce crime and the fear of crime by helping to provide a safer environment for those people who live and work in the area and for visitors.

2.02 The system will provide the police with assistance to detect, deter and prevent **crime**. It will:

- help identify, apprehend and prosecute offenders
- provide the police with evidence to enable criminal and civil proceedings to be brought in the courts
- help to maintain public order.

2.03 In addition, the system will enable traffic and parking to be monitored by the Council.

2.04 The system will be operated at all times with due regard for the **privacy** of individuals and will not to be used to invade the privacy of any individual in residential, business or other private premises, buildings or land.

2.05 The system will not be used to harass any person or group of persons going about their business in a lawful way.

2.06 Any user found to have contravened the privacy of individuals in breach of this Code of Practice will be subject to the disciplinary procedures of the Council or police as appropriate.

2.07 The **key objectives** of the system are:

- to provide public reassurance and to deter crime
- to detect, prevent or reduce the incidence of all crime
- to improve general security in the area, both in terms of personal safety and the security of buildings and premises
- to reduce the theft of and from vehicles both on the street and in car parks
- to reduce graffiti, vandalism and other criminal damage

- to reduce the level of disorder and minor crime in the area
- to improve communication between, and the operational response of, police patrols in and around the town centre and assist in the policing of the area
- to reduce the fear of crime and encourage the regeneration of the area
- to assist the police with specific operations aimed at either catching criminals or intelligence gathering and in the event of acts of terrorism or civil emergencies
- to assist in traffic management by monitoring traffic accidents or obstructions thereby preventing or alleviating interruptions to traffic flow
- to identify missing persons.

2.08 Evidence in the form of recorded material is only available to the police and tapes are handed over only after the relevant reports have been completed. Other statutory bodies, such as Customs and Excise, may also be provided with recorded evidence on receipt of an official request. The criteria governing the release of tapes is stated in paragraph 15.00 **Recorded Material**.

2.09 The Metropolitan Borough of Wirral Council and the Merseyside Police are **committed** to complying with this Code of Practice in all their dealings with the CCTV system.

2.10 A joint **Operational Guidelines Manual** covering the operation of the CCTV system has been prepared jointly by the Council and the Merseyside Police and both organisations will strive to comply with that manual at all times. To maintain the integrity of the system the manual is a restricted document.

3.00 DATA PROTECTION IMPLICATIONS

3.01 The activities carried out under the CCTV system will not fall within the scope of the Data Protection Act 1984.

3.02 Should the operation of the CCTV subsequently fall within the scope of this Act, then it will be so registered and a statement to that effect will be included in the annual report and added to this Code of Practice.

4.00 CHANGES TO THE CODE OF PRACTICE

4.01 **Major changes** to the Code of Practice will only take place after full consultation between the Council and the Merseyside Police. Notice of major changes will be placed in the local press prior to implementation to allow for public comments to be taken into account. These changes will only become effective after the approval of the Council and will be reported in the annual report each year.

4.02 . **Minor changes** to the Code of Practice will be made by the Principal Community Safety Officer on behalf of the Council and the local Police Superintendent on behalf of the Merseyside Police and these changes will be reported in the annual report each year.

4.03 A **major change** is one which will have a significant impact upon the Code of Practice or upon the operation of the system. A **minor change** is one which, for example, may be required for clarification or which arises as a result of technical changes to the system and will not have major implications.

4.04 This Code of Practice will be subject to periodic review to ensure that it reflects best practice and responds to changes in criminal or case law.

5.00 RESPONSIBILITIES OF THE COUNCIL

5.01 As the owner of the system, the Metropolitan Borough of Wirral is responsible for the introduction, implementation and updating of the Code of Practice in consultation with the police and for ensuring compliance with the **Operational Guidelines Manual**.

5.02 The Council will have regard to the requirements for accountability and the protection of the interests of the public and of the individual and will be responsible for public consultation as appropriate.

6.00 MANAGEMENT OF THE SYSTEM

6.01 The **day to day management** of the system will be carried out by the Council's **Principal Community Safety Officer** and the Community Patrols Section. It includes daily tape changing and review, daily liaison with the police, fault identification and repair instigation.

6.02 **Access to the Council's control room** is strictly controlled and the names of all visitors are recorded in a log book. Access to that control room for police officers is only permitted upon production of the officer's warrant card.

6.03 Access to the police control room is controlled by separate police regulations.

6.04 Access to recorded material is controlled by the Council's Community Patrols Section and police officers are permitted to review and retain video tapes only after providing the relevant report and signing the log of borrowed tapes.

6.05 The documentation used for the daily management of the system is included in the **Operational Guidelines**.

7.00 INSTALLATION

- 7.01 The introduction of CCTV to the area was carried out only after extensive **consultation** between the Council, the public and the police.
- 7.02 Camera positions are those identified as being the most effective in detecting or preventing crime. Where building-mounted, the express permission and agreement of the freeholder and any leaseholders has been obtained. This agreement is formalised by a licence sealed by all parties including the Council and provides for future maintenance and emergency repairs to be carried out by the Council's authorised contractor.
- 7.03 There is no provision in the system installation for **sound** to be transmitted or recorded.
- 7.04 The equipment may be **changed** at any time to take account of technological improvements. Changes will be agreed by the representatives of the Council and the police. Any technological change will be included in the annual report.
- 7.05 **Dummy cameras** will not be deployed as part of the system.

8.00 ACCOUNTABILITY

- 8.01 **The Public** will have access to copies of this Code of Practice and the annual report in accordance with the Local Government (Access to Information) Act 1985.
- 8.02 **The Council** will receive regular reports on the deployment and effectiveness of the system and will receive and approve the annual report including details of crime statistics relevant to the area covered by the system.
- 8.03 Procedures for audit of council procedures are described in paragraph 10.03 Audit of the System.
- 8.04 **The police** will comply with this Code of Practice in all matters relating to the operation of the CCTV system.
- 8.05 Internal police procedures are in place to ensure proper monitoring and audit of the police use of the system. The officer responsible for such audit is the Inspector responsible for Strategy and Planning at Birkenhead Police Station.

9.00 PUBLIC INFORMATION

- 9.01 All **cameras** will be overt and readily identifiable in full view of the public. Dummy cameras and covert cameras will not be deployed as an integral part of the system.

- 9.02 Signs indicating that CCTV monitoring is taking place will be prominently displayed in the area covered by the system. The signs will not define the precise areas covered by the field of view of the cameras but will be distributed throughout the area as a deterrent to criminals and a reassurance to the general public.
- 9.03 This **Code of Practice** is a public document as defined under the Local Government (Access to Information) Act 1985 and is available for inspection by members of the public. Copies are available at the Hamilton Quarter office, all public libraries and information points within Council premises.
- 9.04 In addition, a copy of the Code is available for inspection at Birkenhead and Wallasey police stations.
- 9.05 This Code of Practice and the Operational Guidelines Manual have been compiled using the advice contained in the Local Government Information Unit document - A Watching Brief (A Code of Practice for CCTV).
- 9.06 The council, in consultation with the police, will publish an **annual report** on the operation of the CCTV system to the Council's Policy and Resources General Panel. The report will be available to the public in accordance with the Local Government (Access to Information) Act 1985.
- 9.07 The report will include comparative crime statistics for the area covered by the system; details of significant arrests achieved through the deployment of the cameras; an assessment of the effectiveness of the system in addressing the key objectives and details of any complaints. Costs of maintaining and repairing the system will also be included.
- 9.08 The report will also include a review of partnership changes (if any) and policy developments which are likely to affect the purpose and operation of the system.

10.00 ASSESSMENT OF THE SCHEME AND CODE OF PRACTICE

- 10.01 The scheme will be independently evaluated periodically and the **evaluation** will include the following:
- an assessment of the impact the scheme has had upon crime in the area covered;
 - comparison with neighbouring similar areas not covered by CCTV;
 - the views of voluntary organisations;
 - whether the key objectives have been and are continuing to be met;
 - a commitment from the Council that recommendations from the evaluation will be taken into account in the future operation of the scheme;

- an assessment of the operation of the Code of Practice and the Operational Guidelines Manual.

10.02 The Principal Community Safety Officer will **monitor** the operation of the scheme and the implementation of the Code of Practice.

10.03 Regular **audit** of the operation of the system, the Code of Practice and the Operational Guidelines Manual will be undertaken by the Hamilton Quarter and will include examination of control room records; video tape histories and their contents and will be undertaken sufficiently frequently to provide effective monitoring of the system.

11.00 COMPLAINTS

11.01 The **procedure** will be that followed universally throughout the Metropolitan Borough of Wirral. Further information, details and the necessary documentation are available at any Council office.

11.02 The **annual report** will contain statistical information on the complaints received during that year. Any complaints which result in changes in policy or to the Code of Practice will be described in the annual report.

11.03 Any complaint about the **police** involvement of the system will be dealt with under the statutory police complaints procedure.

12.00 BREACHES OF THE CODE AND SECURITY

12.01 Prime responsibility for the Code of Practice and for security surrounding the system rests with Metropolitan Borough of Wirral. This responsibility includes ensuring that breaches are investigated and remedied.

12.02 **Responsibility** for security on a day-to-day basis rests with the Principal Community Safety Officer. The Community Patrols Section maintains a rota to cover absence to maintain proper security at all times.

12.03 Major **breaches** of the Code of Practice will be investigated by the Council's **Senior Inspector (Management Services of the Education Department)** and he shall have responsibility for making recommendations to remedy any major breach which is proved. If a **criminal offence** is disclosed then the matter will be referred to the police.

12.04 Minor breaches will be investigated by the Principal Community Safety Officer.

13.00 CONTROL AND OPERATION OF CAMERAS

- 13.01 Information recorded shall be accurate, adequate, relevant and not exceed that necessary to fulfil the purpose of the system.
- 13.02 Information recorded shall have been obtained in accordance with the provisions of the Code of Practice.
- 13.03 **Operation** of camera equipment will be carried out with the utmost probity. Only staff responsible for using the equipment will have access to the operating controls. All use of cameras will accord with the purposes and key objectives of the system as defined by the Code of Practice.
- 13.04 Cameras will not be used to look into private property except where there are substantial grounds for believing that a serious offence is taking place.
- 13.05 Camera operators are subject to supervision and disciplinary procedures as set out in the paragraph 2.04 Privacy. Camera operators are aware that video tapes are subject to routine audit and that they may be required to justify their interest in a member of the public or premises.

14.00 ACCESS TO AND SECURITY OF CONTROL ROOM

- 14.01 Access to the **control room** is strictly controlled and only those persons on legitimate business are allowed access.
- 14.02 A record is maintained of all visitors to the control room and access is only allowed after formal identification has taken place.
- 14.03 Access for visitors to view the system will only be permitted after full consultation with the system manager or the Principal Community Safety Officer.
- 14.04 A **log book** of visits to the control room is maintained. This book contains details of the individual and organisation, date, time and purpose of visit.
- 14.05 All works to the control room will be carried out in strict compliance with current **Health and Safety** requirements and in accordance with accepted best practice.

15.00 RECORDED MATERIAL

- 15.01 Recorded material will only be used for the purposes defined in the Code of Practice.
- 15.02 Access to recorded material will only take place as defined in the Code of Practice.

- 15.03. Recorded material will not be sold or used for commercial purpose or the provision of entertainment.
- 15.04 The showing of recorded material to the public will only be allowed in accordance with the law. This can be done in response to the needs of the police in connection with the investigation of crime and will be conducted in accordance with the provisions of any relevant Code of Practice under the Police and Criminal Evidence Act 1984 and any advice and guidance given to the police from time to time or in any other circumstances provided by law.
- 15.05 Sufficient tapes will be available including a supply of spare tapes to replace those removed for evidential purposes.
- 15.06 Tapes will be used in strict rotation and be retained for 28 days before being reused. All tapes will be separately indexed and those required by the police for evidential purposes will be separately stored to avoid accidental re-use.
- 15.07 The tape retention policy has been agreed with the police and the Crown Prosecution Service.
- 15.08 All tapes will be degaussed mechanically immediately prior to reuse and used no more than twelve times before replacement. After twelve uses the tapes will be degaussed and disposed of to charitable organisations approved by the Council.
- 15.09 Tapes will be stored in a secure cupboard or cabinet. Tapes will be individually and uniquely identified and labelled. A register will be kept giving dates when individual tapes were used. The tape register and method of storing tapes will be subject to regular audit.
- 15.10 Tapes required for **evidential purposes** shall be treated as exhibits and be retained and stored according to procedures agreed from time to time with the police and the Crown Prosecution Service.
- 15.11 Council staff will provide the police with a statement confirming the tape's integrity if required for evidential purposes.
- 15.12 Tapes provided to the police shall at no time be used for anything other than the purpose specified and identified when the tape is released to the police by the Council.
- 15.13 An authorised police officer may, by agreement with the Council, visit the control room from time to time to confirm that agreed procedures for tape handling are being followed.
- 15.14 Access to tapes by third parties in connection with civil disputes may be obtained only by court order. Lawyers acting for defendants or victims in connection with criminal proceedings may apply for access to the tapes only in accordance with rules of discovery.

15.15 Other requests, including those from the media or commercial undertakings will be considered by the Principal Community Safety Officer in conjunction with such other advisers as he may choose to consult. Generally, taped material will not be released unless it can be clearly demonstrated that the release would assist with the investigation of an incident or crime to which taped record relates. In no event, will taped records be released for commercial or media exploitation or gain. In the event that release under the foregoing terms is recommended, then, written approval must be obtained before handing over the tape(s) takes place.

15.16 The Partnership is committed to working closely with the National Missing Persons Helpline, and tape extracts or hard copy from the system tapes may be passed to the NMPH where it is jointly considered that this will directly assist in the location of a missing person.

16.00 PHOTOGRAPHS

16.01 Still photographs from live incidents will only be taken at the request of the police officer in charge at the scene.

16.02 A police officer authorised by a police officer of at least the rank of sergeant may request the production of a still photograph taken at a live incident or a still photograph from a video recording. The authorising officer should be satisfied that the still photograph is required for the prevention or detection of crime.

16.03 All still photographs will remain the property of the Council. Any still photographs released to the police will be dealt with by the police as an exhibit and shall not be used for anything other than the purpose specified and identified when released to the police.

16.04 Procedures for the taking, retention and supply of still photographs will be subject to regular audit.

17.00 POLICE USE OF THE SYSTEM

17.01 Police use of the system will be in accordance with local needs and the purpose of the system and will be in accordance with the Code of Practice.

17.02 The police will use the system in response to specific incidents to protect life and property and to prevent or detect crime.

17.03 The police may direct the operational use of the system in the event of a pre-planned event after consultation between the Principal Community Safety Officer and the Senior Police Officer in charge of the event.

17.04 In the event of the above situations, responsibility for recordings will remain with the Council.