



Corporate Services Overview and Scrutiny Committee

Date:	Thursday, 2 April 2009
Time:	5.30 pm
Venue:	Committee Room 3 - Wallasey Town Hall

Contact Officer: Andrew Mossop
Tel: 0151 691 8501
e-mail: andrewmossop@wirral.gov.uk
Website: <http://www.wirral.gov.uk>

AGENDA

1. DECLARATIONS OF INTEREST/PARTY WHIP

Members are asked to consider whether they have personal or prejudicial interests in connection with any item(s) on this agenda and, if so, to declare them and state what they are.

Members are reminded that they should also declare, pursuant to paragraph 18 of the Overview and Scrutiny Procedure Rules, whether they are subject to a party whip in connection with any item(s) to be considered and, if so, to declare it and state the nature of the whipping arrangement.

2. MINUTES (Pages 1 - 4)

To receive the minutes of the meeting held on 5 March, 2009.

3. USE OF POWERS UNDER THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA) (Pages 5 - 72)

Following the Committee's request at its last meeting for a report on the Regulation of Investigatory Powers Act, this report, which has been considered by the Chief Officer's Management Team and is being considered by the Standards and Audit and Risk Management Committees and Cabinet, is submitted for the Committee's information.

4. BUILDING MAINTENANCE (Pages 73 - 76)

5. ANY OTHER URGENT BUSINESS APPROVED BY THE CHAIR

CORPORATE SERVICES OVERVIEW AND SCRUTINY COMMITTEE

Thursday, 5 March 2009

Present: Councillor L Fraser (Chair)

Councillors C Meaden K Wood
C Teggin P Southwood
J Crabtree J Keeley

Cabinet Member Councillor S Holbrook

47 DECLARATIONS OF INTEREST/PARTY WHIP

Members were asked to consider whether they had personal or prejudicial interests in connection with any item(s) on this agenda and, if so, to declare them and state what they were. Members were reminded that they should also declare, pursuant to paragraph 18 of the Overview and Scrutiny Procedure Rules, whether they were subject to a party whip in connection with any item(s) to be considered and, if so, to declare it and state the nature of the whipping arrangement.

No such declarations were made.

48 MINUTES

Members were requested to receive the minutes of the meetings of the Corporate Services Overview and Scrutiny Committee held on 12 January and 4 February, 2009.

Resolved – That the minutes of the meetings held on 12 January and 4 February, 2009, be approved as a correct record.

49 PERFORMANCE MONITORING REPORT - QUARTER 3

The Deputy Chief Executive / Director of Corporate Services submitted the third quarter Performance Monitoring report. The report included progress on key actions and performance indicator exceptions together with sickness absence figures and a financial summary as at 31 December, 2008 for both the Corporate Services and Law, HR and Asset Management Departments.

Both the Directors of Corporate Services and Law, HR and Asset Management responded to comments from Members on the sickness figures and the Director of Law, HR and Asset Management stated that he would provide a written response to clarify the performance indicator figures on the percentage of local authority employees declaring that they met the Disability Discrimination Act 1995 disability definition.

Resolved – That the report be noted.

50 ACCOMMODATION CHANGE - UPDATE

Further to minute 43 (12/1/09), the Director of Law, HR and Asset Management submitted a report on the development of an implementation programme for office change.

In agreeing the Strategic Asset Review, the Council had also resolved that the office accommodation aspects of the review be implemented and that officers be asked to accelerate the process of making savings from the rationalisation of the Council's office accommodation.

The Council's Asset Management Plan contained its accommodation strategy, the key elements of which were to reduce the average office space occupied by employees to 10 sq. m. per person and concentrate directorate staff in fewer locations. Implementation of the plan had resulted in some smaller administrative buildings being vacated and released for disposal. In the light of the SAR and the savings target created the Council's accommodation strategy now required review. The lead officer on the review would be the Head of Asset Management.

At the same time the Head of Transformation had been examining the use of and need for office space by different services and functions across the authority, and researching accommodation change programmes in other authorities. This, coupled with an understanding of service and business changes currently in progress, had enabled the identification of areas most suitable and ready for change. In addition some pilot agile working projects had been undertaken, and lessons learned from these, together with learning from other authorities, would be used to shape Wirral's accommodation change programme. The report went on to outline the next steps which would be taken and also detailed the lease arrangements for the Cheshire Lines building.

In response to comments from Members, the Director stated that it was probable that the proposed Project Manager for accommodation change would be an internal appointment utilising existing resources within the department and that it would need to be a full time position. The Project Team would contain officers from across the Council; in particular from the key resource areas (Asset Management, IT, HR, Finance and Transformation) and from the major services affected.

There was a budget of up to £100,000 for consultancy work in relation to the office accommodation review although if some of this work could be undertaken in-house, subject to existing capacity, then it would be.

The Director also explained the restrictions on the lease arrangements for the Cheshire Lines building.

Resolved – That the report be noted.

51 UPDATE ON WORK PROGRAMME

The Committee received an update on its work programme, which indicated those reports which it had considered over the past municipal year.

The Director of Corporate Services explained how the Committee's work programme had been set for the year.

The Chair stated that Committee members were always able to ask for reports. A member suggested that the Committee could do some more pro-active work, setting the agenda for scrutiny rather than reacting to issues as they arose.

With the permission of the Chair, the Cabinet Member addressed the Committee and stated that he would welcome a more pro-active role by the Committee and Committee members generating ideas for debate.

On a motion by Councillor Southwood, seconded by Councillor Teggins, it was then –

Resolved – That an extra meeting of the Committee be arranged prior to the 9 April Cabinet, on a date to be agreed by the Chair in consultation with the Party spokespersons, to consider 2 issues:

- **The Regulation of Investigatory Powers Act**
- **Buildings Maintenance**

This page is intentionally left blank

STANDARDS COMMITTEE - 30 MARCH 2009

AUDIT AND RISK MANAGEMENT COMMITTEE – 31 MARCH 2009

CORPORATE SERVICES O&S COMMITTEE – 2 APRIL 2009

CABINET – 9 APRIL 2009

REPORT OF THE DIRECTOR OF LAW, HR AND ASSET MANAGEMENT

USE OF POWERS UNDER THE REGULATION OF INVESTIGATORY POWERS ACT (RIPA)

1. Background

- 1.1. The Regulation of Investigatory Powers Act 2000 (“RIPA”) governs how public bodies use surveillance methods. Wirral Council, like other local authorities may use directed surveillance where doing so is in the public interest for the purpose of preventing or detecting crime or preventing disorder.
- 1.2 The Office of the Surveillance Commissioner (“OSC”) is responsible for overseeing the operation of RIPA. The Council has to account to the OSC on an annual basis on its use of RIPA. The Council has been the subject of 2 inspections by the OSC in July 2003 and July 2007. The Council’s use of RIPA was also the subject of a recent review by the Internal Audit Section. One of the recommendations of that review was that the Council’s Policy and Procedures on the use of RIPA be updated. The Policy was most recently reviewed in 2004.

2. THE USE OF RIPA BY LOCAL AUTHORITIES

- 2.1. There has been much debate in the last 12 months around the use of surveillance powers by local authorities. This has led the LGA to write to Leaders of all Councils. John Healey MP, the Minister for Local Government also wrote to all Chief Executives in November 2008 regarding the use of surveillance by local authorities. The Home Office has announced an intention to consult on the use of RIPA powers by public authorities in early 2009.
- 2.2. Unfortunately there has been a large degree of misreporting of the subject of surveillance. The Home Office has published on its website a document on some of the misconceptions. A copy is attached as Appendix 1 to this report.
- 2.3. The Council has used directed surveillance to support its enforcement activity since the passing of RIPA. In the year 2007/8 the Council granted 45 authorisations. These related to cases investigated by the Wirral Anti-social Behaviour Team (36) and the Trading Standards team (9). The use of these powers has assisted in legal action to tackle rogue traders and to obtain court orders to tackle anti-social behaviour. The Council has used surveillance evidence in numerous court actions and its use has never been challenged. In some cases surveillance evidence obtained by the Council under RIPA has been used by the police to secure criminal convictions.
- 2.4. The use of RIPA is overseen by the Office of the Surveillance Commissioner (OSC). The OSC carries out regular inspections of public bodies. The OSC last inspected the Council in July 2007. A copy of the report is attached as Appendix 2 to this report. It considers the previous report of the OSC in 2003 and concludes that:

Whilst the actions taken by the Council have addressed many of the significant issues raised in the previous inspection report, more works need to be done to fully rectify the previous deficiencies.

2.2 The report sets out a number of recommendations. These are set out below followed in italics by the actions taken to implement the recommendations:

(a) the Head of Legal and Member Services should ensure that the correct current forms are being used.

The current versions of the forms have been circulated to all teams using or which may potentially directed surveillance

(b) ;the Central Record should be regularly updated;

A new procedure has been implemented to ensure that Departments update the central record immediately upon authorisation being granted

(c) the Central Record should capture all the information required by the Codes of Practice;

The new will system will ensure that this is done

(d) the central record should be used more appropriately to provide central oversight and monitoring of authorisations;

The new system will enable Legal and Member Services to have better access to the applications in a timely manner to monitor use of RIPA

(e) a training needs analysis should be undertaken to identify any knowledge gaps and thereafter a corporate training event held to educate and inform all potential applicants and authorising officers;

An assessment has been carried out and a training event took place on 7 October 2008 which was well attended. A further event is due to take place in April 2009. It will be a requirement that all authorising officers who have not received training in the past two years shall attend one of those sessions. It is intended that after the second event has taken place all applying officers will have received training. The training is specifically tailored to Wirral and will highlight the issues raised in the OSC report.

(f) there is a need to attach a central unique reference to each application;

The new system provides for this.

(g) there should be an annual report to COMT on the use of RIPA;

The first such report was received by COMT in June 2008 and further reports will be brought to COMT.

2.3 A review of the use of RIPA has also been carried out by Internal Audit at the request of the Chair of the Audit and Risk Management Committee in December 2008. This identified a number of areas for improvement and an action plan was agreed. A copy is attached as Appendix 3.

2.3 The action plan identified the need for the Council's policy and procedure on the use of powers under RIPA to be updated. A draft policy is attached which has been considered by Chief Officers Management Team. It is also being considered by:

Standards Committee– 30 March 2009;
Audit and Risk Management Committee – 31 March 2009; and
Cabinet – 9 April 2009.

4.0 RECOMMENDATION

4.1 Members note the report.

BILL NORMAN
DIRECTOR OF LAW, HR AND ASSET MANAGEMENT

This page is intentionally left blank

Misconceptions about RIPA

Misunderstandings about RIPA and its use - your questions answered.

RIPA is an anti-terrorism legislation

It's not. RIPA legislates for and regulates the use of a range of covert techniques for a range of purposes. The more intrusive of these powers (such as interception) are limited to law enforcement and intelligence agencies and can be used to investigate serious crime as well as terrorism.

Other less intrusive powers such as directed surveillance or access to communications data can be used by a greater number of public authorities for a wider range of purposes, including the prevention and detection of crime generally.

Local authorities and councils are wrongly using anti-terrorism powers

Recent stories in the media have often misrepresented RIPA and what parliament agreed that local authorities can do under the legislation. Parliament gave permission to a range of public authorities to use covert investigatory powers under RIPA, where they need them to carry out their statutory functions.

Under RIPA, local authorities are able to use a far more restricted range of investigatory techniques than intelligence and law enforcement agencies.

They are limited to using the least intrusive types of communications data; directed surveillance (which means covert surveillance in public places) and covert human intelligence sources (such as informants), and only for detecting or preventing crime and preventing disorder where it is necessary and proportionate for them to do so.

For example, trading standards departments are responsible for investigating and prosecuting rogue traders and other scams. Local authorities also deal with people who are claiming housing benefits which they are not entitled to, in other words, people who commit benefits fraud. It is for individual authorities to decide in each case whether it is necessary and proportionate to make use of the powers in the specific circumstances.

Local authorities cannot carry out intrusive surveillance, or seek warrants for interception. Nor are they able to access the most intrusive form of communications data, namely traffic data.

RIPA powers can be used by local councils on 'trivial matters'

There are strict rules to protect people from unnecessary or inappropriate intrusion and any use of the powers must be both necessary and proportionate to the crime being investigated. Where individuals believe powers have been used inappropriately, they can take their case to the Investigatory Powers Tribunal.

The Local Government Association and the Communities and Local Government Minister have each written to all local councils to ensure that their use of RIPA powers is necessary and proportionate as required by the legislation.

The Home Office and the Department for Communities and Local Government are working together to ensure all local authorities have a good understanding of RIPA and circumstances when it would be appropriate and when it would not be appropriate to use covert surveillance.

During 2009, the Home Office will be issuing a revised code of practice on the use of directed and intrusive surveillance for public consultation. This will then be considered by parliament before replacing the existing code.

Confusion over the difference between interception and communications data

Many stories in the media confuse interception (for example, listening to someone's telephone conversations or reading an e-mail or letter) which can only be conducted by law enforcement and intelligence agencies with a Secretary of State warrant, with access to communications data (eg subscriber details or billing information) which is available to a wider number of public authorities.

RIPA is another example of the erosion of our privacy and civil liberties

RIPA is a pro-human rights law that, rather than 'giving' powers, controls activities that need to be regulated. It puts in place the proper mechanism to consider the key issues of necessity and proportionality. In fact, it did not create any new powers or techniques at all; nor did it permit any public authority to use powers which it could not have used prior to RIPA.



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

31st July 2007

**OSC INSPECTION REPORT – WIRRAL METROPOLITAN BOROUGH
COUNCIL**

Date of Inspection : 30th July 2007

Inspector : Mr Richard Allsopp

Address of Public Authority : This report should be sent to Mr Stephen Maddox, Chief Executive, Wirral Metropolitan Borough Council, Town Hall, Brighton Street, Wallasey, Wirral, Merseyside CH44 8ED.

REVIEW OF PROGRESS

Structures and Procedures

1. The last OSC inspection of the Wirral Metropolitan Borough Council was conducted in June 2003 by an Assistant Surveillance Commissioner with the subsequent report dated 2nd July 2003. The overall structure of the Council remains as previously reported.
2. At the time of the last inspection the Council had no corporate guidance document covering the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA) relying instead on various documents adopted by the departments involved in covert activity. A centrally retrievable record of authorisations had not been established and departments were keeping their own records. Acting on the advice of the Assistant Surveillance Commissioner, all the matters raised at the last inspection have been incorporated into a Council RIPA Policy and Employees Guide covering Directed Surveillance and the Use of Covert Human Intelligence Sources. It was published to all departments in December 2003 and revised in 2004 in order to reflect the changes brought about by Statutory Instrument 2003 No 3171.

RESTRICTED

RESTRICTED

3. The latest version of the RIPA forms have been obtained from the Home Office but as yet they have not been brought into use.
4. Six Authorising Officers have been nominated covering the four departments actively using the powers vested in the Council, all of whom accord to the designation contained in latest Statutory Instrument. The specific responsibilities of the Chief Executive have been recognised.
5. The policy requires the Authorising Officer to forward details to the Head of Legal and Member Services for inclusion in the central record which is maintained on his behalf by Simon Goacher, a Solicitor in Legal Services. In practice, at quarterly intervals copies of all applications, authorisations, renewals and cancellations are called for and entered in the central record. The documents are in paper format and retained in folders, with an overview sheet for each department containing all the details required by paragraph 2.14 of the Covert Surveillance Code of Practice. A computerised system is under consideration. There is no corporate system for allocating the documents a Unique RIPA Reference Number. A limited amount of central monitoring is conducted by Mr Goacher. The Community Safety Solicitor meets the Anti Social Behaviour Team on a weekly basis to review their investigations and provide appropriate advice over the use of covert surveillance.

Use of RIPA

6. Since the last inspection 96 authorisations have been granted for Directed Surveillance, the majority on behalf of the Anti Social Behaviour Team who deploy covert video recorders from the homes of complainants to capture images of anti social behaviour by neighbours. A private contractor is engaged to provide and deploy the equipment. Three other departments have obtained a small number of Directed Surveillance authorisations; Trading Standards, Planning Enforcement and the Insurance Section. The latter employs Private Investigators to conduct covert surveillance on its behalf.
7. Covert Human Intelligence Sources have not been used and no other Services have sought authorisations. None of the authorisations involved the possible acquisition of 'confidential information/material' or had been 'self authorised'.

Previous Recommendations

8. The 2003 OSC inspection report contained nine recommendations.
 - (i) A corporate policy on RIPA applicable to all Departments should be introduced as soon as possible.
 - (ii) In that policy care must be taken to remedy the defects in the existing separate policy statements used by the Departments.

Action: Suitable policy has now been published and adopted by all Departments.

RESTRICTED

2

RESTRICTED

(iii) Future training must ensure that the concepts of *necessity* and *proportionality* are fully understood by all staff likely to become involved in covert surveillance.

(iv) It is not advisable for Authorising Officers to grant authorisations without themselves receiving relevant training.

Action: When RIPA was first introduced the then Authorising Officers undertook training on the subject and since then a number have received guidance from attending courses and seminars held by their own professional bodies or the Home Office. In 2006 the entire Anti Social Behaviour Team undertook a five day surveillance training course provided by the Merseyside Police which included RIPA as a component within it. The Applicant from Planning Enforcement has attended no less than three training courses on RIPA and the Trading Standards Manager attended a RIPA Review Stakeholder Forum organised by the Home Office in April of this year. As a result, he is currently working on developing a three day training course for all Enforcement Officers, an element of which will be RIPA. It is hoped that the course will be repeated regularly and will be modular in nature so that the RIPA element could be used as initial training for new Enforcement Officers and also refresher training for existing Officers.

Whilst various initiatives have been introduced, the Council has not adopted a corporate response to these two recommendations. In those applications examined, proportionality is still not described adequately and action plans to minimise collateral intrusion are not protecting innocent members of the public sufficiently. From interviews with Applicants and Authorising Officers, it is apparent that there are still gaps in the training provision and refresher courses are needed. A training needs analysis is long overdue to identify those members of staff requiring either initial or refresher RIPA training. Thereafter the Council should provide this training at a corporate level.

(v) Care must be taken in all future applications for authorisation to ensure that any proposed course of action is fully described in order to avoid the possibility of errors made in *R v Sutherland & Others*.

Action: Applicants are now more fully describing the surveillance activity they wish to carry out but Authorising Officers are not providing a comprehensive statement outlining the activity they are prepared to sanction. Instead they are relying on a pre-printed statement in the now outdated Home Office form which refers to the application for detail. It was pointed out to all Authorising Officers that the latest Home Office model authorisation form requires a number of points to be covered and they were strongly advised to use the form in any future authorisations. This is particularly relevant when outside agencies such as Private Investigators are employed to carry out the surveillance. A comprehensive authorisation statement should be provided to them to ensure their activity is within the parameters set.

(vi) A system of regular reviews of authorisations should be introduced in order to ensure prompt cancellations.

Action: The Council policy requires regular reviews of authorisations to be conducted but none of the authorisations inspected appeared to have been formally

RESTRICTED

3

RESTRICTED

reviewed. In most cases the Authorising Officer failed to record a review date. It is accepted that informal reviews are being conducted, particularly within the Anti Social Behaviour Team which meets with a Solicitor on a weekly basis but the requirements of paragraph 4.21 of the Covert Surveillance Code of Practice are being overlooked, particularly the need to record the results of the review on the central record of authorisations. The Home Office RIPA review form should be taken into use as a matter of urgency. All but one case inspected had been properly cancelled.

(vii) A central record of authorisations should be created in order to comply with the Code of Practice.

Action: A central record is now being maintained but not in full accordance with the Code of Practice. The details contained in paragraph 2.14 are recorded but only on a quarterly basis, thus at any one time it could be significantly outdated. In discussions with Simon Goacher, the Solicitor responsible for its upkeep, the Inspector pointed out the requirement for the record to be regularly updated, whenever an authorisation is granted, renewed or cancelled. Reviews are not being recorded and there is no provision to highlight 'self authorised' cases as required by paragraph 4.14 of the Code.

(viii) An appropriate officer of the Council should be designated as Monitoring Officer for RIPA and be responsible for the maintenance and safe custody of the central record.

Action: The Head of Legal and Member Services has been delegated to carry out this role and a Solicitor in his department conducts the day to day work on his behalf. It is evident that insufficient central monitoring is being conducted, the record should be used more pro-actively to identify critical dates and ensure all the relevant documents are submitted and recorded. At present there is no reporting mechanism to members on the use of RIPA. It is proposed that there be an annual report to the Chief Officers Management Team and Cabinet on the use of RIPA.

(ix) It is good practice to make copies of the Home Office Codes of Practice available at the Council's offices for consultation by members of the public on request.

Action: The Council does not believe that it is likely that members of the public will need to access a paper copy of the Codes of Practice and has not adopted this practice. It has however ensured that all officers who deal with investigations do have copies and this was confirmed during the inspection. It is worthy of note that whilst the interim Codes of Practice advocated this approach, the substantive Codes have not thought it necessary to re-iterate this advice.

9. Whilst the actions taken by the Council have addressed many of the significant issues raised in the previous inspection report, more work needs to be done to fully rectify the previous deficiencies.

RESTRICTED

4

RESTRICTED

SIGNIFICANT ISSUES

10. Central record

The record needs to be regularly updated on a day by day basis rather than the present quarterly arrangement and contain the record of reviews and any self authorised cases. It should be used more pro-actively as a central management tool to ensure full compliance across all departments. There is no corporate system for the issuing of a Unique RIPA Reference Number (URN) to the various documents.

11. Training

A training needs analysis is long overdue to help identify knowledge gaps and a corporate approach to the provision of appropriate training is needed.

12. Directed Surveillance

- Applications are being drafted to a reasonable standard but Applicants are still unaware of the need to properly explain the proportionality of their intended surveillance activity and to provide an action plan to minimise collateral intrusion.
- Applicants within the Anti Social Behaviour Team are mistakenly submitting multiple applications covering a single operation. Typically, if they wish to place a covert video camera watching the front of a particular property and another covering the rear, they are submitting two separate applications and obtaining two authorisations for the same operation. It was pointed out to them that a comprehensive application could cover a multitude of appropriate tactics which the Authorising Officer could then consider within a single authorisation statement. However, they were cautioned against using fresh tactics at a later date which had not been initially authorised.
- Authorising Officers are not providing a comprehensive authorisation statement, relying on the pre printed statement on the now outdated Home Office forms. Effective start and end times are not being recorded.
- Reviews of authorisations are not being called for or documented.
- Ordinary authorisations are being granted for less than the prescribed three months, in some cases one month.
- In one case an authorisation was renewed after it had time expired in contravention of paragraph 4.24 of the Code of Practice.

13. Forms

The Council has recently acquired the latest version of the Home Office forms but has not yet introduced them. The Inspector is satisfied that many of the imperfections found in the earlier applications and authorisations inspected will be corrected by the

RESTRICTED

5

RESTRICTED

use of the new forms because they prompt the author to provide the relevant information.

14. At the commencement of the inspection, the Inspector was courteously welcomed to the Council by Mr Mark Reaney (Head of Legal and Member Services). At the conclusion, it was pleasing that the Chief Executive Mr Stephen Maddox found time in his busy schedule to receive feedback. The Chief Executive was extremely knowledgeable and showed considerable interest in all matters affecting RIPA. The Inspector is grateful for all the facilities made available to him both before and during the inspection by Mr Simon Goacher and for the co-operation and openness of all the staff he met.

RECOMMENDATIONS

15. The Head of Legal and Member Service, 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 (paragraphs 3 and 13).

16. 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 (paragraphs 8(vii), 8(viii) and 10).

17. 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 (paragraphs 8(iv) and 11).

18. The issues and imperfections discovered during this inspection should be included in the curriculum of any future corporate RIPA training event (paragraphs 8(v), 8(vi) and 12).



**Richard Allsopp
Surveillance Inspector**



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 set out exactly how the Council will use its surveillance powers and comply with best practice.
- 1.3 The Council uses cover surveillance to supports 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, 35 in anti-social behaviour case and 9 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 including a local 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.

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. 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;
 - preventing or detecting crime or of preventing disorder;
 - public safety;
 - protecting public health;

- assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; 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 kept to a minimum.
- 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**.

4.4 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.

4.3 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)

4.4 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 CHIS's 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 4. 8 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, oversee 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 1

RIPA CO-ORDINATORS GROUP

Department

Representative

Department of Law, HR and Asset
Management

Simon Goacher

Department of Finance

Malcolm Flanagan

Department of Regeneration

John Malone/Lucy

Pritchard

Department of Technical Services

Phil Black

Department of Children's Services

N/a

Department of Adult Social Services

N/a

Department of Corporate Services

N/a

Appendix 2

RIPA REGISTER OF AUTHORISING AND APPLYING OFFICERS AND TRAINING

Authorising Officers

<u>Department</u>	<u>Officer</u>	<u>Date Appointed</u>	<u>Most Recent Training*</u>
Regeneration	John Malone Caroline Laing Lucy Pritchard		
Finance	David Smith Malcolm Flanagan Stephen Rowley		
Technical Services	Dave Green		

Applying Officers

<u>Department</u>	<u>Officer</u>	<u>Date Appointed</u>	<u>Most Recent Training*</u>
Regeneration	Alison McFarland Jean Booth Andy Pike Andy O'Rourke Carolyn Richley Zhara Jones John Sebborn Louise Alexander Mike O'Brien Andy Bushell		
Finance	Kris Ng		
Technical Services	Lee Walsh		

* - all authorising officers must have received training within the last 2 years

Last updated 19/03/09

Unique Reference Number	
-------------------------	--



Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance

Form RIPADS1

Public Authority <i>(including full address)</i>	Wirral Council, Town Hall, Brighton Street, Wallasey, Wirral. CH44 8ED		
Name of Applicant		Unit/Branch /Division	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

DETAILS OF APPLICATION
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003; No. 3171.¹
2. Describe the purpose of the specific operation or investigation.
3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.
4. The identities, where known, of those to be subject of the directed surveillance.
<ul style="list-style-type: none"> • Name: • Address: • DOB: • Other information as appropriate:
5. Explain the information that it is desired to obtain as a result of the directed surveillance.

¹ For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.

6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA. Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on.(SI 2003 No.3171)

- In the interests of national security;
- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom;
- In the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 2.4]

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 2.6 to 2.10.]

Describe precautions you will take to minimise collateral intrusion

9. Explain why this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means? [Code paragraph 2.5]

10. Confidential information. [Code paragraphs 3.1 to 3.12]

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

Unique Reference Number	
-------------------------	--

11. Applicant's Details.			
Name (print)		Tel No:	
Grade/Rank		Date	
Signature			
12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]			
<p>I hereby authorise directed surveillance defined as follows: [<i>Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?</i>]</p>			
13. Explain <u>why</u> you believe the directed surveillance is necessary. [Code paragraph 2.4] Explain <u>why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. [Code paragraph 2.5]			

Unique Reference Number	
--------------------------------	--

--

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 3.1 to 3.12

--

Date of first review	
-----------------------------	--

Programme for subsequent reviews of this authorisation: [Code paragraph 4.22]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.

--

Name (Print)		Grade / Rank	
---------------------	--	---------------------	--

Signature		Date and time	
------------------	--	----------------------	--

Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59]

Unique Reference Number	
-------------------------	--

15. Urgent Authorisation [Code paragraphs 4.17 and 4.18]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

--

16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer

--

Name (Print)		Grade/ Rank		
Signature		Date and Time		
Urgent authorisation Expiry date:		Expiry time:		
<i>Remember the 72 hour rule for urgent authorities – check Code of Practice.</i>	e.g. authorisation granted at 5pm on June 1 st expires 4.59pm on 4 th June			

This page is intentionally left blank

Unique Reference Number	
-------------------------	--



Part II of the Regulation of Investigatory Powers Act 2000

Review of a Directed Surveillance authorisation

Form RIPADS2

Public Authority <i>(including address)</i>	Wirral Council, Town Hall, Brighton Street, Wallasey, Wirral. CH44 8ED
---	--

Applicant		Unit/Branch /Division	
Full Address			
Contact Details			
Operation Name		Operation Number* <small>*Filing Ref</small>	
Date of authorisation or last renewal		Expiry date of authorisation or last renewal	
		Review Number	

Details of review:

1. Review number and dates of any previous reviews.	
Review Number	Date

2. Summary of the investigation/operation to date, including what private information has been obtained and the value of the information so far obtained.
--

Unique Reference Number	
--------------------------------	--

--

3. Detail the reasons why it is necessary to continue with the directed surveillance.

--

4. Explain how the proposed activity is still proportionate to what it seeks to achieve.

--

5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.

--

6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

--

7. Applicant's Details

Name (Print)		Tel No	
Grade/Rank		Date	

Unique Reference Number	
--------------------------------	--

Signature	
------------------	--

8. Review Officer's Comments, including whether or not the directed surveillance should continue.

9. Authorising Officer's Statement.
I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue [until its next review/renewal][it should be cancelled immediately].
Name (Print) Grade / Rank - - - - -
Signature - - - - - Date - - - - -

10. Date of next review.	
---------------------------------	--

This page is intentionally left blank

Unique Reference Number	
-------------------------	--



Part II of the Regulation of Investigatory Powers Act 2000

Cancellation of a Directed Surveillance authorisation

Form RIPADS3

Public Authority <i>(including full address)</i>	Wirral Council, Town Hall, Brighton Street, Wallasey, Wirral. CH44 8ED
--	--

Name of Applicant		Unit/Branch /Division	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

--

Unique Reference Number	
--------------------------------	--

2. Explain the value of surveillance in the operation:

3. Authorising officer's statement.
--

I, [insert name], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.

Name (Print)

Grade

Signature

Date

4. Time and Date of when the authorising officer instructed the surveillance to cease.

Date:		Time:	
--------------	--	--------------	--

5. Authorisation cancelled.	Date:	Time:
------------------------------------	--------------	--------------

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	
--	--



Part II of the Regulation of Investigatory Powers Act (RIPA) 2000

Application for authorisation of the conduct or use of a Covert Human Intelligence Source (CHIS)

Form RIPACHIS1

Public Authority <i>(including full address)</i>	Wirral Council, Town Hall, Brighton Street, Wallasey, Wirral. CH44 8ED		
Name of Applicant		Service/Department /Branch	
How will the source be referred to? i.e. what will be his/her pseudonym or reference number			
The name, rank or position of the person within the relevant investigating authority who will have day to day responsibility for dealing with the source, including the source's security and welfare. (Often referred to as the Handler)			
The name, rank or position of another person within the relevant investigating authority who will have general oversight of the use made of the source. (Often referred to as the Controller)			
Who will be responsible for retaining (in secure, strictly controlled conditions, with need-to-know access) the source's true identity, a record of the use made of the source and the particulars required under RIP (Source Records) Regulations 2000 (SI 2000/2725)?			

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	
--	--

Investigation/Operation Name (if applicable)	
--	--

DETAILS OF APPLICATION
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2003; No. 3171. ¹ Where appropriate throughout amend references to the Order relevant to your authority.
2. Describe the purpose of the specific operation or investigation.
3. Describe in detail <u>the purpose</u> for which the source will be tasked or used.
4. Describe in detail the proposed covert conduct of the source or <u>how</u> the source is to be used.
5. Identify on which grounds the conduct or the use of the source is <u>necessary</u> under Section 29(3) of RIPA. Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on. (eg. SI 2003 No.3171)

¹ For local authorities: The formal position of the authorising officer should be given. For example, Head of Trading Standards.

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).

- In the interests of national security;
- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom;
- In the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.

6. Explain why this conduct or use of the source is necessary on the grounds you have identified [Code paragraph 2.4]

7. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 2.6 to 2.10.]
Describe precautions you will take to minimise collateral intrusion and how any will be managed.

8. Are there any particular sensitivities in the local community where the source is to be used? Are similar activities being undertaken by other public authorities that could impact on the deployment of the source? (see Code 2.9)

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	
--	--

--

9. Provide an assessment of the risk to the source in carrying out the proposed conduct. (see Code 2.9)

--

10. Explain why this conduct or use of the source is proportionate to what it seeks to achieve. How intrusive might it be on the subject(s) of surveillance or on others? How is this intrusion outweighed by the need for a source in operational terms, and could the evidence be obtained by any other means? [Code paragraph 2.5]

--

**11. Confidential information. [Code paragraphs 3.1 to 3.12]
Indicate the likelihood of acquiring any confidential information.**

--

References for any other linked authorisations:

12. Applicant's Details.

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	
--	--

Name (print)		Grade/Rank/Position	
Signature		Tel No:	
Date			

13. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW – in this and the following box.] THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE, NOT THE TRUE IDENTITY.

--

**14. Explain why you believe the conduct or use of the source is necessary. [Code paragraph 2.4]
 Explain why you believe the conduct or use of the source to be proportionate to what is sought to be achieved by their engagement. [Code paragraph 2.5]**

--

15. (Confidential Information Authorisation.) Supply details demonstrating compliance with Code paragraphs 3.1 to 3.12

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	
--	--

--

16. Date of first review:	
----------------------------------	--

17. Programme for subsequent reviews of this authorisation: [Code paragraphs 4.19 and 4.20]. Only complete this box if review dates after first review are known. If not, or inappropriate to set additional review dates, then leave blank.

--

18. Authorising Officer's Details
--

Name (Print)		Grade/Rank/Position	
Signature		Time and date granted*	
		Time and date authorisation ends	

** Remember, an authorisation must be granted for a 12 month period, i.e. 1700 hrs 4th June 2006 to 2359hrs 3 June 2007*

19. Urgent Authorisation [Code paragraphs 4.17 and 4.18]: Authorising Officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.
--

--

20. If you are entitled to act only in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully designated Authorising Officer
--

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	
--	--

--

21. Authorising Officer of urgent authorisation			
Name (Print)		Grade/Rank/Position	
Signature		Date and Time	
Urgent authorisation expiry date:		Expiry time:	

*Remember the 72 hour rule for urgent authorisations – check Code of Practice [Code Paragraph 4.18].
e.g. authorisation granted at 1700 on 1st June 2006 expires 1659 on 4th June 2006*

This page is intentionally left blank

Unique Operation Reference Number* (*Filing Ref)	
--	--



Part II of the Regulation of Investigatory Powers Act (RIPA) 2000

Review of a Covert Human Intelligence Source (CHIS) authorisation

Form RIPACHIS2

Public Authority <i>(including full address)</i>	Wirral Council, Town Hall, Brighton Street, Wallasey, Wirral. CH44 8ED
--	--

Applicant		Unit/Branch	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Operation Name		Operation Number* <small>*Filing Ref</small>	
Date of authorisation or last renewal		Expiry date of authorisation or last renewal	
		Review Number	

Unique Operation Reference Number* (*Filing Ref)	
---	--

Details of review:

1. Review number and dates of any previous reviews.

Review Number	Date

2. Summary of the investigation/operation to date, including what information has been obtained and the value of the information so far obtained.

--

3. Detail the reasons why it is necessary to continue with using a Covert Human Intelligence Source.

--

4. Explain how the proposed activity is still proportionate to what it seeks to achieve.

--

5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.

--

Unique Operation Reference Number* (*Filing Ref)	
---	--

6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

--

7. Give details of the review of the risk assessment on the security and welfare of using the source.

--

8. Applicant's Details

Name (Print)		Tel No	
Grade/Rank		Date	
Signature			

9. Review Officer's Comments, including whether or not the use or conduct of the source should continue?

--

10. Authorising Officer's Statement. THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE NOT THE TRUE IDENTITY.

--

Name (Print)	Grade / Rank	
Signature	Date	

Unique Operation Reference Number* (*Filing Ref)	
---	--

Date of next review:	
-----------------------------	--

Unique Operation Reference Number* (*Filing Ref)	
--	--



**Part II of the Regulation of Investigatory Powers
Act (RIPA) 2000**

**Cancellation of an authorisation for the use or conduct of a
Covert Human Intelligence Source**

Form RIPACHIS3

Public Authority <i>(including full address)</i>	Wirral Council, Town Hall, Brighton Street, Wallasey, Wirral. CH44 8ED
--	--

Name of Applicant		Unit/Branch	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Investigation/Operation Name (if applicable)			

Unique Operation Reference Number* (*Filing Ref)	
---	--

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

2. Explain the value of the source in the operation:

3. Authorising officer's statement. THIS SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE NOT THE TRUE IDENTITY.

Name (Print)	Grade
Signature	Date

4. Time and Date of when the authorising officer instructed the use of the source to cease.

Date:		Time:	
--------------	--	--------------	--

Unique Operation Reference Number* (*Filing Ref)	
---	--



Part II of the Regulation of Investigatory Powers Act (RIPA) 2000

Application for renewal of a Covert Human Intelligence Source (CHIS) Authorisation

(Please attach the original authorisation)

Form RIPACHIS4

Public Authority <i>(including full address)</i>	Wirral Council, Town Hall, Brighton Street, Wallasey, Wirral. CH44 8ED
--	--

Name of Applicant		Unit/Branch	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Investigation/Operation Name (if applicable)			
Renewal Number			

Details of renewal:

1. Renewal numbers and dates of any previous renewals.

**Unique Operation Reference
Number*** (*Filing Ref)

Renewal Number	Date

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.

3. Detail why it is necessary to continue with the authorisation, including details of any tasking given to the source.

4. Detail why the use or conduct of the source is still proportionate to what it seeks to achieve.

5. Detail the use made of the source in the period since the grant of authorisation or, as the case may be, latest renewal of the authorisation.

Unique Operation Reference Number* (*Filing Ref)	
---	--

--

6. List the tasks given to the source during that period and the information obtained from the conduct or use of the source.

--

7. Detail the results of regular reviews of the use of the source.

--

8. Give details of the review of the risk assessment on the security and welfare of using the source.

--

9. Applicant's Details

Name (Print)		Tel No	
---------------------	--	---------------	--

Unique Operation Reference Number* (*Filing Ref)	
---	--

Grade/Rank		Date	
Signature			

10. Authorising Officer's Comments. <u>This box must be completed.</u>

11. Authorising Officer's Statement. THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE NOT THE TRUE IDENTITY.
--

--

Name (Print)	Grade / Rank
Signature	Date
Renewal From:	Time:
	Date:
	End date/time of the authorisation

NB. Renewal takes effect at the time/date of the original authorisation would have ceased but for the renewal

Date of first review:	
Date of subsequent reviews of this authorisation:	

Acquisition and Disclosure of Communications Data

Guidance for the Layout of a
Chapter II Application Form and
Guidance for Applicants and
Designated Persons Considering
Necessity and Proportionality

HOME OFFICE
November 2007

DATA COMMUNICATIONS GROUP
November 2007

Introduction

This paper has been produced jointly by the Home Office and the Data Communications Group (DCG)*, in consultation with the Interception of Communications Commissioner's Office (IOCCO), to clarify what information should be included in an application for the acquisition of communications data in accordance with the Regulation of Investigatory Powers Act 2000 ("the Act") and the code of practice approved by Parliament under section 71 ("the code").

Where appropriate, the **GUIDANCE** set out in this paper should be included within a public authority's application process to assist applicants and designated persons.

The layout of this specimen document is for a paper based administration and has been prepared in **Microsoft Word 2002** using **Verdana** text.

Sections of the form can be amended to suit the working practice of the public authority whether managed on paper or on a database. However, changes must be in accordance with the Act and the code.

If you are viewing the specimen form in something other than Microsoft Word 2002, the colours and pagination may differ from the original.

*The Data Communications Group comprises representatives of ACPO, ACPO(S), HMRC, SOCA, other public authorities and senior members of communication service providers and their trade associations.

Application

An application, comments by the single point of contact (SPoC), considerations of the designated person, authorisations and notices may be made in writing (“paper”) or electronically (“database”).

Insert name of your public authority here

Chapter II of Part I of the Regulation of Investigatory Powers Act 2000

Application for Communications Data

1) Applicant's Name		4) Unique Reference Number	
2) Office, Rank or Position		5) Applicant's Telephone Number	
3) Applicant's Email Address		6) Applicant's Fax Number	
7) Operation Name (if applicable)		8) STATUTORY PURPOSE	
		Click here for options:-	

Subject to the restrictions upon public authorities, the Statutory Purposes for which communications data can be required are as follows (see paragraph 2.2 of the code);

- In the interests of National Security S22 (2)(a)
- For the prevention and detection of crime or preventing disorder S22 (2)(b)
- Economic well being of the United Kingdom S22 (2)(c)
- In the interests of public safety S22 (2)(d)
- For the purpose of protecting public health S22 (2)(e)
- For the purpose of assessing or collecting tax, duty levy or other imposition, contribution of charge payable to a government department S22 (2)(f)
- For the purpose, in an emergency, of preventing death or injury or damage to a persons physical or mental health or of mitigating any injury or damage to a persons physical or mental health S22 (2)(g)
- To assist investigations into alleged miscarriages of justice Article 2(a)
- For the purpose of assisting in identifying any person who has died otherwise than as a result of crime or who is unable to identify himself because of a physical or mental condition, other than one resulting from crime Article 2(b)(i)

- For the purpose of obtaining information about the next of kin or other connected persons of such a person or about the reason for his death or condition Article 2(b)(ii)

The police may use all the statutory purposes listed except for S22 (f) and Article 2(a).

Some of the statutory purposes have restrictions as to when it may be appropriate to use them (see footnotes 13, 14 and 15 of the code)

The drop down menu **STATUTORY PURPOSE** has been drafted for police use - other public authorities must amend the drop down menu appropriate to the statutory purposes permitted for their authority.

There is a restriction on the acquisition of communications data for S22 (d), S22 (e) & S22 (f). Only communications data within the meaning of S21 (4) (c) may be acquired for these purposes (see paragraph 2.3 and 2.4 of the code).

9) COMMUNICATIONS DATA

Describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s)

This text box can be made bigger or smaller, it is not set out to indicate how much should be written

It may be appropriate for the section **COMMUNICATIONS DATA** to include 'text boxes' to enable the applicant to set out the:

- telephone number, email address, etc;
- where appropriate the 'between times / dates' of the data set required;
- type of data required, for example subscription details, outgoing calls, incoming calls.

An application may contain several requests for various 'data sets' relating to a specific investigation or operation. However, consideration should be given as to how this may affect the efficiency of the public authority's processes and the impact of managing disclosure issues before, during and after a criminal trial.

10) NECESSITY

State the nature of the investigation or operation and how it relates to a purpose at question 8

Give a short explanation of the crime (or other purpose), the suspect, victim or witness and the phone or communications address and how all these three link together.

This text box can be made bigger or smaller, it is not set out to indicate how much should be written

GUIDANCE

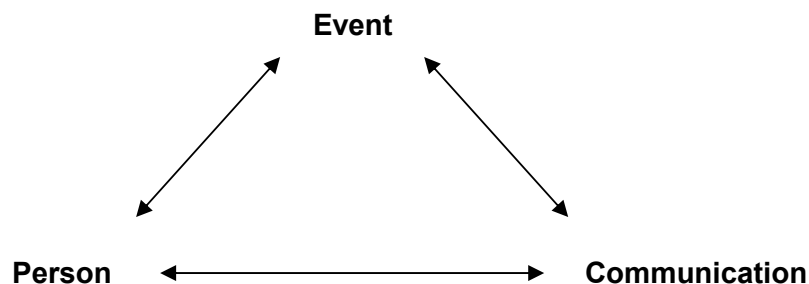
NECESSITY – In order to justify the application is necessary the applicant needs to cover three main points:

- crime / offence / circumstances (“the **event**”) under investigation;
- suspect(s) / offender(s) / witness(es) / victim(s) (“the **person**”) and how the person(s) is/are linked to the event;
- telephone number(s), IP Address(es) etc (“the **communication**”) and how this/these relate or link the person and the event.

Sensitive sources of intelligence or covert investigation techniques may be referred to in the application but the applicant must be mindful of the appropriate security handling of the application once completed. It may be sufficient to refer to an intelligence reference number within the body application dependant on the security issues involved.

The information given by the applicant (which includes ‘background information’ or the ‘intelligence case’) should be set out within an application under the headings of **Necessity** and **Proportionality** (which includes the consideration of meaningful collateral intrusion). This will minimise the need to repeat information within an application and enable the process to be streamlined.

In essence, necessity should be a short explanation of the a) **event**, b) the **person** and c) the **communication** and how these three link together.



The applicant must establish a link (which may, where justified, include an inferential link) between the three aspects to be able to demonstrate the acquisition of communications data is necessary for the statutory purpose specified.

A brief description of the investigation or operation may assist the designated person better understand the reason for the application.

In a long term or complex investigation or operation it is important to set the application in context with the overall investigation or operation and set the scene and background, which then leads into the applicant's specific investigative or operational requirements (which should be covered in the proportionality section).

Necessity does not entail explaining, 'what will be achieved by acquiring the data' or 'why specific time periods have been requested' – these points are relevant to proportionality and should be covered in the relevant section to stop repetition.

11) PROPORTIONALITY

State why obtaining the communications data is proportionate to what you are seeking to achieve

Outline what is expected to be achieved from obtaining the data and explain how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. When considering the benefits to the investigation or operation, can the level of intrusion be justified against the individual's right to privacy? Explain why you have requested the specific date/time periods i.e. how these are proportionate.

This text box can be made bigger or smaller, it is not set out to indicate how much should be written

12) COLLATERAL INTRUSION

Consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the privacy of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances

If you have identified any meaningful degree of collateral intrusion, explain what it is.

This text box can be made bigger or smaller, it is not set out to indicate how much should be written

GUIDANCE

PROPORTIONALITY - Applicants should outline how obtaining the data will benefit the investigation or operation. The two basic questions:

- “What are you looking for within the data to be acquired?”
- “If the data contains what you are looking for, what will be your next course of action?”

The relevance of any time periods requested must be explained outlining how these periods are proportionate to the event under investigation.

An explanation as to how communications data will be used, once acquired, and how it will benefit the investigation or operation will enable the applicant to set out the basis of proportionality.

An investigation or operation which is seeking to acquire several sets of traffic data or service use data should engage with the SPoC to develop strategies (or collection plans) to obtain the communications data and the detail of that strategy may be included within the application (see paragraph 3.17 of the code).

COLLATERAL INTRUSION forms part of the **PROPORTIONALITY** considerations and becomes increasingly relevant when applying for traffic data or service use data and applicants should outline specifically what collateral intrusion may occur, how the time periods requested impact on the collateral intrusion, whether they are likely to obtain data which is outside the realm of their investigation and outline their plans for managing it, for example during the course of an investigation and to establish certain facts it may be necessary and proportionate for an investigator (applicant) to require access to communications data that relates to witnesses as well as the associates of a suspect or target.

The question to be asked is, "Will the data set to be acquired result in collateral intrusion to persons outside the line of enquiry the data is being obtained for? For example, due to the very specific nature of telephone subscriber check/s, collateral intrusion on a person other than the subscriber detail/s will be consistently absent whereas itemised billing on the subject's family home will be likely to contain calls made by the family members.

Applicants should not write about a potential or hypothetical 'error' and if the applicant can not identify any meaningful collateral intrusion that factor should be recorded in the application i.e. "none identified".

13) TIMESCALE	
----------------------	--

Identify and explain the timescale within which the data is required	
---	--

GUIDANCE

TIME SCALE - Completion of this section assists the SPoC to prioritise the request.

DCG has an agreed Grading System that indicates to the CSP any urgent timescales, which is synchronised with the Urgent Oral Process (see footnote 40 and paragraph 3.56 of the code).

14) APPLICANT

I undertake to inform the SPoC of any change in circumstances that no longer justifies the acquisition of the data

Applicant's Signature		Date	
----------------------------------	--	-------------	--

GUIDANCE

If the application is being recorded within a database (or other electronic format), and is attributable to the applicant, a signature is not required.

Considerations of the SPoC

An application, comments by the single point of contact (SPoC), considerations of the designated person, authorisations and notices may be made in writing (“paper”) or electronically (“database”).

15) ASSESSMENT BY ACCREDITED SPoC.	
How much will the acquisition of the data cost?	
Are there other factors the DP should be aware of? <i>For example, the requirement:</i> <ul style="list-style-type: none"> • <i>is NOT reasonably practical for the CSP to do;</i> • <i>will cause an adverse cost or resource implication to either your public authority or the CSP (for instance does the investigation or operation have the analytical capacity to undertake analysis of the communications data once acquired);</i> • <i>will produce excess data to that required.</i> 	
Name of Accredited SPoC	

16) AUTHORISATION (Completed by Accredited SPoC when appropriate)	
Specify the reason why the collection of communications data by means of an authorisation is appropriate:	
<input type="checkbox"/> There is an agreement in place between the public authority and the CSP relating to the appropriate mechanisms for the disclosure of the data ◆	
<input type="checkbox"/> The designated person considers there is a requirement to identify to whom a service is provided (for example subscriber check) but a CSP has yet to be conclusively determined as the holder of the communications data ◆	
<input type="checkbox"/> CSP is not capable of obtaining or disclosing the communications data ▲	
Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought.*	
Describe the course of conduct required to obtain the data.	<input type="checkbox"/> ◆ Traffic or Service Use data – acquisition by SPoC directly from CSP <input type="checkbox"/> ◆ Subscriber Information – acquisition by SPoC or, where SPoC can not acquire data directly from CSP, serve assurance of the Authorisation on CSP ¹ <input type="checkbox"/> ▲ Other conduct – specify
<i>The statutory purpose for which the conduct may be authorised is set out at section 8 of this form.</i> <i>The office, rank or position of the designated person should be recorded within section 17 of this form together with a record of the date & time the granting of an authorisation is made.</i>	

*The question, “Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought”, is appropriate where

¹ See paragraph 3.30 of the code

the communications data sought by the applicant may need refinement by the SPoC, for example incoming calls to a telephone number held by a CSP that does not keep a data set that can reveal such calls. The SPoC would state that several Authorisations and Notices will need to be undertaken with CSPs that can reveal calls instigating from their networks to the telephone number in question.

The designated person, having considered the comments of the SPoC, may decide the acquisition is not justified because of the significant resources required by the CSP to retrieve and disclose the data or it will be impractical for the public authority to undertake an analysis of the data.

It will also be appropriate for the SPoC to comment where the data sought by the applicant will require the acquisition of excess data, specifically where it is not practicable for the CSP to edit or filter the data, for example a specific incoming call in a data set with outgoing calls and cell site contained in it. If the designated person considers this to be necessary and proportionate for the acquisition of the specific incoming call then the Authorisation or Notice must specifically include the acquisition of the outgoing call, incoming calls and cell site.

Considerations of the Designated Person

An application, comments by the single point of contact (SPoC), considerations of the designated person, authorisations and notices may be made in writing (“paper”) or electronically (“database”).

17. DESIGNATED PERSON			
<p>The designated person considers the application and if approved records their considerations:</p> <ul style="list-style-type: none"> • Why do you believe acquiring the communications data is necessary for one of the purposes within section 22(2) of the Act; • Why do you believe the conduct involved in obtaining the data is proportionate to the objective(s)? In making that judgement you should take in consideration any additional information from the SPoC. If the applicant has identified any <u>meaningful degree of collateral intrusion</u>, why you believe the request remains justified and proportionate to the objective(s)? 			
<p>My considerations in approving / not approving this application are:</p> <p><i>This text box can be made bigger or smaller, it is not set out to indicate how much should be written</i></p>			
<p><input type="checkbox"/> I authorise the conduct to be undertaken by the SPoC as set out in section 16 of this form.</p> <p><input type="checkbox"/> I give Notice and require the SPoC to serve it on (insert name of CSP) . The Notice* bears the unique reference number</p>			
Name		Office, Rank or Position	
Signature		Time and Date	

GUIDANCE

The **DESIGNATED PERSON** must be able to show he or she has understood the need for the application and considered necessity and proportionality to a standard that will withstand scrutiny.

The designated person should tailor their comments to a specific application as this best demonstrates the application has been properly considered.

If the designated person having read the application considers the applicant has met all the requirements then he or she should simply record that fact. In such cases a simple note by the designated person should be recorded.

There may be circumstances where the designated person having read the case set out by the applicant and the considerations of the SPoC will want to comment why it is still necessary and proportionate to obtain the data despite excessive data being acquired.

If the designated person does not consider the case for obtaining the data has been met the application should be rejected and referred back to the SPoC and the applicant.

*A Notice must include a unique reference number that also identifies the public authority. This can be a code or an abbreviation. For police services it will be appropriate to use the Police National Computer (PNC) force coding. See also paragraph 3.37 (and footnote 53) of the code.

If the designated person is recording their considerations within a database (or other electronic format) and is attributable to the designated person, a signature is not required.

WIRRAL COUNCIL

CORPORATE SERVICES OVERVIEW AND SCRUTINY COMMITTEE - 02 APRIL 2009

REPORT OF THE DIRECTOR OF LAW, HR AND ASSET MANAGEMENT

BUILDING MAINTENANCE

1. EXECUTIVE SUMMARY

1.1 The purpose of this report is to advise Members of the Committee of the current situation regarding the repair and maintenance of the Council's building stock.

2. Background

2.1 At its meeting on 5th March 2009, it was resolved that an extra meeting of the Committee be arranged prior to the 9th April Cabinet, to consider 2 issues.

1. The Regulation of Investigatory Powers Act
2. Building Maintenance

This report deals with the latter topic.

3. Building Maintenance

3.1 At its meeting on 19th March 2009, the Cabinet received a report regarding Property Performance Management.

3.2 That report referred to the attached Appendix and advised that the number of buildings surveyed has been increased from 148 in 2007/08 to 387 in 2008/09. The total maintenance backlog, in respect of structural elements only (not mechanical and electrical) is now approximately £5.8 million. As a rule of thumb guide, where £6 of expenditure is needed on structural repairs, a further £4 is likely to be required to address mechanical and electrical repairs.

3.3 In the corresponding report to Cabinet on 13 March 2008, the total maintenance backlog figure, including M & E costs, was estimated to be £9.89 million. There are only a handful of additional properties to be surveyed and once that information is included, the figures now reported will confirm this estimate, based on more detailed and accurate information.

4. Financial implications

4.1 Building Maintenance is financed from the Planned Preventative Maintenance Budget and the Capital Programme.

5. Staffing implications

5.1 None

6. Equal Opportunities implications

6.1 None

7. Community Safety implications

7.1 None

8. Local Agenda 21 implications

8.1 None

9. Planning implications

9.1 None

10. Anti-poverty implications

10.1 None

11. Human Rights implications

11.1 None

12. Social Inclusion implications

12.1 None

13. Local Member Support implications

13.1 This will be relevant to all Members who have Council Assets in their wards.

14. Background Papers

14.1 None

15. RECOMMENDATION

15.1 That the report be noted.

Bill Norman

Director of Law, HR and Asset Management

Appendix 2

NUMBER	P.M.I A, B, C & D: CONDITION & REQUIRED MAINTENANCE (National Indicator)	2007-2008 (Based on 148 Condition Surveys)	2008-2009 (Based on 387 Condition Surveys)
OBJECTIVE	<p>To measure the condition of the asset for it's current use</p> <p>To measure changes in condition</p> <p>To measure the annual spend on required maintenance</p>		
INDICATOR: A	% Gross internal floor space in condition categories A - D	<p>Condition Category A – 68%</p> <p>Condition Category B – 15%</p> <p>Condition Category C – 17%</p> <p>Condition Category D – 0%</p>	<p>Condition Category A – 16%</p> <p>Condition Category B – 64%</p> <p>Condition Category C – 8%</p> <p>Condition Category D – 12%</p>
B	<p>Required maintenance by cost expressed:</p> <p>i) as total cost in priority levels 1 – 3</p> <p>ii) as a % in priority levels 1 – 3</p> <p>iii) overall cost per square meter GIA</p>	<p>i) Priority Level 1 - £217,015</p> <p>Priority Level 2 - £855,256</p> <p>Priority Level 3 - £2,023,469</p> <p>Total Cost Priority Level 1-3 £2,023,469</p> <p>ii) Priority Level 1 – 7%</p> <p>Priority Level 2 – 28%</p> <p>Priority Level 3 – 65%</p> <p>iii) £16.21 per square meter GIA</p>	<p>i) Priority Level 1 - £427,011</p> <p>Priority Level 2 - £2,149,219</p> <p>Priority Level 3 - £3,257,793</p> <p>Total Cost Priority Level 1-3 £5,834,024</p> <p>ii) Priority Level 1 – 7%</p> <p>Priority Level 2 – 37%</p> <p>Priority Level 3 – 56%</p> <p>iii) £2.81 per square meter GIA</p>

This page is intentionally left blank