Policy and Procedures for undertaking Directed Covert Surveillance and the use of Covert Human Intelligence Sources and Communications Data acquisition for the prevention and detection of crime or the prevention of disorder.

Regulation of Investigatory Powers Act 2000 (RIPA) Corporate Policy

Version Control Sheet

Title:	RIPA and non-RIPA Policy for Castle Point Borough Council
Purpose:	To advise staff of the procedures and principles to follow to comply with the RIPA Act 2000 and for non-RIPA activities.
Author:	Jason Bishop
Owner:	Jason Bishop: Solicitor to the Council/ Head of Legal Services
Approved by:	Version 3 approved by Investigatory Powers Commissioner's Office.
Date:	24 April 2020
Version Number:	3.0
Status:	Approved.
Review Frequency:	Biennially
Next review date:	2022

Contents:

Appendices:

Any enquiries about this policy should be referred to Jason Bishop, Solicitor to the Council/Head of Legal Services on 01268 882462.

A. Introduction

The performance of certain investigatory functions of Local Authorities may require the surveillance of individuals or the use of covert human intelligence sources. Such actions may intrude on the privacy of individuals and can result in private information being obtained and as such, should not be undertaken lightly or without full and proper consideration. Legislation governs how Local Authorities should administer and record surveillance and the use of intelligence sources/ undercover officers and which renders evidence obtained lawful for all purposes. This Policy sets out the Council's rules and procedures.

The purpose of this Policy is to ensure that there is a consistent approach to the undertaking and authorisation of surveillance activity in Castle Point Borough Council's area. Therefore, this Policy is to be used by all Council service areas and officers undertaking investigation work using these techniques of surveillance or the use of Covert Human Intelligence Sources (CHIS's). Where such work is outsourced to other partner authorities, enquiries should be made to ensure that the partner local authority has in place a suitable RIPA policy.

1. A brief overview of RIPA

(For text in **bold**, see glossary of terms – Appendix 1)

The Regulation of Investigatory Powers Act (the Act) was introduced by Parliament in 2000. The Act sets out the reasons for which the use of **directed surveillance** (DS) and **covert human intelligence source** (CHIS) may be authorised.

Local Authorities' abilities to use these investigation methods are restricted in nature and may only be used for the prevention and detection of crime or the prevention of disorder. Local Authorities are not able to use **intrusive surveillance.**

Widespread, and often misinformed, reporting led to public criticism of the use of surveillance by some Local Authority enforcement officers and investigators. Concerns were also raised about the trivial nature of some of the 'crimes' being investigated. This led to a review of the legislation and ultimately the introduction of the Protection of Freedoms Act 2012 and the RIPA (Directed Surveillance and CHIS) (Amendment) Order 2012 (Appendix 2).

In addition to defining the circumstances when these investigation methods may be used, the Act also directs how applications will be made and how, and by whom, they may be approved, reviewed, renewed, cancelled and retained.

The Act must be considered in tandem with associated legislation including the Human Rights Act (HRA) (Appendix 3), and the Data Protection Act (DPA) (Appendix 4).

The purpose of Part II of the Act is to govern the use of directed covert surveillance or covert human intelligence sources. As a public authority, Castle Point Borough Council, has the ability to lawfully infringe the rights of individuals of Castle Point, provided that it does so in accordance with the rules, which are contained within Part II of the Act. Should the Council not follow the rules, the authority loses the impunity otherwise available to it. This impunity may be a defence to a claim for damages or a complaint to supervisory bodies, or as an answer to a challenge to the admissibility of evidence in a trial.

Further, a Local Authority may only engage the Act when performing its 'core functions'. For example, a Local Authority may rely on the Act when conducting a criminal investigation as this would be considered a 'core function', whereas the disciplining of an employee would be considered a 'non-core' or 'ordinary' function.

Some examples of when local authorities may use RIPA and CHIS are as follows:

- Trading standards, including action taken against loan sharks and rogue traders, consumer scams, sale of counterfeit goods, unsafe toys and electrical goods.
- Environmental health, including action against large-scale waste dumping, dangerous workplaces, pest control and the sale of unfit food.
- Benefit fraud, including action to counter fraudulent claims for housing benefits, investigating 'living together' and 'working whilst in receipt of benefit' allegations and council tax evasion.
- Local authorities are also responsible for tackling issues as diverse as anti-social behaviour, unlicensed gambling, threats to children in care, underage employment and taxi regulation.

The examples do not replace the key principles of necessity and proportionality or the advice and guidance available from the relevant oversight Commissioners. **The offences must be in accordance with the Crime Threshold mentioned below.**

2. Directed Surveillance

This policy relates to all staff directly employed by Castle Point Borough Council when conducting relevant investigations for the purposes of preventing and detecting crime or preventing disorder, and to all contractors and external agencies that may be used for this purpose as well as to those members of staff tasked with the authorisation and monitoring of the use of directed surveillance, CHIS and the acquisition of communications data.

The policy will be reviewed biennially or whenever changes are made to relevant legislation and codes of practice.

It is essential that the Chief Executive, or Head of Paid Service, together with the Directors and the Heads of Service should have an awareness of the basic requirements of RIPA and an understanding of how it might apply to the work of individual Castle Point Borough Council departments. Without this knowledge at senior level, it is unlikely that any authority will be able to develop satisfactory systems to deal with the legislation. Those who need to use, or conduct directed surveillance or CHIS on a regular basis will require more detailed specialised training (IPCO – Investigatory Powers Commissioner's Office).

The use of directed surveillance or a CHIS must be necessary and proportionate to the alleged crime or disorder. Usually, it will be considered to be a tool of last resort, to be used only when all other less intrusive means have been used or considered.

Necessary

A person granting an authorisation for directed surveillance must consider *why* it is necessary to use covert surveillance in the investigation *and* believe that the activities to be authorised are necessary on one or more statutory grounds. The statutory grounds are, if it is necessary;

a) in the interests of national security;

b) for the purpose of preventing or detecting crime or of preventing disorder;

c) in the interests of the economic well-being of the United Kingdom;

d) in the interests of public safety;

e) for the purpose of protecting public health;

f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

g) for any purpose (not falling within paragraphs (a) to (f)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

As a local Authority we are only able to proceed with a RIPA Application on the basis of point (b) above.

If the activities are deemed necessary, the authoriser must also believe that they are proportionate to what is being sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

Proportionate

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity

should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

Castle Point Borough Council will conduct its directed surveillance operations in strict compliance with the DPA principles and limit them to the exceptions permitted by the HRA and RIPA, and solely for the purposes of preventing and detecting crime or preventing disorder.

The **Senior Responsible Officer** (SRO) (as named in Appendix 5) will be able to give advice and guidance on this legislation. The SRO will appoint a **RIPA Coordinating Officer** (RCO) (as named in Appendix 5) The RCO will be responsible for the maintenance of a **central register** that will be available for inspection by the (IPCO) – Investigatory Powers Commissioner's Office. The format of the central register is set out in Appendix 6.

The use of hand-held cameras and binoculars can greatly assist a directed surveillance operation in public places. However, if they afford the investigator a view into private premises that would not be possible with the naked eye, the surveillance becomes intrusive and is not permitted. Best practice for compliance with evidential rules relating to photographs and video/CCTV footage is contained in Appendix 8. Directed surveillance may be conducted from private premises. If they are used, the applicant must obtain the owner's permission, in writing, before authorisation is given. If a prosecution then ensues, the applicant's line manager must visit the owner to discuss the implications and obtain written authority for the evidence to be used. (See R v Johnson (Kenneth) 1988 1 WLR 1377 CA (Appendix 10).

The general usage of Castle Point Borough Council's CCTV system is not affected by this policy. However, if cameras are specifically targeted for the purpose of directed surveillance, a RIPA authorisation must be obtained.

Wherever knowledge of **confidential information** is likely to be acquired or if a vulnerable person or juvenile is to be used as a CHIS, the authorisation must be made by the Chief

Executive, who is the Head of Paid Service (or in their absence whoever deputises for this role).

Directed surveillance that is carried out in relation to a **legal consultation** on certain premises will be treated as intrusive surveillance, regardless of whether legal privilege applies or not. These premises include prisons, police stations, courts, tribunals and the premises of a professional legal advisor. Local Authorities are not able to use intrusive surveillance. Operations will only be authorised when there is sufficient, documented, evidence that the alleged crime or disorder exists and when directed surveillance is considered to be a necessary and proportionate step to take in order to secure further evidence.

Low level surveillance, such as a 'drive-by' or everyday activity observed by officers in the course of their normal duties in public places, does not need RIPA authority. If surveillance activity is conducted in immediate response to an unforeseen activity, RIPA authorisation is not required. However, if repeated visits are made for a specific purpose, authorisation may be required. In cases of doubt, legal advice should be taken.

When vehicles are being used for directed surveillance purposes, drivers must always comply with relevant traffic legislation.

Collateral Intrusion

The authorising officer should also consider the risk of intrusion into the privacy of persons other than those who are directly the subject of the investigation (collateral intrusion). Measures should be taken to avoid any unnecessary intrusion into the lives of those not directly connected with the investigation or operation. Castle Point Borough Council may not engage in 'intrusive' surveillance i.e. no surveillance of the inside of residential areas of any premises. Regular reviews of authorisations shall be undertaken to assess the need for the surveillance to continue. Particular attention is drawn to the need to review authorisations frequently where the surveillance involves collateral intrusion.

The person applying for authorisation and the authorising officer must consider the necessity for the use of the tactic, the proportionality of the investigation and the collateral intrusion on any individual's private life, against the need for the activity.

Measures should be taken, wherever practicable, to avoid or minimise interference with the private and family life of those who are not the intended subjects of the investigation. Where such collateral intrusion is unavoidable, the activities may still be authorised providing this collateral intrusion is considered proportionate to the intended aims of authorised activity. Any collateral intrusion should be kept to the minimum necessary to achieve the objective(s) of the operation or investigation.

All applications should therefore include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the authorising officer to fully consider the proportionality of the proposed actions.

Crime Threshold

An additional barrier to authorising directed surveillance is set out in the Regulation of Investigatory Powers (Directed Surveillance and CHIS) (Amendment) Order 2012. This provides a 'Crime Threshold' whereby only crimes which are either punishable by a maximum term of at least 6 months' imprisonment (whether on summary conviction or indictment) or are related to the underage sale of alcohol or tobacco can be investigated through Directed Surveillance.

The crime threshold applies only to the authorisation of directed surveillance by local authorities under RIPA, not to the authorisation of local authority use of CHIS or their acquisition of CD. The threshold came into effect on 1 November 2012.

Castle Point Borough Council cannot authorise directed surveillance under RIPA 2000 for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment. Non-RIPA processes are considered in appendix 11.

Castle Point Borough Council may therefore continue to authorise use of directed surveillance in more serious cases so long as the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a Magistrate has been granted. Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more could include more serious criminal damage, dangerous waste dumping and serious or serial fraud.

For example, an offence which only allows a maximum sentence of 3 months custody cannot be investigated using RIPA authorisation. However, if the offence allows a maximum sentence of 6 months in custody this can be investigated using RIPA.

Castle Point Borough Council may also continue to authorise the use of directed surveillance for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the necessity and proportionality test is met and prior approval from a Magistrates' Court has been granted.

A local authority such as Castle Point Borough Council may not authorise the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences. Non-RIPA processes are considered in appendix 11.

3. Covert Human Intelligence Sources (CHIS)

A person who reports suspicion of an offence is not a CHIS, nor do they become a CHIS if they are asked if they can provide additional information, e.g. details of the suspect's vehicle or the time that they leave for work. It is only if they establish or maintain a personal relationship with another person for the purpose of covertly obtaining or disclosing information that they become a CHIS.

If it is deemed unnecessary to obtain RIPA authorisation in relation to the proposed use of a CHIS for test purchasing, the applicant should complete Castle Point Borough Council's CHIS form and submit to an Authorising Officer for authorisation. Once authorised, any such forms must be kept on the relevant investigation file, in compliance with the Criminal Procedure for Investigations Act 1996 ("CPIA").

The times when a local authority will use a CHIS are limited. The most common usage is for test-purchasing under the supervision of suitably trained officers.

Officers considering the use of a CHIS under the age of 18, and those authorising such activity must be aware of the additional safeguards identified in The Regulation of Investigatory Powers (Juveniles) Order 2000 and its Code of Practice.

A vulnerable individual should only be authorised to act as a CHIS in the most exceptional circumstances. A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness, and who is or may not be able to take care of himself. The Authorising Officer in such cases must be the Chief Executive, who is the Head of Paid Service, or in their absence whoever deputises for this role.

Any deployment of a CHIS should take into account the safety and welfare of that CHIS. Before authorising the use or conduct of a CHIS, the authorising officer should ensure that an appropriate bespoke risk assessment is carried out to determine the risk to the CHIS of any assignment and the likely consequences should the role of the CHIS become known. This risk assessment must be specific to the case in question. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset.

A CHIS handler is responsible for bringing to the attention of a CHIS controller any concerns about the personal circumstances of the CHIS, insofar as they might affect the validity of the risk assessment, the conduct of the CHIS, and the safety and welfare of the CHIS.

The process for applications and authorisations have similarities to those for directed surveillance but there are also significant differences, namely that the following arrangements must be in place at all times in relation to the use of a CHIS:

- There will be an appropriate officer of Castle Point Borough Council who has day-today responsibility for dealing with the CHIS, and for the security and welfare of the CHIS; and

- There will be a second appropriate officer of the use made of the CHIS, and who will have responsibility for maintaining a record of this use. These records must also include information prescribed by the Regulation of Investigatory Powers (Source Records) Regulations 2000. Any records that disclose the identity of the CHIS must not be available to anyone who does not have a need to access these records.

An Authorising Officer's Aide-Memoire has been produced to assist Authorising Officers when considering applications for directed surveillance.

Public authorities should ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing individual officers acting as 'controller' and 'handler' for each CHIS (as defined in sections 29(4A) and (4B) and 29(5)(a) and (b) of the 2000 Act).

The person referred to in section 29(5)(a) of the 2000 Act (the "handler") will have day to day responsibility for:

- dealing with the CHIS on behalf of the authority concerned;
- directing the day to day activities of the CHIS;
- recording the information supplied by the CHIS; and
- monitoring the CHIS's security and welfare.

The person referred to in section 29(5)(b) of the 2000 Act (the "controller") will normally be responsible for the management and supervision of the "handler" and general oversight of the use of the CHIS.

Detailed records must be kept of the authorisation and use made of a CHIS. Section 29(5) of the 2000 Act provides that an authorising officer must not grant an authorisation for the use or conduct of a CHIS unless they believe that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS. The Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No: 2725 details the particulars that must be included in these records. Where a CHIS is authorised under the terms of a Police Act 1996 collaboration agreement, that agreement should explicitly state on which force or agency's central record the authorisation should be recorded. This is likely to be either the force or agency providing the authorising officer, or the designated lead force or agency. The fact that the authorisation was given under these terms should be recorded on the central record.

4. The Authorisation Process

The processes for applications and authorisations for CHIS are similar as for directed surveillance, but note the differences set out in the CHIS section above. Directed Surveillance applications and CHIS applications are made using forms that have been set up in a shared network drive by Castle Point Borough Council. These forms must not be amended, and applications will not be accepted if the approved forms are not completed.

The authorisation process involves the following steps:

Investigation Officer

A risk assessment will be conducted by the Investigation Officer before an application is drafted. This assessment will include the number of officers required for the operation; whether the area involved is suitable for directed surveillance; what equipment might be necessary, health and safety concerns of all those involved and affected by the operation and insurance issues. Particular care must be taken when considering surveillance activity close to schools or in other sensitive areas. If it is necessary to conduct surveillance around school premises, the applicant should inform the head teacher of the nature and duration of the proposed activity, in advance. A Police National Computer Records (PNC) check on those targets should be conducted as part of this assessment by the Counter Fraud & Investigation team or the Safer Communities Officer.

The Investigation Officer prepares an application. When completing the forms, Investigation Officers must fully set out details of the covert activity for which authorisation is sought to enable the Authorising Officer to make an informed judgment. Consideration should be given to consultation with a member of the Legal Department concerning the activity to be undertaken (including scripting and tasking).

The Investigation Officer will obtain a unique reference number (URN) from the central register before submitting an application.

The Investigation Officer will submit the application form to an authorising officer for approval (see Appendix 5).

All applications to conduct directed surveillance (other than under urgency provisions – see below) must be made in writing in the approved format.

Authorising Officer (AO)

The AO considers the application and if it is considered complete the application is signed off and forwarded to the SRO for review and counter approval.

An Authorising Officer's Aide-Memoire has been produced to assist AO's when considering applications for directed surveillance.

If there are any deficiencies in the application further information may be sought from the Investigation Officer, prior to sign off.

Once final approval has been received from the SRO (see below), the AO and the Investigation Officer will retain copies and will create an appropriate diary method to ensure that any additional documents are submitted in good time.

Senior Responsible Officer (SRO)

The SRO then reviews the AO's approval and countersigns it.

If the application requires amendment the SRO will return this to the AO for the necessary revisions to be made prior to sign off. Once the SRO is satisfied that concludes the internal authorisation procedure and he or she will countersign the application.

Application to Justice of the Peace/Magistrates' Court

The countersigned application form will form the basis of the application to the Justice of the Peace/Magistrates' Court (see further below)

Authorised Activity

Authorisation takes effect from the date and time of the approval from the Justice of the Peace/Magistrates' Court.

Notification of the operation will be made to the relevant police force intelligence units where the target of the operation is located in their force area. Contact details for each force intelligence unit are held by the Group Manager Counter Fraud & Investigation - Counter Fraud & Investigation team or the Safer Communities Officer.

Before directed surveillance activity commences, the Investigation Officer will brief all those taking part in the operation. The briefing will include details of the roles to be played by each officer, a summary of the alleged offence(s), the name and/or description of the subject of the directed surveillance (if known), a communications check, a plan for discontinuing the operation and an emergency rendezvous point. A copy of the briefing report (Appendix 7) will be retained by the Investigation Officer.

Where 3 or more officers are involved in an operation, officers conducting directed surveillance will complete a daily log of activity an example shown at Appendix 9. Evidential notes will also be made in the pocket notebook of all officers engaged in the operation

regardless of the number of officers on an operation. These documents will be kept in accordance with the appropriate retention guidelines and Criminal Procedure and Investigations Act 1996 (CPIA).

Where a contractor or external agency is employed to undertake any investigation on behalf of Castle Point Borough Council, the Investigation Officer will ensure that any third party is adequately informed of the extent of the authorisation and how they should exercise their duties under that authorisation.

Conclusion of Activities

As soon as the authorised activity has concluded the Investigation Officer will complete a Cancellation Form.

The original document of the complete application will be retained with the central register.

5. SRO Review and Sign Off

The SRO will review the AO approval prior to it being submitted for Magistrates'/JP authorisation.

If in the SRO's opinion there are inconsistencies, errors or deficiencies, in the application such that the AO's approval requires amendments or augmentation, the SRO will return the application form to the AO with recommendation for alternative wording or further information and the AO will incorporate the same.

The form will then be returned to the SRO for final quality assurance.

Once the SRO has quality assured the form this will form the basis of the application to the Magistrates' Court for authorisation.

There is however only one "authorising officer" and the SRO's role is limited to ensuring the integrity of the process.

6. Judicial Authorisation

From 1 November 2012, sections 37 and 38 of the Protection of Freedoms Act 2012 came in to force. This requires that local authorities who wish to authorise the use of directed surveillance and use of a CHIS under RIPA will need to obtain an order approving the grant or renewal of an authorisation or notice from a Justice of the Peace or District Judge (JP/DJ) before it can take effect. If the JP/DJ is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

The judicial approval mechanism is in addition to the existing authorisation process under the relevant parts of RIPA as outlined above and in this section. The current process of assessing necessity and proportionality, completing the RIPA authorisation/application form and seeking approval from an authorising officer/designated person will therefore remain the same.

The appropriate officer from Castle Point Borough Council will provide the DJ/JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the DJ/JP and should contain all information that is relied upon.

The original RIPA authorisation or notice should be shown to the DJ/JP but also be retained by Castle Point Borough Council so that it is available for inspection by the Commissioners' officers and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT). The Court may also wish to keep a copy so an extra copy should be made available to the Court.

Importantly, the appropriate officer will also need to provide the DJ/JP with a partially completed judicial application/order form.

Although the officer is required to provide a brief summary of the circumstances of the case on the judicial application form, this is supplementary to and does not replace the need to supply the original RIPA authorisation as well.

The order section of the form will be completed by the DJ/JP and will be the official record of the DJ/JP's decision. The officer from Castle Point Borough Council will need to obtain judicial approval for all initial RIPA authorisations/applications and renewals and will need to retain a copy of the judicial application/order form after it has been signed by the DJ/JP. There is no requirement for the DJ/JP to consider either cancellations or internal reviews.

The authorisation will take effect from the date and time of the DJ/JP granting approval and Castle Point Borough Council may proceed to use the techniques approved in that case.

It will be important for each officer seeking authorisation to establish contact with Her Majesty's Court and Tribunals Service (HMCTS) administration at the magistrates' court. HMCTS administration will be the first point of contact for the officer when seeking DJ/JP approval. Castle Point Borough Council will need to inform HMCTS administration as soon as possible to request a hearing for this stage of the authorisation.

On the rare occasions where out of hours access to a DJ or JP is required, then it will be for the officer to make local arrangements with the relevant HMCTS legal staff. In these cases, we will need to provide two partially completed judicial application/order forms so that one can be retained by the DJ/JP. They should provide the court with a copy of the signed judicial application/order form the next working day.

In most emergency situations where the police have power to act, then they are able to authorise activity under RIPA without prior DJ/JP approval. No RIPA authority is required in immediate response to events or situations where it is not reasonably practicable to obtain it (for instance when criminal activity is observed during routine duties and officers conceal themselves to observe what is happening).

Where renewals are timetabled to fall outside of court hours, for example during a holiday period, it is the local authority's responsibility to ensure that the renewal is completed ahead of the deadline. Out of hours procedures are for emergencies and should not be used because a renewal has not been processed in time. The hearing is a 'legal proceeding' and therefore our officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the DJ/JP.

The hearing will be in private and heard by a District Judge or a single JP who will read and consider the RIPA authorisation or notice and the judicial application/order form. He/she may have questions to clarify points or require additional reassurance on particular matters.

The attending officer will need to be able to answer the DJ/JP's questions on the policy and practice of conducting covert operations and the detail of the case itself. Castle Point Borough Council officers may consider it appropriate for the SPoC (single point of contact) to attend for applications for RIPA authorisations. This does not, however, remove or reduce in any way the duty of the authorising officer to determine whether the tests of necessity and proportionality have been met. Similarly, it does not remove or reduce the need for the forms and supporting papers that the authorising officer has considered, and which are provided to the DJ/JP to make the case (see 4. Authorisation Process in particular investigation officer paragraphs 1 and 2).

It is not Castle Point Borough Council policy that legally trained personnel are required to make the case to the DJ/JP, however if a member of the Legal Department wishes to attend with the applicant this is not discouraged.

It is advised that the Authorising Officer be the appropriate officer or at the very least attend the Court to assist the DJ/JP if necessary.

The forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided. The DJ/JP may note on the form any additional information he or she has received during the course of the hearing but information fundamental to the case should not be submitted in this manner.

If more information is required to determine whether the authorisation or notice has met the tests, then the DJ/JP will refuse the authorisation. If an application is refused the local authority should consider whether they can reapply, for example, if there was information to

support the application which was available to the local authority, but not included in the papers provided at the hearing.

The DJ/JP will record his/her decision on the order section of the judicial application/order form. HMCTS administration will retain a copy of the local authority RIPA authorisation or notice and the judicial application/order form. This information will be retained securely. Magistrates' Courts are not public authorities for the purposes of the Freedom of Information Act 2000.

7. Authorisation periods

The authorisation will take effect from the date and time of the DJ/JP granting approval and Castle Point Borough Council may proceed to use the techniques approved in that case.

Renewals should not normally be granted more than seven days before the original expiry date. If the circumstances described in the application alter, the applicant must submit a review document before activity continues.

As soon as the operation has obtained the information needed to prove, or disprove, the allegation, the applicant must submit a cancellation document and the authorised activity must cease.

CHIS authorisations will (unless renewed or cancelled) cease to have effect 12 months from the day on which authorisation took effect, except in the case of juvenile CHIS which will cease to have effect after 4 months (SI/2018/715 refers). Urgent authorisations will unless renewed, cease to have effect after 72 hours.

8. Urgency

Approval for directed surveillance in an emergency can only be obtained in written form. Oral approvals are no longer permitted. In cases where emergency approval is required an AO must be visited by the applicant with two completed RIPA application forms. The AO will then assess the proportionality, necessity and legality of the application. If the application is approved, then the applicant must then contact the out-of-hours HMCTS representative to seek approval from a Magistrate (DJ or JP). The applicant must then take two signed RIPA application forms and the judicial approval form to the Magistrates' Court for the hearing to take place.

As with a standard application the test of necessity, proportionality and the crime threshold must be satisfied. A case is not normally to be regarded as urgent unless the delay would, in the judgment of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation. Examples of situations where emergency authorisation may be sought would be where there is intelligence to suggest that there is a substantial risk that evidence may be lost, a person suspected of a crime is likely to abscond, further offences are

likely to take place and/or assets are being dissipated in a criminal investigation and money laundering offences may be occurring. An authorisation is not considered urgent if the need for authorisation has been neglected or the urgency is due to the authorising officer or applicant's own doing. All forms must then be made available to the SRO for countersigning (if appropriate) and RCO/SPOC for retention in the central register as soon as is reasonably practicable, preferably the next working day.

9. Communications Data, OCDA and NAFN

Before considering submitting an application for the acquisition of communications data, all officers must first refer the matter to the senior responsible officer (SRO) and RCO/SPOC.

Communications Data ('CD') is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). Local Authorities are not permitted to intercept the content of any person's communications.

Part 3 of the Investigatory Powers Act 2016 (IPA) replaced part 1 chapter 2 of RIPA in relation to the acquisition of communications data (CD) and puts local authorities on the same standing as the police and law enforcement agencies. Previously local authorities have been limited to obtaining subscriber details (known now as "entity" data) such as the registered user of a telephone number or email address. Under the IPA, local authorities can now also obtain details of in and out call data, and cell site location. This information identifies who a criminal suspect is in communication with and whereabouts the suspect was when they made or received a call, or the location from which they were using an Internet service. This additional data is defined as "events" data.

A new threshold for which CD "events" data can be sought has been introduced under the IPA as "applicable crime". Defined in section 86(2A) of the Act this means: an offence for which an adult is capable of being sentenced to one year or more in prison; any offence involving violence, resulting in substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy. Further guidance can be found in paragraphs 3.3 to 3.13 of CD Code of Practice:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

Finally, the IPA has also removed the necessity for local authorities to seek the endorsement of a Justice of the Peace when seeking to acquire CD. All such applications must now be processed through NAFN and will be considered for approval by the independent Office of Communication Data Authorisation (OCDA). The transfer of applications between local authorities, NAFN and OCDA is all conducted electronically and will therefore reduce what

can be a protracted process of securing an appearance before a Magistrate or District Judge (see local authority procedures set out in paragraphs 8.1 to 8.7 of the CD Code of Practice).

10. Internet / Social Media / Telephones

Internet

Castle Point Borough Council already has a policy on Internet use by its employees. This is the Internet Security Policy that sets out employees' responsibilities and liabilities. A copy of this Policy is currently made available to all employees on the Intranet. With the increasing availability of the Intranet and internal e-mailing facilities, it is important that all employees are made aware of and subject to the policy.

Castle Point Borough Council's policy of restricting access to certain undesirable Internet sites will continue through web filtering software. During work times, the content of employees' emails should be restricted to matters relating to their work and job descriptions. Any employee who now uses the Internet at work for private e-mails will do so in the knowledge that such usage can be monitored and consequently implicitly consents to the removal of any expectation of privacy.

Telephones

Castle Point Borough Council will also continue its current practice of providing information monthly about telephone usage on a Departmental basis. This information gives details of the call volume from every telephone extension and mobile 'phone supplied to Officers and paid for by Castle Point Borough Council and, if required, can provide a breakdown of the numbers dialled, the duration of the calls and the dates and times they were made.

Employees' use of Castle Point Borough Council's telephones for private calls is already covered in the Staff Handbook and Code of Conduct for Employees. Any employee who now uses work telephones for private calls will do so in the knowledge that such usage can be monitored, as described in this policy and consequently implicitly consents to the removal of any expectation of privacy.

Social Media

Information gathered in relation to investigations regarding members of the public shall be gathered through publicly available information only. Unless the person involved has given their consent in writing to allow the investigating officer to invade their privacy further. **However, continued visits to a person's public page could amount to covert surveillance.**

An example of this is would be viewing a member of the public's publicly available Facebook pages only and not accessing further information through links with their friends.

Any member of a public authority, or person acting on their behalf, who conducts activity on the internet in such a way that they may interact with others, whether by publicly open websites such as an online news and social networking service, or more private exchanges such as e-messaging sites, in circumstances where the other parties could not reasonably be expected to know their true identity, should consider whether the activity requires a CHIS authorisation. A directed surveillance authorisation should also be considered, unless the acquisition of that information is or will be covered by the terms of an applicable CHIS authorisation.

Where someone, such as an employee or member of the public, is tasked by a public authority to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the public authority, in order to obtain or provide access to information, a CHIS authorisation is likely to be required. For example:

- An investigator using the internet to engage with a subject of interest at the start of an operation, in order to ascertain information or facilitate a meeting in person.
- Directing a member of the public (such as a CHIS) to use their own or another internet profile to establish or maintain a relationship with a subject of interest for a covert purpose.
- Joining chat rooms with a view to interacting with a criminal group in order to obtain information about their criminal activities.

A CHIS authorisation will not always be appropriate or necessary for online investigation or research. Some websites require a user to register providing personal identifiers (such as name and phone number) before access to the site will be permitted. Where a member of a public authority sets up a false identity for this purpose, this does not in itself amount to establishing a relationship, and a CHIS authorisation would not immediately be required, though consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met.

> Example 1: An HMRC officer intends to make a one-off online test purchase of an item on an auction site, to investigate intelligence that the true value of the goods is not being declared for tax purposes. The officer concludes the purchase and does not correspond privately with the seller or leave feedback on the site. No covert relationship is formed and a CHIS authorisation need not be sought.
>
> Example 2: HMRC task a member of the public to purchase goods from a number of websites to obtain information about the identity of the seller, country of origin of the

goods and banking arrangements. The individual is required to engage with the seller as necessary to complete the purchases. The deployment should be covered by a CHIS authorisation because of the intention to establish a relationship for covert purposes.

Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as “like” or “follow” to react to information posted by others online would not in itself constitute forming a relationship. However, it should be borne in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if it is intended for an officer of a public authority or a CHIS to engage in such interaction to obtain, provide access to or disclose information.

Example 1: An officer maintains a false persona, unconnected to law enforcement, on social media sites in order to facilitate future operational research or investigation. As part of the legend building activity he “follows” a variety of people and entities and “likes” occasional posts without engaging further. No relationship is formed and no CHIS authorisation is needed.

Example 2: The officer sends a request to join a closed group known to be administered by a subject of interest, connected to a specific investigation. A directed surveillance authorisation would be needed to cover the proposed covert monitoring of the site. Once accepted into the group it becomes apparent that further interaction is necessary. This should be authorised by means of a CHIS authorisation.

When engaging in conduct as a CHIS, a member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without considering the need for authorisation. Full consideration should be given to the potential risks posed by that activity.

Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with section 6.13 of the CHIS 2018 Code of Practice and should include consideration of the risks arising from that online activity including factors such as the length of time spent online and the material to which the CHIS may be exposed. This should also take account of any disparity between the technical skills of the CHIS and those of the handler or authorising officer, and the extent to which this may impact on the effectiveness of oversight.

Where it is intended that more than one officer will share the same online persona, each officer should be clearly identifiable within the overarching authorisation for that operation, providing clear information about the conduct required of each officer and including risk assessments in relation to each officer involved.

The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

Depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide

audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online.

> Example 1: A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.
>
> Example 2: A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)
>
> Example 3: A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.

In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;

- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation.

> Example: Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data by public authorities either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that the broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.

For further Information please see the Office of Surveillance Commissioners Procedures and Guidance notes July 2016, Section 289.

11. Handling of material and use of material as evidence

Material obtained from properly authorised directed surveillance or a source may be used in other investigations. Arrangements shall be in place for the handling, storage and destruction of material obtained through the use of directed surveillance, a source or the obtaining or disclosure of communications data, following relevant legislation such as the Criminal Procedure and Investigations Act (CPIA). Authorising Officers must ensure compliance with the appropriate data protection and CPIA requirements, having due regard to the Public

Interest Immunity test and any relevant Corporate Procedures relating to the handling and storage of material.

Where the product of surveillance could be relevant to pending or future proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

12. Training

Officers conducting directed surveillance operations, using a CHIS or acquiring communications data must have an appropriate accreditation or be otherwise suitably qualified or trained.

Authorising Officers (Appendix 5) will be appointed by the Chief Executive and will have received training that has been approved by the Senior Responsible Officer. The Senior Responsible Officer will have appointed the RIPA Coordinating Officer who will be responsible for arranging suitable training for those conducting surveillance activity or using a CHIS.

All training will take place at reasonable intervals to be determined by the SRO or RCO, but it is envisaged that an update will usually be necessary following legislative or good practice developments or otherwise every 12 months.

13. Surveillance Equipment

All mobile surveillance equipment is kept in secure premises of each investigation and enforcement team in the Civic Offices. Access to the area is controlled by the relevant team, who maintain a spreadsheet log of all equipment taken from and returned to the area.

14. The Inspection Process

The IPCO – Investigatory Powers Commissioner's Office will make periodic inspections during which the inspector will wish to interview a sample of key personnel; examine RIPA and CHIS applications and authorisations; the central register and policy documents. The inspector will also make an evaluation of processes and procedures.

15. GUIDANCE ON CASTLE POINT BOROUGH COUNCIL'S CORPORATE POLICY STATEMENT

All forms of covert surveillance will be regulated by Castle Point Borough Council's Corporate Policy.

Castle Point Borough Council will conduct its covert surveillance operations, including the interception of telecommunications to investigate alleged abuses of telephone, e-mail or Internet facilities, within the eight principles of the Data Protection Act and restrict those

operations to situations falling within the permitted exceptions of the Human Rights Act and RIPA. Consequently, covert surveillance for monitoring or recording communications will only be carried out for the purpose of preventing or detecting crime or of preventing disorder;

Surveillance equipment will be installed or a CHIS, used for one of the above legitimate purposes, only when sufficient evidence exists and has been documented to warrant the exercise and surveillance is shown to be both the least harmful means of meeting that purpose and meets the requirements of this policy and government legislation.

Care must be taken to ensure all reasonable alternative methods to resolve a situation, such as naked eye observation, interview or changing methods of working or level of security, must be considered first and recorded in writing and the reason for surveillance being requested fully documented. [Where the subject of covert surveillance is an employee, the Head of Service/Chief Personnel Officer and Internal Audit must be informed to ensure compliance with Castle Point Borough Council's other relevant policies].

All requests to conduct, extend or discontinue a covert surveillance exercise must be made in writing on the relevant form. Requests must be submitted to the appropriate level of Officer within each Service (see the authorisation section set out in Appendix 5). All requests must be authorised in accordance with this policy before any covert surveillance operation can commence. The power to grant, extend and discontinue authorisations will be limited in accordance with this policy. Written authorisations for a covert surveillance operation will be subject to review within that period to establish whether the authorisation should continue for the entire three-month period.

Officers should ensure that when considering carrying out covert surveillance it is carefully planned so that the necessary consultations regarding risk assessment, insurance and health and safety can be carried out and the required provisions put in place before surveillance commences as per this policy.

In the event of covert surveillance needing to be carried out in an emergency, a written request and authorisation is still required, using the relevant forms. However, Surveillance that is unforeseen and undertaken as an immediate response to a situation when it is not reasonably practicable to get authorisation falls outside the definition of directed surveillance and, therefore, authorisation is not required. If after, however, a specific investigation or operation is to follow an unforeseen response, authorisation must be obtained in the usual way before it can commence. In no circumstances will any covert surveillance operation be given backdated authorisation after it has commenced.
Embarking upon covert surveillance or the use of a CHIS without authorisation or conducting covert surveillance outside the scope of the authorisation will mean that the "protective umbrella" of RIPA is unavailable.

Each Head of Service will ensure that the originals of all authorisation documents are retained and maintain a Register of all requests for authorisations for covert surveillance, together with the reasons for any request being denied, and provide copies to the SRO and RCO/SPOC for retention in the central register.

No covert operation will be embarked upon by a Castle Point Borough Council Officer without detailed consideration of the points in this policy and of the insurance and health and safety implications involved and the necessary precautions and insurance being put in place.

During a covert operation, recorded material or information collected will be stored and transported securely. Both any evidence revealed and the need for authorisation should be reviewed regularly to ensure authorisation is only given for as long as is necessary and, once enough evidence has been collected, consideration should be given to either cancelling it or checking initial authorisation grounds are still valid. It should also be noted under the Data Protection Act 1998 that evidence should only be retained for as long as is necessary and access to it will be restricted to the authorising Officers concerned. The authorising Officer will decide whether to allow requests for access by third parties, including Castle Point Borough Council Officers. Access will generally only be allowed to limited and prescribed parties, including law enforcement agencies, prosecution agencies, legal representatives and the people subject to the surveillance (unless disclosure would prejudice any criminal enquiries or proceedings) in accordance with this policy, the Human Rights Act, the Data Protection Act, RIPA and any other relevant legislation.

Only high-quality video and audio tapes will be used. All video and audio tapes will be identified uniquely and erased prior to re-use.

Once a covert operation results in an individual being under suspicion of having committed a criminal offence that individual must be informed of this as promptly as is reasonably practicable in order to ensure their right to a fair trial or hearing within a reasonable time in accordance with the Human Rights Act. In a situation where it is considered that a matter gives rise to a potential criminal offence, any interview with the suspect must be under caution and conducted by a suitably trained Officer or, if appropriate, the Police must be involved immediately to ensure that evidential procedures and the requirements of current legislation are observed.

16. Resources

Full Codes of Practice can be found on the Home Office website:
http://www.homeoffice.gov.uk/

Covert Surveillance & Property Interference:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

CHIS:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf

Acquisition and Disclosure of Communications Data:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

Further information can also be found on The Investigatory Powers Commissioner's Office website.
https://www.ipco.org.uk/

Appendix 1

GLOSSARY OF TERMS

CD
Communications Data

Collateral intrusion
The likelihood of obtaining private information about someone who is not the subject of the directed surveillance operation.

Confidential information
This covers confidential journalistic material, matters subject to legal privilege, and information relating to a person (living or dead) relating to their physical or mental health; spiritual counselling or which has been acquired or created in the course of a trade/profession/occupation or for the purposes of any paid/unpaid office.

Covert relationship
A relationship in which one side is unaware of the purpose for which the relationship is being conducted by the other.

Directed Surveillance
Surveillance carried out in relation to a specific operation which is likely to result in obtaining private information about a person in a way that they are unaware that it is happening. It excludes surveillance of anything taking part in residential premises or in any private vehicle.

Intrusive Surveillance
Surveillance which takes place on any residential premises or in any private vehicle. A Local Authority cannot use intrusive surveillance.

Legal Consultation
A consultation between a professional legal adviser and his client or any person representing his client, or a consultation between a professional legal adviser or his client or representative and a medical practitioner made in relation to current or future legal proceedings.

Residential premises
Any premises occupied by any person as residential or living accommodation, excluding common areas to such premises, e.g. stairwells and communal entrance halls.

Senior Responsible Officer (SRO)
The SRO is responsible for the integrity of the processes in order for Castle Point Borough Council to ensure compliance when using Directed Surveillance or CHIS.

Service data
Data held by a communications service provider relating to a customer's use of their service, including dates of provision of service; records of activity such as calls made, recorded delivery records and top-ups for pre-paid mobile phones.

Surveillance device

Anything designed or adapted for surveillance purposes.

Appendix 2

Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010

The Order consolidates four previous Orders relating to directed surveillance and the use or conduct of covert human intelligence sources by public authorities under Part II of the Regulation of Investigatory Powers Act 2000 (RIPA) and to reflect the outcome of a public consultation which took place between April and July 2009.

It identifies the 'relevant public authorities' authorised to conduct RIPA and CHIS activities. This list includes local authorities in England and Wales. It also gives examples of such activity, as shown on page 3 of this document.

Appendix 3

The Human Rights Act 1998

Articles 6 and 8 of the Human Rights Act are relevant to RIPA.

Article 6 relates to the right to a fair trial.

Article 8 relates to the right to respect for a private and family life.

If it is proposed that directed surveillance evidence is to be used in a prosecution, or other form of sanction, the subject of the surveillance should be informed during an interview under caution.

Appendix 4

The Data Protection Act 1998 (DPA)

The eight principles of the Act relating to the acquisition of personal data need to be observed when using RIPA. To ensure compliance, the information must:

- Be fairly and lawfully obtained and processed
- Be processed for specified purposes only
- Be adequate, relevant and not excessive
- Be accurate
- Not be kept for longer than is necessary
- Be processed in accordance with an individual's rights
- Be secure
- Not be transferred to non-EEAJ countries without adequate protection.

Appendix 5

List of Authorising Officers

The following post holders may authorise RIPA applications where there is a likelihood of obtaining Confidential Information: Chief Executive or deputy.

The following post holders may authorise the use of a vulnerable person or a juvenile to be used as a Covert Human Intelligence Source: Chief Executive, as Head of Paid Service or his or her deputy.

The following post holders may authorise applications, reviews, renewals and cancellations of Directed Covert Surveillance of Covert Human Intelligence Sources: Chief Executives and Directors, or in their absence, the Head of Legal and Democratic Services.

Principal RIPA Officers

Jason Bishop Solicitor to the Council and Head of Legal Services	Senior Responsible Officer (SRO)	01268 882462	jbishop@castlepoint.gov.uk
Jemma Matlin Legal Executive	RIPA Co-ordinating Officer (RCO) (Single Point of Contact)	01268 882258	jmatlin@castlepoint.gov.uk

Authorising Officers

Chief Executive	Authorising Officer	01268 882401	dmarchant@castlepoint.gov.uk
Head of Environments	Authorising Officer	01268 882476	tbragg@castlepoint.gov.uk
Head of Housing	Authorising Officer	01268 882419	jgrisley@castlepoint.gov.uk
Head of Licensing	Authorising Officer	01268 882369	mharris@castlepoint.gov.uk

Appendix 6

Central Register

A central register will be maintained by the RIPA single point of contact. The register will contain details of all RIPA and CHIS applications (whether approved or not) and all reviews, renewals and cancellations. All non-RIPA applications will also be recorded.

Each operation will be given a unique reference number (URN) from which the department involved, and the year of the operation may be readily identified.

The register will also contain the following information:

- The operation reference name or number
- The name of the applicant
- The name of the subject of the surveillance or CHIS activity (for internal enquiries a pseudonym may be used)
- The date and time that the activity was authorised
- The date and time of any reviews that are to be conducted
- The date and time of any renewals of authorisations
- The date and time of the cancellations of any authorisations

Kept in conjunction with the register will be the details of the training and updates delivered to authorising officers, a list of authorising officers, a copy of the RIPA policy and copies of all relevant legislation.

The original of all documents (f any) will also be held with the register although it is envisaged that all applications, reviews, renewals and cancellations will be kept digitally. In any event, all copies must be available for inspection by the Investigatory Powers Commissioner's Office.

Appendix 7

Briefing Report

Before any RIPA/non-RIPPA or CHIS operation commences, all staff will be briefed by the officer in charge of the case using the format of this briefing report. The original will be retained with the investigation file.

RIPA URN ……

Name and number to identify operation …….

Date, time and location of briefing ……..

……

Persons present at briefing ……..

……

Information (Sufficient background information of the investigation to date to enable all those taking part in the operation to fully understand their role).

Intention (What is the operation seeking to achieve?).

Method (How will individuals achieve this? If camcorders are to be used, remind officers that any conversations close to the camera will be recorded).

Administration (To include details of who will be responsible for maintenance of the log sheet and collection of evidence; any identified health and safety issues; the operation; an agreed stand down procedure – NOTE It will be the responsibility of the officer in charge of the investigation to determine if and when an operation should be discontinued due to reasons of safety or cost-effectiveness – and an emergency rendezvous point. On mobile surveillance operations, all those involved will be reminded that at ALL times speed limits and mandatory road signs MUST be complied with and that drivers must NOT use radios or telephones when driving unless the equipment is 'hands free').

Communications (Effective communications between all members of the team will be established before the operation commences).

Appendix 8

Best practice regarding photographic and video evidence

Photographic or video evidence can be used to support the verbal evidence of what the officer conducting surveillance actually saw. There will also be occasions when video footage may be obtained without an officer being present at the scene. However, it is obtained, it must properly documented and retained in order to ensure evidential continuity. All such material will be disclosable in the event that a prosecution ensues.

Considerations should be given as to how the evidence will eventually be produced. This may require photographs to be developed by an outside laboratory. Arrangements should be made in advance to ensure continuity of evidence at all stages of its production. A new film, tape or memory card should be used for each operation.
If video footage is to be used start it with a verbal introduction to include day, date, time and place and names of officer's present. Try to include footage of the location, e.g. street name or other landmark so as to place the subject of the surveillance.

A record should be maintained to include the following points:

- Details of the equipment used
- Confirmation that the date & time on the equipment is correct
- Name of the officer who inserted the film, tape or memory card into the camera
- Details of anyone else to whom the camera may have been passed
- Name of officer removing film, tape or memory card
- Statement to cover the collection, storage and movement of the film, tape or memory card
- Statement from the person who developed or created the material to be used as evidence

As soon as possible the original recording should be copied, and the master retained securely as an exhibit. If the master is a tape, the record protect tab should be removed once the tape has been copied. Do not edit anything from the master. If using tapes, only copy on a machine that is known to be working properly. Failure to do so may result in damage to the master.

Stills may be taken from video. They are a useful addition to the video evidence.

Appendix 9

Surveillance Log

Daily log of activity, to be kept by each operator or pair of operators.

A – Amount of time under observation
D – Distance from subject
V - Visibility
O - Obstruction
K – Known, or seen before
A – Any reason to remember, subject or incident
T – Time elapsed between sighting and note taking
E – Error or material discrepancy – e.g. description, vehicle reg etc.

Operation name or number …….

Date ……..……..

Time of activity (from) ……..….. (to) …….

Briefing location and time ……

Name of operator(s) relating to THIS log …….

……

Details of what was seen, to include ADVOKATE (as above).

……

……

……

……

……

……

……

Appendix 10

R v Johnson

R. v. Johnson [1988] 1 WLR 1377 laid down the correct procedure when using observation posts:

- The police officer in charge of the observation, who should be of no lesser rank than sergeant, should testify that he had visited the observation posts and ascertained the attitude of the occupiers to the use of the premises and to disclosure which might lead to their identification. (It is suggested that the 'Sergeant' could be replaced by a section manager).

- An inspector should then testify that immediately before the trial he visited those places and ascertained whether the occupiers were the same persons as those at the time of the observations. (It is suggested that 'inspector' could be replaced by head of department).

- If they were not s/he, should testify as to their attitude to the use made of the premises and to possible disclosure which might lead to their identification.

- The judge should explain to the jury when summing up or at some other point the effect of his ruling to exclude the evidence of the location.

Public Interest Immunity (PII) protects the identity of a person who has permitted surveillance to be conducted from private premise, so this extends to the address and any other information that could reveal their identity. If, however, the location can be revealed without identifying the occupier, then it should be.

Appendix 11

Castle Point Borough Council
NON-RIPA Authorisation Procedure.

1. Introduction

This document has resulted from the change in the law in respect of Directed Surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA) and the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2012. From 1 November 2012 Directed Surveillance under RIPA only applied to the detection and prevention of a criminal offence that attracts a penalty of 6 months imprisonment or more or are offences involving the sale of tobacco and alcohol to underage children. This essentially removes the following types of activities from regulation: Surveillance of disorder (unless it carries a 6 month's custodial sentence), most summary offences such as littering, dog fouling, underage sales of fireworks, lower level benefit fraud and anti-social behaviour.

Enforcement officers can still undertake such surveillance but because it is not now regulated by The Investigatory Powers Commissioner's Office, the Council should have procedures in place to ensure that we can prove that we have given due consideration to necessity and proportionality, central tenets of European Law and the likely grounds of any challenge that may be received.

RIPA is there to ensure that certain types of covert surveillance undertaken by public authorities is done in a certain way and is human rights compliant. RIPA is permissive legislation. Authorisation under RIPA affords a public authority a defence of impunity that the activity is lawful for all purposes. However, failure to obtain an authorisation does not make covert surveillance unlawful. Section 80 of RIPA provides that the Act should not be construed so as to make it unlawful to engage in any conduct of that description which is not otherwise unlawful under this Act and would not be unlawful apart from this Act. Case law confirms that lack of authorisation under RIPA does not necessarily mean that the carrying out of directed surveillance is unlawful. Local authorities will still be able use covert surveillance for such purposes as long as it is necessary and proportionate in accordance with Article 8 of the European Convention on Human Rights (right to privacy).

2. Overview

Authority to use Non-RIPA surveillance techniques and the forms to be completed are the same as set out in the main RIPA policy. It will be the responsibility of Authorising Officers to ensure that their relevant members of staff are suitably trained and that applications for Directed Surveillance authorisations are completed correctly and that the same procedures as detailed in the main RIPA policy are followed. A current list of authorising officers is attached at Appendix five. Authorising officers will also ensure that staff who report to them follow this procedure and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document and the main RIPA policy document above.

3. Directed surveillance

The same policy for regulated activities as detailed above should be followed in relation to directed surveillance activities that are not regulated. Any applications for non-RIPPA authority are still required to meet the necessity and proportionality tests as set out on pages 7 and 8 above.

Collateral Intrusion:
The same considerations for collateral intrusion apply.

Crime Threshold:
The use of directed surveillance by local authorities relating to crimes that are not regulated by the Regulation of Investigatory Powers (Directed Surveillance and CHIS) (Amendment) Order 2012, relate to criminal activities that fall under that threshold. These are offences that are not punishable by a maximum term of at least 6 months imprisonment and do not relate to the underage sale of alcohol or tobacco. All surveillance activities that relate to crimes not falling within the regulated regime fall under this policy. It is not therefore necessary to make any applications for judicial authority relating to non-RIPA activity.

4. The Authorisation Process

The same procedures as outlined on pages 13 and 15 above apply, save for the need to seek judicial authority as this is not necessary for non-regulated activities. No application for non-RIPA authority can however be applied for using the emergency provisions set out on pages 18 and 19. It is not envisaged that non-RIPA emergency applications will be necessary.

5. Communications Data

Communications data do not come under this (non-RIPA) policy. Any applications for this material fall under regulated activities and the procedures set out in the RIPA policy must be followed.

6. Internet / Social Media / Telephones

The policies set out on pages 20 to 25 should be followed. If there is any doubt as to whether the surveillance activity falls under RIPA or non-RIPA, legal advice should be sought. Social Media sites are a useful tool for intelligence and evidence gathering. However, there is a fine distinction between accessing readily available personal information posted into the public domain on Social Media and interfering in an individual's private life. The Internet is a surveillance device. Reviewing open source sites does not require authorisation unless the

review is carried out with some regularity, usually when creating a profile, in which case directed surveillance authorisation will be required. If it becomes necessary to breach the privacy controls and become for example 'a friend' on the Facebook site, with the investigating officer utilising a false account concealing his/her identity as a council officer for the purposes of gleaning intelligence, this is a covert operation intended to obtain private information and should be RIPA authorised and the main RIPA policy will need to be followed. If the investigator engages in any form of relationship with the account operator, then they become a Covert Human Intelligence Source (CHIS) requiring authorisation as such and management by a Controller and Handler with a record being kept and a risk assessment created. Some of the examples set out in the RIPA policy above assist in deciding whether the activity requires the use of a CHIS authorisation or not. It will only be in exceptional circumstances that a Non-RIPA authorisation will be considered appropriate for social media. The use of Social Media for the gathering of evidence to assist in enforcement activities should be used with the following considerations:

- It is only in the most exceptional cases that a false identity should be used in order to 'friend' individuals on social networks. Authorisation will be required in accordance with this policy.

- Officers viewing an individual's open profile on a social network should do so only in order to obtain evidence to support or refute their investigation; this should only be done to obtain the information and if necessary, later to confirm the information.

- Systematic viewing of a profile will normally amount to surveillance and an authorisation should be obtained.

- Authorisation should also be considered where a friend request is sent or if a conversation has been entered into with the owner of the page as this may amount to a CHIS.

- Officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, reasonable steps must be taken to ensure its validity.

7. Handling of material and use of material as evidence

The policy relating to this on pages 25 and 26 must be followed.

8. Duration

There are no specified times relating to non-RIPA applications etc, but it is proposed that the same times provided for under RIPA are followed for consistency. Forms must be reviewed in the time stated, renewed and/or cancelled once it is no longer needed. The authorisation to carry out/conduct the surveillance lasts for a maximum of three months (from authorisation)

for Directed Surveillance. In other words, the forms do not expire, they have to be reviewed, renewed and/or cancelled once they are no longer required. Authorisations should be renewed before the maximum period in the authorisation has expired. The Authorising Officer must consider the matter afresh including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred. An authorisation cannot be renewed after it has expired. In such event a fresh authorisation will be necessary.

9. Record Management

As for RIPA applications, a Central Register of all Authorisations, Reviews, Renewals and Cancellations and Rejections will be maintained and monitored by the SRO, RCO/SPOC.

If there is any conflict between this policy and the RIPA policy outlined above, the RIPA policy should be followed and takes precedence. Any concerns or queries should be directed to the RCO/SPOC and then to the SRO.