Appendix 1

TAMWORTH BOROUGH COUNCIL

POLICY & PROCEDURE

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

Jane M Hackett
Solicitor to the Council
Tamworth Borough Council

Policy date: Review: Revised: 24 May 2011

CONTENTS

Section A

Introduction

1. OBJECTIVE: SUSTAINABLE COMMUNITIES; SAFER AND STRONGER COMMUNITIES

Tamworth Borough Council is committed to improving the quality of life for the communities of Tamworth which includes benefiting from an attractive place to live, meeting the needs of local people and employers with opportunities for all to engage in community life. It also wishes to maintain its position as a low crime borough and a safe place to live, work and learn. Although most of the community comply with the law, it is necessary for Tamworth to carry out enforcement functions to take full action against those who flout the law. Tamworth Borough Council will carry out enforcement action in a fair, practical and consistent manner to help promote a thriving local economy.

2. HUMAN RIGHTS ACT 1998 – ARTICLE 8 – RIGHT TO RESPECT FOR PRIVATE & FAMILY LIFE, HOME AND CORRESPONDENCE

The Human Rights Act 1998 brought into UK domestic law much of the European Convention on Human Rights and Fundamental Freedoms 1950. Article 8 of the European Convention requires the Council to respect the private and family life of its citizens, their homes and their correspondence. Article 8 does, however, recognise that there may be circumstances in a democratic society where it is necessary for the state to interfere with this right.

3. USE OF COVERT SURVEILLANCE TECHNIQUES AND HUMAN INTELLIGENCE SOURCES

The Council has various functions which involve observing or investigating the conduct of others, for example, investigating anti-social behaviour, fly tipping, noise nuisance control, planning (contraventions), benefit fraud, licensing and food safety legislation. In most cases, Council officers carry out these functions openly and in a way which does not interfere with a person's right to a private life. However, there are cases where it is necessary for officers to use covert surveillance techniques to undertake a specific investigation. The use of covert surveillance techniques is regulated by the Regulation of Investigatory Powers Act 2000 (RIPA), which seeks to ensure that the public interest and human rights of individuals are appropriately balanced. This document sets out the Council's policy and procedures on the use of covert surveillance techniques and the conduct and use of a Covert Human Intelligence Source. You should also refer to the two Codes of Practice published by the Government. These Codes, which were revised in 2010, are on the Home Office website and supplement the procedures in this document. The Codes are admissible as

evidence in Criminal and Civil Proceedings. If a provision of these Codes appear relevant to any court or tribunal, it must be taken into account.

Covert Surveillance and Property Interference Code of Practice:-

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/covert-surveil-prop-inter-COP

Covert Human Intelligence Sources Code of Practice:

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/covert-human-intel-source-COP

4. ACQUISITION OF COMMUNICATIONS DATA

RIPA also regulates the acquisition of communications data. Communications data is data held by telecommunications companies and internet service providers. Examples of communications traffic data which may be acquired with authorisation include names, addresses, telephone numbers, internet provider addresses, geographical location of the calling or the called parties. Communications data surveillance does not monitor the content of telephone calls or emails. This document sets out the procedures for the acquisition of communications data. You should also refer to the Code of Practice which is available on the Home Office website.

Acquisition and Disclosure of Communications Data Revised Draft Code of Practice:

http://tna.europarchive.org/20100419081706/http://security.homeoffice.gov.uk/ripa/publication-search/general-publications/ripa-cop/acquisition-disclosure-cop

Section B

EFFECTIVE DATE OF OPERATION AND AUTHORISING OFFICER RESPONSIBILITIES

1. The Policy and Procedures in this document have been amended to reflect the two revised Codes of Practice which came into force in April 2010, changes in website addresses and application forms as well as to reflect recommendations arising out of inspection by the Office of Surveillance Commissioners. It is essential, therefore, that Authorising Officers, take personal responsibility for the effective and efficient observance of this document.

2. It will be the responsibility of Authorising Officers to ensure that their relevant members of staff are suitably trained as 'Applicants'.

3. Authorising Officers will also ensure that staff who report to them follow this Policy and Procedures Document and do not undertake or carry out any form of covert surveillance without first obtaining the relevant authorisations in compliance with this document.

4. Authorising Officers must also pay particular attention to health and safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorising Officer approve any RIPA form unless, and until they are satisfied that

   - the health and safety of Council employees/agents are suitably addressed
   - risks minimised so far as is possible, and
   - risks are proportionate to the surveillance being proposed.

   If an Authorising Officer is in any doubt, prior guidance should be obtained from the Solicitor to the Council.

5. Authorising Officers must also ensure that, when sending copies of any Forms to the Solicitor to the Council (or any other relevant authority), that they are sent in **sealed** envelopes and marked '**Strictly Private & Confidential**'.

6. In Accordance with SI 2010 521, the Senior Responsible Officer with responsibility for Authorising Officers is the Solicitor to the Council. The Chief Executive in consultation with Corporate Management Team has power to appoint Authorising Officers for the purposes of RIPA. Authorising Officers will only be appointed on the Chief Executive being satisfied that suitable training on RIPA has been undertaken.

7. The Solicitor to the Council will review the policy every six months and annual reports on performance of the policy will be presented to the Audit and Governance Committee of the Council.

8. Quarterly reports on the use of RIPA will be considered by the Audit and Governance Committee.

Section C

GENERAL INFORMATION ON RIPA

1. The Human Rights Act 1998 requires the Council, and organisations working on its behalf, pursuant to Article 8 of the European Convention, to respect the private and family life of citizens, their homes and their correspondence.

2. The European Convention did not, however, make this an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizen's right mentioned above, if such interference is:-

   (a) **in accordance with the Law;**

   (b) **necessary** (as defined in this document); **and**

   (c) **proportionate** (as defined in this document).

3. The Regulation of Investigatory Powers Act 2000 ('RIPA') provides a statutory mechanism (ie. 'in accordance with the law') for authorising **covert surveillance** and the use of a **'covert human intelligence source' ('CHIS')** – eg. undercover agents. It seeks to ensure that any interference with an individual's right under Article 8 of the European Convention is necessary and proportionate. In doing so, RIPA and this Policy and Procedure document seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

4. Directly employed Council staff and external agencies working for the Council are covered by the Act for the time they are working for the Council. All external agencies must, therefore, comply with RIPA and the work carried out by agencies on the Council's behalf must be properly authorised by one of the Council's designated Authorising Officers. Please refer to Section H and to the paragraph on "Authorising Officers."

5. If the correct procedures are not followed, evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman and/or the Council could be ordered to pay compensation.

6. A flowchart of the procedures to be followed appears at **Appendix 1**.

Section D

WHAT RIPA DOES AND DOES NOT DO

1. RIPA:

- requires prior authorisation of directed surveillance.
- prohibits the Council from carrying out intrusive surveillance.
- requires authorisation of the conduct and use of a CHIS.
- requires safeguards for the conduct and use of a CHIS.

2. RIPA does not:

- make lawful conduct which is otherwise unlawful.
- prejudice or affect any existing powers available to the Council to obtain information by any means not involving conduct that may be authorised under this Act. For example, the Council's current powers to obtain information from the DVLA or from the Land Registry as to the ownership of a property.

3. If the Authorising Officer or any Applicant is in any doubt, s/he should ask the Solicitor to the Council BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

Section E

TYPES OF SURVEILLANCE

'Surveillance' includes:

- monitoring, observing and listening to persons, watching or following their movements, listening to their conversations and other such activities or communications. It may be conducted with or without the assistance of a surveillance device.

- recording anything mentioned above in the course of authorised surveillance.

- surveillance, by or with, the assistance of appropriate surveillance device(s).

Surveillance can be overt or covert.

Overt Surveillance

Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be behaving in the same way as a normal member of the public (eg. in the case of most test purchases), and/or will be going about Council business openly. Similarly, surveillance will be overt if the subject has been told it will happen (eg. where a noisemaker is warned (preferably in writing) that noise will be recorded.

Covert Surveillance

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place. (Section 26(9)(a) of RIPA).

RIPA regulates two types of covert surveillance, (Directed Surveillance and Intrusive Surveillance) and the use of Covert Human Intelligence Sources (CHIS).

Directed Surveillance

Directed Surveillance is surveillance which:-

- is **covert**; and
- is **not intrusive surveillance** (see definition below – the Council cannot carry out any intrusive surveillance).
- is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act reasonable, eg. spotting something suspicious and continuing to observe it; and
- it is undertaken for the purpose of a **specific investigation** or operation in a manner **likely to obtain private information** about an individual (whether or not that person is specifically targeted for purposes of an investigation). (*Section 26(10) RIPA).*

Private Information in relation to a person includes any information relating to his private and family life, his home or his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others with whom s/he comes into contact. Private information may include personal data such as names, addresses or telephone numbers. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate.

Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others. Privacy considerations are likely to arise if several records are examined together to establish a pattern of behaviour.

For the avoidance of doubt, only those Officers appointed as 'Authorising Officers' for the purpose of RIPA can authorise 'Directed Surveillance' IF, AND ONLY IF, the RIPA authorisation procedures detailed in this Document, are followed.

Intrusive Surveillance

This is when it:-

- is covert;
- relates to residential premises and private vehicles, even if used on a temporary basis. This includes the use of tracking devices on vehicles; and
- involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

This form of surveillance can be carried out only by police and other law enforcement agencies. Intrusive surveillance relates to the location of the surveillance, and not any consideration of the information that is likely to be obtained. Council officers cannot carry out intrusive surveillance.

"Proportionality"

This term contains three concepts:-

- the surveillance should not be excessive in relation to the gravity of the matter being investigated;
- the least intrusive method of surveillance should be chosen; and
- collateral intrusion involving invasion of third parties' privacy and should, so far as possible, be minimised.

Section F

CONDUCT AND USE OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

The Council can use a CHIS IF, AND ONLY IF, RIPA procedures, detailed in this document, are followed.

It is unlikely that a Local Authority will want to use a CHIS. If it appears that use of a CHIS may be required Authorising Officers must seek legal advice from the Solicitor to the Council.

Who is a CHIS?

Someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain information. RIPA does not apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information.

What must be authorised?

The conduct or use of a CHIS requires prior authorisation.

- **Conduct** of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or incidental to) obtaining and passing on information.

- **Use** of a CHIS = Actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

Juvenile Sources

Special safeguards apply to the use or conduct of juvenile sources (i.e. those under the age of 18). On no occasion can a child under 16 years of age be authorised to give information against his or her parents or any person with parental responsibility for him or her. Only the Chief Executive, or in his absence, the Deputy Chief Executive can authorise the use of a juvenile as a source.

Vulnerable Individuals

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 be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

A Vulnerable Individual will only be authorised to act as a source in the most exceptional of circumstances. Only the Chief Executive, or in his absence, the Deputy Chief Executive can authorise the use of a vulnerable individual as a source.

Test Purchases

Carrying out test purchases will not (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also directed surveillance.

Authorising Officers should consider the likelihood that the test purchase will lead to a relationship being formed with a person in the shop. If the particular circumstances of a particular test purchase are likely to involve the development of a relationship Authorising Officers must seek legal advice from the Solicitor to the Council.

Anti-Social Behaviour Activities (eg. Noise, Violence, Race etc)

Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (eg. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record without RIPA authorisation if the noisemaker is warned that this will occur. Placing a covert stationary or mobile camera outside a building to record anti-social behaviour on residential estates will require prior authorisation.

Section G

THE ROLE OF THE RIPA CO-ORDINATOR

Key Responsibilities of the RIPA Co-ordinator

- In this document the RIPA Co-ordinator is the Solicitor to the Council. The key responsibilities of the RIPA Co-ordinator are to:

- Retain all applications for authorisation (including those that have been refused), renewals and cancellations for a period of at least **three years** together with any supplementary documentation;

- Provide a unique reference number and maintain the central register of all applications for authorisations whether finally granted or refused (see section below);

- Create and maintain a spreadsheet for the purpose of identifying and monitoring expiry dates and renewal dates although the responsibility for this is primarily that of the officer in charge and the Authorising Officer;

- Monitor types of activities being authorised to ensure consistency and quality throughout the Council;

- Ensure sections identify and fulfil training needs;

- Periodically review Council procedures to ensure that they are up to date;

- Assist Council employees to keep abreast of RIPA developments;

- Provide a link to the Surveillance Commissioner and disseminate information on changes on the law, good practice etc. Officers becoming aware of such information should, conversely, send it to the RIPA Co-ordinator for this purpose;

- Check that Authorising Officers carry out reviews and cancellations on a timely basis.

<u>Central Record of Authorisations</u>

A centrally retrievable record of all authorisations will be held by the RIPA Co-ordinator (Solicitor to the Council) which must be up-dated whenever an authorisation is granted, renewed or cancelled. These records will be retained for a period of **three years** from the ending of the authorisation and will contain the following information:

- The type of authorisation;
- The date the authorisation was given;
- The name and title of the Authorising Officer;

- The unique reference number of the investigation (URN);
- The title of the investigation or operation, including a brief description and the names of the subjects, if known;
- Whether the urgency provisions were used and if so why;
- Whether the investigation will obtain confidential information;
- Whether the authorisation was granted by an individual directly involved in the investigation;
- The dates the authorisation is reviewed and the name and title of the Authorising Officer;
- If the authorisation is renewed, when it was renewed and the name and title of the Authorising Officer;
- The date the authorisation was cancelled.

Access to the data will be restricted to the RIPA Co-ordinator and Authorising Officers to maintain the confidentiality of the information.

Section H

AUTHORISATION PROCEDURES

1. Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.

Appendix 1 provides a flow chart of the process from application consideration to recording of information.

Authorising Officers

Forms can only be signed by Authorising Officers. The Authorising Officers are:

Chief Executive	Tony Goodwin
Deputy Chief Executive	John Wheatley
Deputy Director Assets & Environment	Andrew Barratt
Deputy Director Community, Planning & Partnerships	Rob Mitchell

Appointment of the aforesaid officers is subject to the training requirements set out in the paragraph below.

Authorisations under RIPA are separate from delegated authority to act under the Council's Scheme of Delegation and any internal departmental Schemes of Management.

RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete or about to expire. **The authorisations do not lapse with time.**

Authorising officers should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently or for security reasons. Where an authorising officer authorises such an investigation or operation the centrally retrievable record of authorisations should highlight this and the attention of a Commissioner or Inspector should be invited to it during the next inspection.

Training

Authorising Officers will only be appointed if the Chief Executive is satisfied that they have undertaken suitable training on RIPA. Evidence of suitable training is to be supplied in the form of a certificate/confirmation from the trainer to the effect that the Authorising Officer has completed a suitable course of instruction.

The Solicitor to the Council will maintain a Register of Authorising Officers and details of training undertaken by them.

If the Chief Executive is of the view that an Authorising Officer has not complied fully with the requirements of this document, or the training requirements then that Officer's authorisation can be withdrawn until they have undertaken further approved training or has attended a one-to-one meeting with the Chief Executive.

Application Forms

Only the approved RIPA forms referred to in Appendices 2 and 3 must be used.
The forms have to be downloaded and completed in the applicant's handwriting.

Grounds for Authorisation

Directed Surveillance (A Forms) or the Conduct and Use of the CHIS (B Forms) can be authorised by the Council only on the ground of:-

preventing or detecting crime or preventing disorder.

No other ground is available.

Assessing the Application Form

The following information should be included on the application form:

- the reasons why the authorisation is necessary in the particular case and on the grounds listed in Section 28(3)b of RIPA;
- the nature of the surveillance and the precise location it is to take place;
- the identities, where known, of those to be the subject of the surveillance;
- a summary of the intelligence case and appropriate unique intelligence references where applicable;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve and detail of less intrusive options that have been considered.

Before an Authorising Officer signs a Form, they must:-

(a) Be mindful of this Policy & Procedures Document and the training undertaken
(b) Be satisfied that the RIPA authorisation is:-

(i) **in accordance with the law;**

(ii) **necessary** in the circumstances of the particular case on the ground mentioned in paragraph 10 above; **and**

(iii) **proportionate** to what it seeks to achieve.

(c) In assessing whether or not the proposed surveillance is proportionate, consider other appropriate means of gathering the information.

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:

- *balance the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;*
- *explain how and why the methods to be adopted will cause the least possible intrusion on the subject and others;*
- *consider whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;*
- *evidence, what other methods have been considered and why they were not implemented.*

The least intrusive method will be considered proportionate by the courts.

(d) Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (**collateral intrusion**). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion. This matter may be an aspect of determining proportionality;

(e) Set a date for review of the authorisation and review on only that date;

(f) Obtain a Unique Reference Number (URN) for the application from the Solicitor to the Council on 01827 709258

(g) Ensure that a copy of the RIPA Forms (and any review/cancellation of the same) is forwarded to the Solicitor to the Council, Central Register, **within 5 working days of the relevant authorisation, review, renewal, cancellation or rejection.**

Additional Safeguards when Authorising a CHIS

When authorising the conduct or use of a CHIS, the Authorising Officer must also:-

(a) be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved.

(b) Be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk assessment;

(c) Consider the likely degree of intrusion of all those potentially affected;

(d) Consider any adverse impact on community confidence that may result from the use or conduct or the information obtained;

(e) Ensure **records** contain particulars and are not available except on a need to know basis.

(f) Ensure that if the CHIS is under the age of 18 or is a vulnerable adult the Authorising Officer is the Chief Executive or in his absence, the Deputy Chief Executive.

The Authorising Officer must attend to the requirement of section 29(5) RIPA and of the Regulation of Investigatory Powers (Source Records) Regulations 2000. It is strongly recommended that legal advice is obtained in relation to the authorisation of a CHIS.

Urgent Authorisations

Urgent authorisations should not be necessary.

In exceptional circumstances, however, urgent authorisations may be given orally if the time that would elapse before a written authorisation can be granted would be likely to jeopardise the investigation or operation for which the authorisation was being given.

It will not be urgent where the need for authorisation has been neglected or is of the Officer's own making.

Urgent authorisations last for no more than 72 hours. They must be recorded in writing on the standard form as soon as practicable and the extra boxes on the form completed to explain why the authorisation was urgent.

Urgent authorisations can only be granted by the Chief Executive or in his absence the Deputy Chief Executive.

Duration

It is important that all those involved, including applicants and practitioners, in undertaking directed or intrusive surveillance activities or interference with property under the 2000 Act, 1997 Act or 1994 Act are fully aware of the extent and limits of the authorisation.

The Form **must be reviewed in the time stated and cancelled** once it is no longer needed.

*The 'authorisation' to carry out/conduct the surveillance lasts for **3 months** (from authorisation) for Directed Surveillance. Accordingly, a written authorisation granted by an authorising officer will cease to have effect (unless renewed or cancelled) at*

the end of a period of three months beginning with the time at which it took effect. An authorisation for a CHIS lasts for 12 months (from authorisation).

However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the 'authorisation' is 'spent'. In other words, **the forms do not expire.** The forms have to be reviewed and/or cancelled (once they are no longer required).

Urgent oral authorisation, if not already ratified in a written authorisation, will cease to have effect after 72 hours, beginning with the time when the authorisation was granted.

Authorisations can be renewed in writing when the maximum period 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. All authorisations should be reviewed based on the level of collateral intrusion or the amount of confidential information obtained. Authorising Officers should set review dates based on the likelihood of this information being captured.

The renewal will begin on the day when the authorisation would have expired. In exceptional circumstances, renewals may be granted orally in urgent cases and last for a period of seventy-two hours.

Section I

WORKING WITH / THROUGH OTHER AGENCIES

When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. The agency must be made aware explicitly what they are authorised to do.

When another agency (e.g. Police, Customs & Excise, Inland Revenue etc):-

(a) wishes to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any Officer agrees to allow the Council's resources to be used for the other agency's purposes, the Officer must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the Solicitor to the Council for the Central Register) and/or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources;

(b) wish to use the Council's premises for their own RIPA action, the Chief Officer or Head of Service should, normally, cooperate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's cooperation in the agent's RIPA operation. In such cases, however, the Council's own RIPA forms should not be used as the Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

If the Police or any other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the police or other Agency before any Council resources are made available for the proposed use.

Any person granting or applying for an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of any similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. It is therefore recommended that where an authorising officer from a public authority considers that conflicts might arise they should consult a senior officer within the police force area in which the investigation or operation is to take place.

If in doubt, please consult with the Solicitor to the Council at the earliest opportunity.

Section J

RECORD MANAGEMENT

The Council must keep detailed records of all authorisations, renewals, cancellations and rejections in Departments and a Central Register of all Authorisation Forms will be maintained and monitored by the Solicitor to the Council.

Records Maintained in the Department

The following documents must be retained by the Department authorising the surveillance:

- a copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the Authorising Officer;
- the Unique Reference Number for the authorisation (URN).

Central Register maintained by the Solicitor to the Council

Authorising Officers must forward a copy of the form to the Solicitor to the Council for the Central Register, within 5 working days of the authorisation, review, renewal, cancellation or rejection. The Solicitor to the Council will monitor the same and give appropriate guidance to Authorising Officers from time to time, or amend this document in the light of changes of legislation or developments through case law.

Retention and Destruction of Material

Arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed or intrusive surveillance or property interference. Authorising Officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 1998 and any relevant codes of practice produced by individual authorised relating to the handling and storage of material.

The Council will retain records for a period of at least three years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) can audit/review the Council's policies and procedures, and individual authorisations.

The Office of the Surveillance Commissioners will also write to the Council from time to time, requesting information as to the numbers of authorisations made in a specific period. It will be the responsibility of the Solicitor to the Council to respond to such communications.

Section K

ACQUISITION OF COMMUNICATIONS DATA

What is Communications Data?

Communication data means any traffic or any information that is or has been sent by or over a telecommunications system or postal system, together with information about the use of the system made by any person.

Powers

There are two powers granted by S22 RIPA in respect of the acquisition of Communications Data from telecommunications and postal companies ("Communications Companies").

S22 (3) provides that an authorised person can authorise another person within the same relevant public authority to collect the data. This allows the local authority to collect the communications data themselves, i.e. if a private telecommunications company is technically unable to collect the data, an authorisation under this section would permit the local authority to collect the communications data themselves.

In order to compel a communications company to obtain and disclose, or just disclose communications data in their possession, a notice under S22 (4) RIPA must be issued. The sole grounds to permit the issuing of a S22 notice by a permitted Local Authority is for the purposes of "preventing or detecting crime or of preventing disorder". The issuing of such a notice will be the more common of the two powers utilised, in that the Communications Company will most probably have means of collating and providing the communications data requested.

Single Point of Contact

In accordance with the Home Office Acquisition and Disclosure of Communications Data Code of Practice the Council is required to have a "Single Point of Contact" ("SPoC"). The role of the SPoC is to enable and maintain effective co-operation between a public authority and communications service providers in the lawful acquisition and disclosure of communications data. Before an officer can be a SPoC specialist training recognised by the Home Office has to be undertaken. A SPoC must also register his or her details with the Home Office. The Solicitor the the Council is SPoC for Tamworth Borough Council.

Details of the training undertaken is kept in the Central Register.

The functions of the SPoC are to:

- Assess, where appropriate, whether access to communications data is reasonably practical for the postal or telecommunications operator;

- Advise Applicants and Authorising Officers on the practicalities of accessing different types of communications data from different postal or telecommunications operators
- Advise Applicants and Authorising Officers on whether communications data falls under section 21(4)(a), (b) or (c) of RIPA
- Provide safeguards for authentication
- Assess any cost and resource implications to both the Council and postal or telecommunications operator.

The Senior Responsible Officer

In accordance with the Code of Practice each public authority must have a Senior Responsible Officer who is responsible for:

- The integrity of the process in places within the public authority to acquire communications data;
- Compliance with Chapter II of Part 1 of RIPA and with the Code;
- Oversight of the reporting of errors to the Interception of Communications Commissioner's Office (IOCCO) and the identification of both the cause 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

The Council's Senior Responsible Officer is the Solicitor to the Council.

Application Forms

Only the approved Accessing Communications Data forms referred to in Appendix 4 must be used. The forms have to be downloaded and completed in the Applicants handwriting

Procedure

All applications to obtain communications data must be channelled through the SPoC. If an investigating officer is considering making an application to obtain communications data they should contact the SPoC for advice and to obtain the appropriate forms.

In completing the forms the investigating officer must address the issues of necessity, proportionality and collateral intrusion. The following is guidance on the principles of necessity, proportionality and collateral intrusion.

"Necessity" should be a short explanation of the crime (together with details of the relevant legislation), the suspect, victim or witness and the telephone or communications address and how all these three link together. It may be helpful to outline the brief details of the investigation and the circumstances leading to the application as this will assist with justifying necessity. The source of the telephone number or communications address should also be outlined. E.g. if the number was

obtained from itemised billing or a business flyer there should be specific identifiers such as the telephone number or exhibit number.

As regards “proportionality” there should be an outline of what the investigating officer expects to achieve 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. The investigating officer should give an explanation as to why specific date/time periods of data have been requested. An explanation of what is going to be done with the communications data once it is acquired and how that action will benefit the investigation will assist with the justification of proportionality. The investigating officer should outline what other checks or methods have been tried e.g. visiting other known addresses, ringing the number etc or why such methods are not deemed feasible.

“Collateral intrusion” should also be addressed on the suspect or individual in question to demonstrate that the intrusion is not arbitrary or unfair. There will only be minimal collateral intrusion in relation to subscriber checks or none will be identified at the time of making the application. In some case it will be clear that the suspect has been contacted on the actual telephone number by the complainant or the investigating officer and therefore this reduces the potential for collateral intrusion. Investigating officers should also mention whether it is known that the telephone number (or other type of data) has been used to advertise the business, either in the press/internet or on business cards/flyers as this would also be evidence to show that the suspect is actually using the telephone number and further reduce the potential for collateral intrusion. Collateral intrusion becomes more relevant when applying for service use data and investigating officers should outline specifically what collateral intrusion may occur, how the time periods requested impact on collateral intrusion and whether they are likely to obtain data which is outside the realm of their investigation.

Once the investigating officer has completed the application form it should be passed to the SPoC together with a draft Notice to the Communications Service Provider. If the SPoC is satisfied that the application should proceed, the Application and the draft Notice to the Communications Service Provider will be considered by an Authorising Officer[1]. If the SPoC decides that the application is not justified it will be rejected. If the SPoC requires further information in order to consider the application this will be requested from the investigating officer and recorded on the SPoC Log Sheet.

The Authorising Officer must consider:

(a) whether the case justifies the accessing of communications data for the **purposes of preventing or detecting crime or of preventing disorder** and why obtaining the data is **necessary;**

and

(b) whether obtaining access to the data by the conduct authorised, or required of the postal or telecommunications operator in the case of a notice, is **proportionate** to what is sought to be achieved.

The Authorising Officer will complete the Application Form as appropriate.

If the Authorising Officer becomes directly involved in the operation, such involvement and their justification for undertaking the role of Authorising Officer must be explicit in the written considerations on the Application Form or alternatively the application should be passed to another Authorising Officer for consideration.

If the accessing of communications data is authorised the Authorising Officer will sign the Notice to the Communication Service Provider, complete the date/time of issue and return all forms to the SPoC

The SPoC will then issue the Notice to the Communications Service Provider

1. NOTE: The Code of Practice referred to in paragraph 5 above refers to "Designated Persons" as those whose authority is obtained with regard to the application. However, for the purposes of this policy and procedure the term "Authorising Officer" will be used for that of "Designated Person".

Duration

Authorisations and notices are only valid for one month. A shorter period should be specified if this is satisfied by the request. An authorisation or notice may be renewed during the month by following the same procedure as obtaining a fresh authorisation or notice.

An Authorising Officer shall cancel an authorisation or notice as soon as it is no longer necessary or the conduct is no longer proportionate to what is sought to be achieved. The duty to cancel a notice falls on the Authorising Officer who issued it.

Record Management

Applications, authorisations and notices for communications data must be retained by the SPoC until audited by the IOCCO. All such documentation must be kept in locked storage.

Errors

Where any errors have occurred in the granting of authorisations or the giving of notices, a record shall be kept and a report and explanation sent to the IOCCO as soon as reasonably practicable.

Oversight

The IOCCO will write to the Council from time to time requesting information as to the numbers of applications for communications data and confirmation as to whether there have been any errors which have occurred when obtaining data communications. It will be the responsibility of the Solicitor to the Council to respond to such communications.

Section L

CONCLUSION

Obtaining an authorisation under RIPA and following the guidance and procedures in this document will assist in ensuring that the use of covert surveillance or a CHIS is carried out in accordance with the law and subject to safeguards against infringing an individual's human rights. Complying with the provisions of RIPA protects the Council against challenges for breaches of Article 8 of the European Convention on Human Rights.

Authorising Officers will be suitably trained and they must exercise their minds every time they are asked to sign a Form. They must never sign or rubber stamp Form(s) without thinking about their personal and the Council's responsibilities.

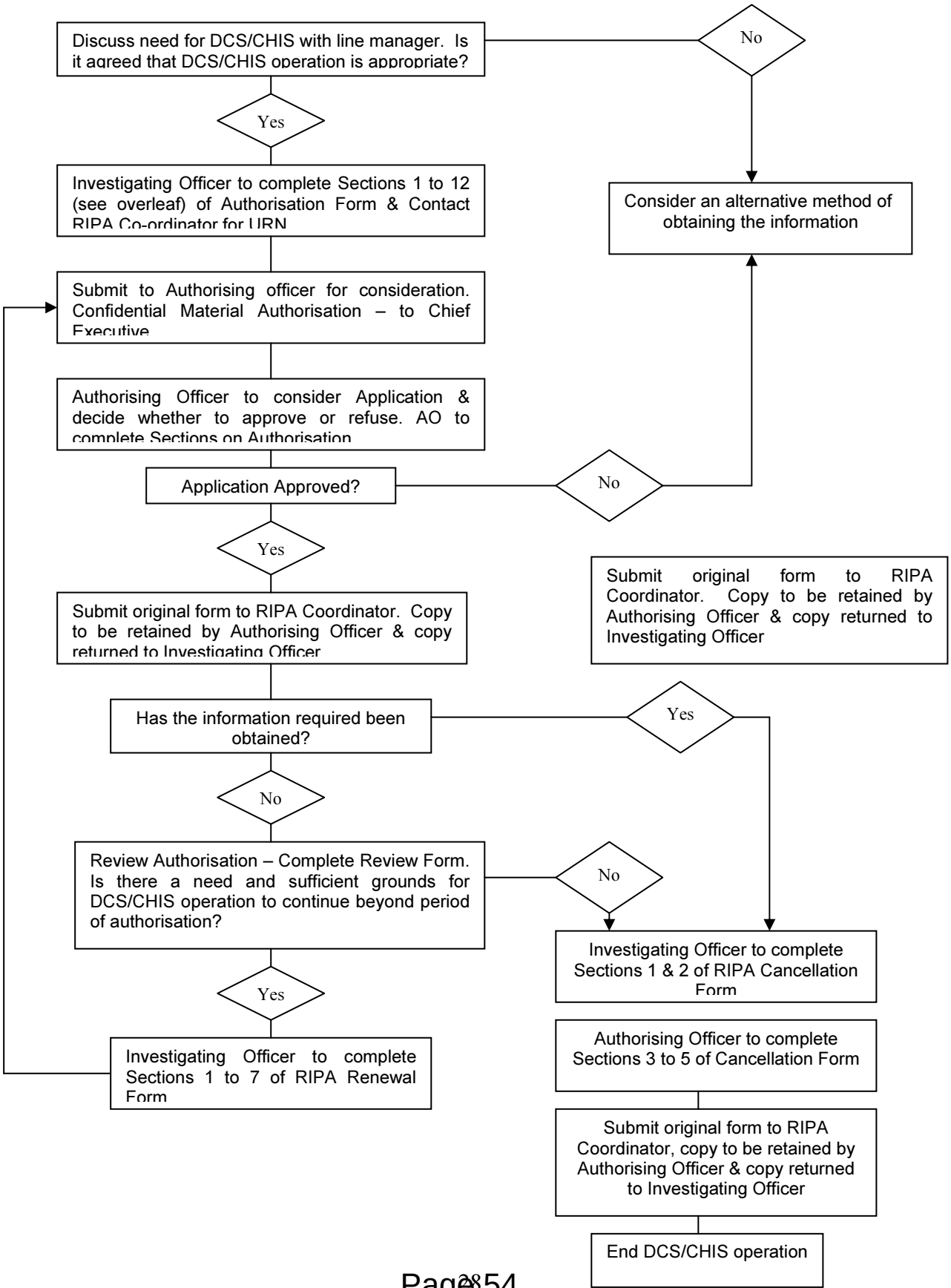
Any boxes not needed on the Form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and the form retained for future audits.

For further advice and assistance on RIPA, please contact the Solicitor to the Council (who is also the Monitoring Officer).

APPENDIX 1

It is important that all those involved including applicants, practitioners and authorising officers in undertaking directed or intrusive surveillance activities or interference with property under the 2000 Act or 1994 Act are fully aware of the extent and limits of the authorisation.

PROCEDURE FOR OBTAINING RIPA



APPENDIX 2

A FORMS

DIRECTED SURVEILLANCE

All forms can be obtained from:

http://www.homeoffice.gov.uk/counter-terrorism/ripa-forms/

The form has to be downloaded and completed in the applicant's handwriting. The Authorising Officer must also complete the relevant section of the form in handwriting. The original form has to be passed to the Solicitor to the Council.

Application for Authorisation Directed Surveillance

Application for Review of a Directed Surveillance Authorisation

Application for Renewal of a Directed Surveillance Authorisation

Application for Cancellation of a Directed Surveillance Authorisation

APPENDIX 3

B FORMS

CONDUCT OF A COVERT HUMAN INTELLIGENCE SOURCE

All forms can be obtained from:

http://www.homeoffice.gov.uk/counter-terrorism/ripa-forms/

The form has to be downloaded and completed in the applicant's handwriting. The Authorising Officer must also complete the relevant section of the form in handwriting. The original form has to be passed to the Solicitor to the Council.

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

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

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

Application for Cancellation of an authorisation for the use or Conduct of a Covert Human Intelligence Source.

APPENDIX 4

C FORMS

ACQUISITION OF COMMUNICATIONS DATA

All forms can be obtained from the Home Office: RIPA Codes of Conduct website: http://www.homeoffice.gov.uk/counter-terrorism/ripa-forms/

The form has to be downloaded and completed in the applicant's handwriting. The Authorising Officer must also complete the relevant section of the form in handwriting. The original form has to be passed to the Solicitor to the Council.

Part I Chapter II request schedule for subscriber information

Specimen Part I Chapter II authorisation

Specimen Part I Chapter II Notice

Chapter II application for communications data

Guidance notes regarding chapter II application form

RIPA Section 22 notice to obtain communications data from communications service providers

Reporting an error by a CSP to the IOCCO

Reporting an error by a public authority to the IOCCO

Appendix 5

USE OF COVERT SURVEILLANCE EQUIPMENT – Technical Guidance

1. Introduction

The use of covert CCTV systems across the Tamworth Borough Council is governed by law and policy. The The CCTV and Parking Manager Manager has to ensure the Council comply with the provisions of the Data Protection Act 1998, the Human Rights Act 1998 and the Regulation of Investigatory Powers Act 2000. Compliance with these Acts, their associated Codes of Practice and the council's RIPA Policy will assist the users of the surveillance equipment in meeting their legal obligations.

2. Initial Assessment Procedures

Before installing and using covert surveillance equipment users will need to ENSURE authorisation to install surveillance had been obtained and establish the purpose or purposes for which they intend to use the equipment, as the First Data Protection Principle requires Data Controllers to have a legitimate basis for processing personal data, in this case images of individuals. Hence the following procedures should be carried out:

1. Assess the appropriateness of, and reasons for, using CCTV or similar surveillance equipment and document this process.

2. Establish the purpose of the operation.

3. Establish the person or persons responsible for ensuring the day-to-day compliance with this Code of Practice.

4. Establish the associated security and disclosure policies.

5. Obtain the approval of the authorising officer for this activity by using the specified forms and processes set out in the RIPA Policy.

There are only 4 persons in Tamworth Borough Council who can authorise surveillance operations:-

Chief Executive,
Deputy Chief Executive,
Corporate Director Resources and
Deputy Director Assets and Environment.

3. Equipment

The Council currently has access to surveillance systems. The system consists of two types of covert systems; one for internal locations which has three cameras and one hard drive recorder. The second system for external use

consists of a battery box, 6 bullet cameras and two hard drive recorders. All the equipment is kept in locked storage and can only be accessed by key, which is managed by a diary. All equipment being removed MUST be logged out in the dairy. The CCTV and Parking Manager has sole access to the data collected.

4. Deploying the Systems/cameras

1. The equipment should be sited in such a way that it monitors only the area intended, i.e. where the incident of fly tipping is likely to occur.

2. The user/s should only use the covert system/s as set out in the authorisation document.

3. Investigating officers must be aware of the purpose(s) for which the operation has been established.

4. Investigating officers are expected to fill in the appropriate risk assessment and premises consent forms when necessary.

5. Handling of the Images

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. The following standards should therefore be observed:

1. Carry out an initial check on installation to ensure that the equipment performs properly.
2. Ensure that, where tapes are used they are of good quality.
3. Images should be retained until prosecution is completed.
4. ALL storage discs must be kept in the metal locked cupboard except in the case of viewing, production as evidence of court proceeding.
5. Media should not continue to be used once it becomes clear that the quality of the images has begun to deteriorate.
6. All systems and cameras should be properly maintained and serviced to ensure that clear images are recorded and a maintenance log kept.
7. Cameras should be protected from vandalism in order to ensure that they remain in working order.

6. Processing the Images

To maintain the integrity of the images and to protect the rights of the individual, the following standards should be maintained:

1. Access to recorded images should be restricted to the person responsible for managing the investigation (the Data Owner) or his/her nominee who will decide whether to allow requests for access by third parties.
2. Where images are retained, it is essential that their integrity be maintained, whether to ensure their evidential value or to protect the rights of the people whose images may have been recorded.

3. Images should not be retained for longer than is necessary; once the retention period has expired, the images should be removed or erased. If in doubt. Speak to the The CCTV and Parking Manager Manager or Legal Services.
4. If the images are retained for evidential purposes, they should be kept in a secure place (locked metal cupboard) to which access is controlled.
5. On removing the medium on which images have been recorded for use in legal proceedings, the operator should ensure that s/he has documented the date on which the images were removed from the general system for such use, the reason for doing so, any crime incident number to which the images may be relevant, the new location of the images and the signature of the person collecting the images. In such instances this will only be officer from Staffordshire Police or an Authorising officer within the Council.

7. Access to and Disclosure of Images to Third Parties

It is important that access to, and disclosure of, the images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled, not only to ensure that the rights of the individual are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. Staff should maintain the following standards:

1. Access to recorded images should be restricted to those staff who need to have access in order to achieve the purpose(s) of using the recording equipment.
2. All access to the medium on which images are recorded should be documented.
3. Disclosure of recorded images to third parties, whether officers of the Enforcement Team or not, should only be made in limited and prescribed circumstances.
4. All requests for access or for disclosure should be recorded and, if access is denied, the reason should be documented.
5. If access to or disclosure of images is allowed, then the following should be recorded:
    - The date and time access was allowed or disclosure made.
    - The identification of any third party who was allowed access or to whom disclosure was made.
    - The reason for allowing access or disclosure.
    - The extent of the information to which access was allowed or which was disclosed.

8. Monitoring Compliance with this Code of Practice

1. The The CCTV and Parking Manager Manager will undertake regular reviews of the documented procedures and the above processes to ensure that the provisions of this Code are being complied with.