APPENDIX A

Corporate Policy and Procedures Document

On

Regulation of Investigatory Powers Act 2000 (RIPA)

Covert Surveillance, Acquisition of Communications Data and Use of Covert Human Intelligence Sources

INDEX

1. BACKGROUND INFORMATION

1.1. INTRODUCTION

Peterborough City Council ("PCC") has a duty to enforce a wide range of offences arising under legislation relating to public health and safety, quality of life, preservation of public and residential amenity, maintenance of the environment and the protection of public funds. In fulfilment of this, it will in exceptional circumstances become necessary to obtain private information using covert techniques.

PCC's use of covert techniques is governed by The Regulation of Investigatory Powers Act 2000 ("RIPA") and the Home Office's Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources ("the Codes").

PCC recognises and respects the privacy of the people within the community it serves and takes very serious its statutory responsibilities in this respect. The purpose of this Policy is therefore to outline the covert techniques available to PCC as well as when, how and by whom they should be used in order to ensure strict compliance with RIPA and the Codes.

Both directly employed staff and external agencies are covered by RIPA and therefore this Policy at all times whilst they are working for PCC.

This Policy will be reviewed annually by the Senior Responsible Officer. At all other times throughout the year the RIPA Group will monitor changes to any relevant legislation and guidance to ensure that this Policy is updated at the earliest opportunity. The most up-to-date and authoritative position will remain within the Act and Codes themselves and persons are therefore encouraged to read this Policy in conjunction with them and/or make enquiries with the Compliance and Ethical Standards Manager in the event of *any* uncertainty.

The Compliance and Ethical Standards Manager will maintain and check the Corporate Register of all RIPA authorisations, reviews, renewals, cancellations and rejections as well as organising training and development opportunities for Officers of PCC tasked with implementing or where appropriate supervising the implementation of this Policy. Regular training and awareness programmes will also be delivered to elected Members who have a scrutiny role in the use of RIPA.

PCC has and will continue to be inspected by the Office of Surveillance Commissioners ("the OSC") whose representatives are required to review and provide independent oversight of the use of RIPA. PCC will work with the OSC's representatives as part of this process and will ensure compliance with any recommendations made.

An electronic copy of this Policy will be available within the Regulatory Powers and Investigation Section of Insite and should be read with reference to the RIPA Toolkit which can be found in the same location.

1.2. SUBORDINATE LEGISLATION/CONSIDERATIONS

1.2.1. General

It is essential for the purpose of preserving the rights of individuals and the reputation of PCC that all involved with RIPA carefully consider their obligations under and ensure compliance with all subordinate legislation and guidance.

A failure to comply with legislative requirements is likely to expose PCC to legal risk which will inevitably result in financial and reputational implications.

1.2.2. Human Rights Act

The Human Rights Act 1998 requires PCC 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 correspondence. However, this provision is qualified in that interference with it is permitted where it is:

- In accordance with the law;
- Necessary; and
- Proportionate.

Where properly applied RIPA provides the statutory basis through which interference will be lawful and consideration of the necessity and proportionality of an application should occur in all circumstances.

1.2.3. Data Protection Act

Authorising Officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of material. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer.

1.2.4. Confidential Material

It is a requirement of every application that due consideration is given to the likelihood that an authorisation will result in the acquisition of confidential material.

Authorisation and use of covert techniques which will or are likely to result in confidential material being obtained are subject to additional safeguards and may only be granted by the Chief Executive.

Where the proposed use of covert techniques is likely to or will result in confidential material being obtained this should be specifically highlighted as part of the application process.

Where, after an authority has been granted it becomes apparent that the approved use of a covert technique is likely immediate advice should be sought from the Compliance and Ethical Standards Manager.

"Confidential Material" consists of:

(a) Matters Subject to Legal Privilege;

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

(b) Confidential Personal Information

Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples include consultations between a health professional and patient or information from a patient's medical record.

Spiritual counselling will include conversations with a Minister of Religion acting in his-her official capacity were the person being counselled is seeking or the Minister is imparting forgiveness or absolution of conscience.

(c) Confidential Journalistic Material

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

1.3. SENIOR RESPONSIBLE OFFICER AND THE ROLE OF COUNCILLORS

PCC has and will continue to appoint a Senior Responsible Officer who will be responsible for:

- The integrity of the processes PCC has put in place for the management and use of covert techniques;
- Compliance with RIPA and any related legislation and Guidance;
- Engagement with the OSC inspectors when they conduct their inspections; and
- Where necessary oversight of the implementation of the post-inspection action plans.

Details of the currently appointed Senior Responsible Officer can be viewed within the 'RIPA Group and Authorised Officers' section of the RIPA Toolkit.

It shall be the role of the Audit Committee to annually review PCC's use of RIPA and to set the general surveillance Policy. Furthermore, Members of the Audit Committee shall on a quarterly basis consider internal reports on the use of RIPA to ensure that it is being used consistently with this Policy and that this Policy remains fit for purpose in that respect.

1.4. AUTHORISING OFFICERS

The Senior Responsible Officer will ensure that a sufficient number of key personnel within PCC are trained and appointed as 'Authorising Officers' for the purpose of assessing and granting applications from staff or agents wishing to use covert techniques.

Key personnel for these purposes will be limited to Directors, Heads of Services, Service Managers or their equivalents.

A List of currently authorised personnel can be viewed within the 'RIPA Group and Authorised Officers' section of the RIPA Toolkit.

Authorised Officers must fully familiarise themselves with the contents of this Policy as well as the Codes. In the event of *any* uncertainty on the part of the Authorising Officer as to the credibility of an application or ongoing authorisation, advice should be sought from the Compliance and Ethical Standards Manager.

It will be the responsibility of Authorising Officers to ensure that covert techniques are not utilised without appropriate authorisation and that the applications received by them comply with the requirements of this Policy.

Authorising Officers must also pay attention to Health and Safety issues that may arise in consequence of a covert technique being used. The use of a covert techniques is strictly prohibited unless the Authorising Officer is satisfied that the health and safety of PCC's employees or authorised agents are suitably addressed and/or associated risks are minimised so far as is possible and proportionate to the required aim.

1.5. USEFUL WEBSITES

General Guidance
www.surveillancecommissioners.gov.uk

RIPA Forms
http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms

Code of Practice- Surveillance
http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-covert

Code of Practice- Covert Human Intelligence
http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-practice-human-intel

Code of Practice – Acquisition and Disclosure of Communications Data
http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-acquisition

2. COVERT TECHNIQUES

2.1. SURVEILLANCE

2.1.1. Introduction

Most of the surveillance carried out by PCC will be done overtly i.e. there will be nothing secretive about it. In many cases, Officers will be behaving in the same way as a member of the public and will be openly undertaking PCC's business. Similarly, surveillance will be overt if the subject(s) have been told it will happen (e.g. where a noisemaker is warned in writing that the noise will be recorded if it is not abated).

RIPA regulates the use of directed and intrusive covert surveillance however, Local Authorities such as PCC can only be authorised to undertake covert directed surveillance as set out below.

Practical examples relating to the application of this Policy can be viewed within the RIPA Toolkit.

Please note that PCC is strictly prohibited in any circumstance from the use of any covert technique which may involve 'property interference' which is taken to include entry on or interference with property or with wireless telegraphy.

2.1.2. What is Surveillance?

Surveillance includes:

- monitoring, observing or listening to persons, watching or following their movements, listening to their conversations and other such activities or communication;

- recording anything mentioned above in the course of authorised surveillance; and

- surveillance by or with the assistance of a surveillance device.

2.1.3. When is Surveillance Covert?

Surveillance is covert when it is carried out in a manner calculated to ensure that the subject or others affected by it are unaware that it is or may be taking place.

Covert surveillance will not be necessary (and therefore compliant with the Human Rights Act) in circumstances where there are reasonably available overt means of obtaining the same information.

2.1.4. When is Surveillance Directed?

Surveillance is 'Directed' if it is not intrusive and is undertaken:

- for the purposes of a specific investigation or a specific operation;

- in such a manner as is likely to result in the obtaining of private information about a person (whether or not such a person is specifically identified for the purposes of the investigation or operation); and

- otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

2.1.5. What is Private Information

Private information includes any information relating to an individual's private or family life, their home and correspondence.

The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in obtaining private information about a person.

Prolonged surveillance targeted on a single person will undoubtedly result in obtaining private information about them and others that they come into contact or associated with. Accordingly, the use of overt CCTV cameras may require authorisation in circumstances where they are to be directed for a specific purpose to observe particular individuals.

2.1.6. When will Surveillance Amount to an 'Immediate Response'?

RIPA recognises that in circumstances where an immediate response to events is required it may not be possible to obtain prior authority to undertake surveillance which might otherwise fall within its remit.

The opportunities for those circumstances to arise are very narrow and specific for example, using overt CCTV cameras to specifically track the movements of a person who has just committed a street crime. However, if as a result of that immediate response specific monitoring of that person is undertaken for the purpose of obtaining "private information" about him/her then authorisation is required.

2.1.7. When is Surveillance Intrusive?

Surveillance is Intrusive if it:

- Is covert; and

- is carried out in relation to anything taking place on any "residential premises" or in any "private vehicle"; and

- involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

PCC'S Employees and/or its agents or representatives are not permitted to authorise or carry out intrusive surveillance *in any circumstance.*

2.1.8. Authorising Surveillance

For covert directed surveillance an Authorising Officer will not grant an authorisation unless he/she believes (and the prescribed forms require that the factors below are shown to have been taken into account):

(a) that an authorisation is necessary; and

(b) that the authorised surveillance is proportionate to what is sought to be achieved by carrying it out.

NECESSITY

RIPA specifically prescribes the circumstances in which an application for directed surveillance may be granted with the most applicable to PCC being:

- for the purpose of preventing or detecting crime or of preventing disorder.

PROPORTIONALITY

An authorisation will be proportionate if the person granting the authorisation has balanced the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in investigative or operational terms. The activity will not be proportionate if it is excessive in the overall circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means.

The following are therefore relevant considerations:

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

COLLATERAL INTRUSION

Collateral intrusion will arise in any circumstance where there is a risk to the privacy of persons other than those who are directly the subject of the investigation. In any such circumstances measures should be wherever practicable to avoid or minimise unnecessary intrusion.

Such collateral intrusion or interference would be a matter of greater concern in cases where there are special sensitivities, for example in cases of premises used by lawyers or for any form of medical or professional counselling or therapy, or in a particular community.

Any application for authorisation or renewal should include an assessment of risk of any collateral intrusion or interference. The authorising officer will take this into account in considering the proportionality of the request.

The obligation to be mindful of collateral intrusion continues throughout the life of the authorisation and those responsible for carrying out the permitted surveillance should inform the Authorising Officer immediately if there is an unexpected interference with the privacy of unconnected individuals. The Authorising Officer should consider whether the authorisation requires amendment or reauthorisation in order to ensure compliance with RIPA.

More information as to the definition and authorisation of covert directed surveillance can be found within the Home Office Guidance entitled 'Covert Surveillance and Property Interference' as referenced within the Useful Websites section of this Policy.

2.2. COVERT USE OF HUMAN INTELLEGENCE SOURCES ("CHIS")

2.2.1. RESTRICTIONS ON USE

The use of a CHIS will only be authorised in exceptional circumstances.

At all times extreme caution should be taken to ensure that the ordinary provision of information by members of the public does not give rise to a situation in which authorisation would be required.

In any circumstance in which it is proposed that a CHIS should be utilised to obtain information, advice should first be sought from PCC's Monitoring Officer or their duly nominated representative.

2.2.2. Who is a CHIS?

A person is a CHIS if:

- He/she establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything either of the following;
    - Covertly using the relationship to obtain information or provide access to any information to another person; or
    - Covertly disclosing information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose.

The above clearly covers the use of professional witnesses where they are required to obtain information and evidence in such circumstances.

2.2.3. What Must be Authorised

Both the conduct and the use of a CHIS must be authorised. I.e. it is not only the actions of the CHIS that will require prior approval but also the decision to use one and any subsequent attempts to induce, ask or assist a person to carry out those actions.

Authorisation is not required 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 (e.g. a Housing Benefit Fraud hotline).

Practical examples relating to the application of this Policy can be viewed within the RIPA Toolkit.

2.2.4. Authorisation

Similarly to the authorisation of surveillance, in order for an application to be granted, the proposed use and conduct of the CHIS should be necessary and proportionate to the required aim. Equally, necessity will be established in circumstances where the proposed use and conduct of the CHIS is for the prevention and detection of crime or the prevention of disorder. Further, the same principles will apply in determining proportionality.

Applications may only be authorised by the Chief Executive in consultation with the Senior Responsible Officer.

Before granting any application, consideration must be given to the safety and welfare of the CHIS and the foreseeable consequences to others of the tasks they are asked to carry out. A risk assessment should be carried out before authorisation is given. Consideration from the start, for the safety and welfare of the CHIS, even after cancellation of the authorisation, needs to be considered.

The Applicant will have day-to-day responsibility for dealing with the CHIS and for their security and welfare. The Senior Responsible Officer will be responsible for the management and supervision of the Applicant in this context.

The Applicant must keep a detailed record of the tasks undertaken by the CHIS. Any such records should be provided to the Senior Responsible Officer for retention in accordance with the Regulation of Investigatory Powers (Source Records) Regulations. The Senior Responsible Officer will at all times have general oversight of the records to ensure compliance with the authorisation.

2.2.5. Additional Considerations

2.2.5.1. Juvenile Sources

Special safeguards apply to the use or conduct of juvenile sources (i.e. persons under 18 years of age).

On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to given information against his parents or any person who has parental responsibility for them.

2.2.5.2. Test Purchasing by Juvenile Sources

In any circumstance where a test purchasing exercise is proposed, officers must carefully consider whether or not the circumstances will bring into effect a relationship between the seller and buyer sufficient to require authorisation.

Practical examples relating to the application of this Policy can be viewed within the RIPA Toolkit.

2.2.5.3. 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 themselves or protect themselves against significant harm or exploitation.

A vulnerable individual will only be authorised to act as a CHIS in the most exceptional of circumstances.

More information as to the definition and authorisation of a CHIS can be found within the Home Office Guidance entitled 'Covert Human Intelligence Sources'' as referenced within the Useful Websites section of this Policy.

2.2.6. COMMUNICATIONS DATA

2.2.6.1. What is Communications Data?

Communications 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.

Practical examples relating to the application of this Policy can be viewed within the RIPA Toolkit.

2.2.6.2. Authorisation

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 Communications Service Provider is technically unable to collect the data, an authorisation under the section would permit the local authority to collect the communications data themselves.

In order to compel a Communications Service Provider to obtain and disclose, or just disclose Communications Data in their possession, a notice under S22 (4) RIPA must be issued.

The sole ground 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 Service Provider will most probably have means of collating and providing the communications data requested.

Once a notice has been issued, it must be sent to the Communications Service Provider. In issuing a notice, the Authorising Officer can authorise another person to liaise with the Communications Service Provider covered by the notice.

The Council's Compliance and Ethical Standards Manager is an accredited Home Office Single Point of Contact (SPoC) and is the authorised person permitted to liaise with the Communications Service Providers. All approaches should be made *via* this officer.

3. AUTHORISATION

3.1. GENERAL

Before any officer of the Council undertakes surveillance of any individual(s) they must assess whether the activity is directed or intrusive and as such requires authorisation.

In order to ensure that authorising officers have sufficient information to make an informed decision it is important that detailed records are maintained. The prescribed forms (held by the Authorising Officer) must be fully completed.

It is also sensible to make any authorisation sufficiently wide enough to cover all that is required. This will also enable effective monitoring of what is done against what is authorised.

3.2. ORAL/WRITTEN AUTHORISATION

For urgent grants or renewal, oral authorisations are acceptable however confirmation that such authorisation has been given should be recorded in writing by the applicant as a matter of priority. It is not necessary for the full details of the application to be recorded at this stage however, as soon as is reasonably practicable (usually the next working day), those details should also be recorded in writing.

A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the operation or investigation for which the authorisation was being given. An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the applicant's or authorising officer's own making.

In all other cases, authorisations must be in writing. Prescribed forms (held by Authorising Officers) must be used. Officers must direct their mind to the circumstances of the individual case with which they are dealing when completing the form.

Separate forms are to be completed to maintain the distinction between Directed Surveillance, Acquisition of Communications Data and the use of a Covert Human Intelligence Source.

3.3. DURATION OF AUTHORISATIONS

Authorisations under RIPA do not lapse with time and should therefore be reviewed, renewed or cancelled once the specific surveillance is complete (in cases of surveillance or the use of a CHIS) or is about to expire (in all cases). An application will expire at the end of the following periods:

ORAL: within 72 hours beginning with the time when the authorisation was granted.

WRITTEN - CHIS - 12 months beginning with the day on which the authorisation took effect except in the case of juveniles. The authorisation of a juvenile as a CHIS will expire within a period of 1 month.

WRITTEN - Directed Surveillance – 3 months from the grant or last renewal.

WRITTEN - Communications Data – Notices/Authorities issued under s.22 compelling disclosure of Communications Data are only valid for one month but can be renewed for subsequent periods of one month at any time.

3.4. RENEWAL OF AUTHORISATIONS

Any person entitled to grant a new authorisation can renew an existing authorisation in the same terms at any time before it ceases to have effect.

However, for the conduct of a Covert Human Intelligence Source, an Authorising Officer should not renew unless a review has been carried out and that person has considered the results of the review when deciding whether to renew or not. A review must cover what use has been made of the source, the tasks given to them and information obtained.

Authorising Officers are responsible for ensuring that authorisations undergo timely reviews and are cancelled promptly after upon the use of the relevant covert technique no longer being necessary.

3.5. REVIEW OF AUTHORISATIONS

Regular review of authorisations should be undertaken where possible by the original authorising officer to assess the need for the continued use of the relevant covert technique.

In each case the authorising officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable but should not prevent reviews being conducted in response to changing circumstances.

The results of the review need to be sent for recording on the Central Register.

3.6. CANCELLATION OF AUTHORISATIONS

The Authorising Officer who granted or last renewed the authorisation must cancel it where applicable any part of it if he is satisfied the authorisation no longer meets the criteria upon which it was authorised.

As soon as the decision is taken to discontinue the authorisation, the instruction must be given to those involved to cease using the relevant cover technique(s).

The date of cancellation of the authorisation should be centrally recorded and any documentation retained. There is no requirement for any further details to be recorded when cancelling a directed surveillance authorisation however effective practice suggests that a record should be retained detailing the product obtained from the surveillance and whether or not objectives were achieved.

3.7. COMBINED AUTHORISATIONS AND JOINT WORKING

A single authorisation may combine two or more different authorisations under RIPA.

In cases of joint working, for example, with other agencies on the same operation, authority for directed surveillance by a Housing Benefit Investigator must be obtained from the Council's authorising officers. Authority cannot be granted by the authorising officer of another body for the actions of the Council staff and vice versa.

Use of the Council's CCTV systems by other public authorities will be in accordance with the Council's joint protocol in this respect.

3.8. CENTRAL REGISTER AND RETENTION OF RECORDS

It is a requirement that PCC keeps a centrally retrievable record of all authorisations. In compliance with this, a Central Register is kept by the Compliance and Ethical Standards Manager.

Whenever an authorisation is granted, renewed or cancelled (and this includes authorisations issued by the Police or other third parties using Council CCTV or other facilities) the Authorising Officer must arrange for copies to be forwarded to the Compliance and Ethical Standards Manager. Any information forwarded in this way should be placed in a sealed envelope marked both for the attention of the Compliance and Ethical Standards Manager only as well as strictly private and confidential.

Authorisations (together with the application, reviews, renewals and cancellation) should be retained by the Authorising Officer, for a period of 3 years. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review. It is each department's responsibility to securely retain all authorisations within their departments.

3.9. USE OF THE INFORMATION OBTAINED

Subject to compliance with this Policy and the legislative requirements underpinning it, information obtained through the use of cover techniques may be used as evidence in criminal proceedings.

3.10. THE OFFICE OF THE SURVEILLANCE COMMISSIONERS AND THE TRIBUNAL

The Chief Surveillance Commissioner will keep under review, the exercise and performance by the persons on who are conferred or imposed, the powers and duties under RIPA.

A tribunal has been established to consider and determine complaints made under RIPA if it is the appropriate forum. Complaints can be made by persons aggrieved by conduct e.g. direct surveillance. The forum hears application on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that.

The tribunal can order, among other things, the quashing or cancellation of any warrant or authorisation and can order destruction of any records or information obtained by using a warrant or authorisation, and records of information held by any public authority in relation to any person. The Council is however, under a duty to disclose or provide to the tribunal all documents they require if:

- A Council officer has granted any authorisation under RIPA.
- Council employees have engaged in any conduct as a result of such authorisation.
- A disclosure notice requirement is given.

4. CONCLUDING REMARKS

This Policy sets out the options available to Peterborough City Council in using covert techniques to investigate and enforce against criminal behaviour.

Peterborough will take a firm stance with offenders and utilise all appropriate powers in this respect. However, in all circumstances great emphasis will be placed on thehuman rights of citizens and proportionality will be an overriding consideration in granting and reviewing any authorisation.