F

AUDIT COMMITTEE – 10 JANUARY 2014

THE REGULATION OF INVESTIGATORY POWERS ACT 2000

1. INTRODUCTION

1.1. The purpose of this report is to provide the Audit Committee with a summary of the Council's use of its powers under the Regulation of Investigatory Powers Act 2000 (RIPA).

1.2. RIPA provides a statutory framework whereby certain surveillance and information gathering activities can be authorised and conducted by the Council in a lawful manner where they are carried out for the prevention and detection of crime and, in some cases, for the prevention of disorder.

1.3. The Council has adopted two policies relating to its use of RIPA:

1.3.1. Surveillance Policy (**Appendix 1**). Last updated: March 2013

1.3.2. Policy for the Acquisition of Communications Data (**Appendix 2**). Last updated: April 2013

1.4. In accordance with these policies the RIPA Monitoring Officer is required to report to the Audit Committee annually on the Council's use of RIPA.

2. BACKGROUND

2.1. When the Human Rights Act 1998 came into force in 2000 it made the fundamental rights and freedoms contained in the European Convention on Human Rights (ECHR) enforceable in the UK.

2.2. Article 8 of the ECHR provides that individuals have the right to respect for private and family life and Article 6 of the ECHR provides that individuals have the right to a fair trial.

2.3. The use of covert surveillance techniques is considered to be an interference with this Article 8 right and therefore RIPA provides a framework to render lawful surveillance activities which might otherwise be in breach of the ECHR. It is also aimed at ensuring that evidence obtained against a person to be used in criminal proceedings if obtained in a fair manner.

2.4. RIPA regulates three surveillance techniques available to local authorities, namely:

2.4.1 Directed surveillance - covert surveillance which is carried out as part of a specific investigation and is likely to involve the obtaining of private information about the person under investigation;

2.4.2 Covert Human Intelligence Sources (CHIS) – use of a person who establishes and maintains a relationship with the person under investigation in order to obtain and disclose information; and

2.4.3 The acquisition and disclosure of communications data - obtaining information from communication service providers (e.g. the postal service, telephone

companies and internet companies) about the use made of a service (e.g. itemised billing, internet connections or records of registered post) and user information (e.g. subscriber names, addresses or other customer information).

2.5 RIPA provides that the above activities may be authorised but must be necessary and proportionate.

3. THE COUNCIL'S USE OF RIPA

3.1 The Council uses its powers under RIPA infrequently.

3.2 The Council did not authorise any surveillance activities under RIPA in 2013 .

4. ENVIRONMENTAL IMPLICATIONS

4.2 There are no environmental implications arising from this report.

5. CRIME AND DISORDER IMPLICATIONS

5.1 The Council's use of RIPA relates to the prevention and detection of crime and, in some cases, the prevention of disorder. It is essential the Council complies with RIPA if covert surveillance techniques are used in order to prevent legal challenge and ensure that evidence obtained is admissible in criminal proceedings. As stated above, the Council rarely uses its powers under RIPA.

6. CONCLUSION

6.1 RIPA provides the Council with a statutory framework to follow so that it may carry out various covert investigatory activities in a lawful manner.

6.2 The Council uses its powers under RIPA infrequently, but when use is made of such powers it is essential that this is done in accordance with the law and the Council's policies.

7. RECOMMENDATION

It is recommended that:-

7.1 Members note the use made by the Council of its powers under RIPA.

Further Information

Grainne O'Rourke
Head of Legal and Democratic Services
& RIPA Monitoring Officer
Telephone: 02380 285588
Email: grainne.orouke@nfdc.gov.uk

Background Papers

- Published documents

New Forest
DISTRICT COUNCIL

SURVEILLANCE POLICY

Human Rights Act 1998,

Regulation of Investigatory Powers Act 2000

& Protection of Freedoms Act 2012

THIS POLICY MUST BE READ IN CONJUNCTION WITH THE CURRENT HOME OFFICE CODES OF PRACTICE: "COVERT SURVEILLANCE AND PROPERTY INTERFERENCE" AND "COVERT HUMAN INTELLIGENCE SOURCES" AND THE OFFICE OF SURVEILLANCE COMMISSIONERS "PROCEDURES AND GUIDANCE" (DECEMBER 2011).

CONTENTS

1 BACKGROUND

1.1 When the Human Rights Act 1998 came into force in 2000 it made the fundamental rights and freedoms contained in the European Convention on Human Rights enforceable in UK Courts and Tribunals.

1.2 Article 8 of the Convention reads as follows: -

"Everyone has the right to respect for his private and family life his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of public safety, for the protection of order, health or morals, or for the rights and freedoms of others."

1.3 Investigating Officers of the Council may, from time to time, engage in activities which interfere with a person's right under Article 8 of the Convention to respect for their private and family life. Such interference is only permissible where it complies with the exceptions set out in Article 8.

1.4 The Regulation of Investigatory Powers Act 2000 ("RIPA") provides a statutory framework whereby certain surveillance activities can be authorised and conducted compatibly with Article 8 by public bodies.

1.5 Officers of New Forest District Council ("the Council") may seek authorisation under RIPA to engage in the following types of surveillance: -

- Directed surveillance
- Use of a Human Covert Intelligence Source

1.6 These surveillance techniques can **only** be authorised under RIPA where the use of the surveillance is necessary for the **prevention or detection of crime**, or (in some cases) for the **prevention of disorder**. From **1 November 2012**, it will **only** be possible to authorise directed surveillance under RIPA where the matter under investigation constitutes a **criminal offence** for which the courts could impose a maximum term of at least six months' imprisonment, **or** where the surveillance is in connection with the sale of alcohol or tobacco to children.

1.7 The Council can only authorise surveillance under RIPA in connection with the performance of the specific public functions which it carries out. It cannot use RIPA to authorise surveillance in connection with the ordinary functions (e.g., employment issues) which are carried out by all public authorities.

1.8 This Surveillance Policy explains what is involved in each of these two types of surveillance. The policy sets out the relevant responsibilities of the Council and its officers, and is designed to ensure that any such surveillance is conducted in a manner that will comply with the safeguards embodied in the Human Rights Act 1998 and RIPA.

1.9 All Investigating Officers and Authorising Officers should be familiar with RIPA, this Surveillance Policy, the Codes of Practice issued by the Home Office relating to the Use of Covert Human Intelligence Sources and Covert Surveillance and Property Interference, and the Procedures and Guidance issued by the Office of Surveillance Commissioners.

2 DEFINITIONS:

2.1 Confidential Information

This includes:

- Matters subject to legal privilege. Information relating to communications between a professional legal advisor and their client for the purposes of giving advice, in contemplation of legal proceedings or relating to legal proceedings.
- Confidential personal information: Information which relates to the physical or mental health, or spiritual counselling of a person (living or dead) who can be identified from it. For example, information about medical consultations/medical records.
- Confidential constituent information: Information relating to communications between a Member of Parliament and constituent in respect of constituency matters.
- Confidential journalistic information

2.2 Collateral Intrusion

Collateral Intrusion is the likely effect of the use of surveillance on the private and family life of persons who are not the intended subjects of the activity.

2.3 Surveillance

Surveillance includes

- monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.
- recording anything monitored, observed or listened to in the course of surveillance.
- surveillance by, or with, the assistance of a surveillance device.

Surveillance can be **overt** or **covert**.

2.4 Overt Surveillance

Overt surveillance is surveillance which is not secretive or hidden. It includes surveillance where the subject has been told it will happen.

2.5 Covert Surveillance

Covert surveillance is surveillance carried out in a manner calculated to ensure that subjects of it are unaware that it is or may be taking place.

2.6 Directed Surveillance

Directed surveillance is **covert** but **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 one 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

2.7 Intrusive surveillance

Intrusive Surveillance occurs when surveillance:

- is covert;
- relates to residential premises and/or private 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.

Intrusive surveillance cannot be carried out or approved by the Council.

2.8 The conduct and use of covert human intelligence sources (CHIS)

The conduct and use of covert human intelligence sources occurs when a person establishes or maintains a personal or other relationship with a person:

- For the covert purpose of using the relationship to obtain information or to provide access to any information to another person or
- To covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

A CHIS **does not** always need to be asked by the Council to exploit a relationship for a covert purpose for them to be classified as a CHIS.

3 DIRECTED SURVEILLANCE

3.1 This paragraph should be read in conjunction with the Home Office Code of Practice "Covert Surveillance and Property Interference" which can be found at http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-covert?view=Binary

3.2 Directed surveillance is surveillance which meets **all** of the following criteria:

i. It is covert, but not intrusive surveillance

Surveillance will be covert if it is carried out in a way calculated to ensure that the subject of the surveillance is unaware that it is taking place.

The Council **cannot** engage in intrusive surveillance.

ii. It is conducted for the purposes of a specific investigation or operation

iii. It is likely to result in the obtaining of private information about a person (whether or not specifically identified for the purposes of the investigation or operation)

"Private information" includes any information relating to a person's private or family life, including their relationships with others, their family, and professional or business relationships.

For more information about what constitutes "private information", see paragraph 5 below.

iv. It is conducted otherwise than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonable for an authorisation under RIPA to be sought.

For example, if an officer happens to spot an offence taking place, they may stop and take photographs as evidence of that offence, without requiring prior authorisation under RIPA.

3.3 Any officer intending to conduct directed surveillance must seek prior authorisation of that surveillance under RIPA (see paragraphs 7,8 & 9 below, regarding applications and authorisations).

3.4 At present, directed surveillance may be authorised under RIPA where it is necessary for the prevention or detection of crime, or for the prevention of disorder. From **1 November 2012**, it will **only** be possible to authorise directed surveillance under RIPA where the matter under investigation constitutes a **criminal offence** for which the courts could impose a maximum term of at least six months' imprisonment, **or** where the surveillance is in connection with the sale of alcohol or tobacco to children.

3.5 **Examples**

3.5.1 With effect from 1 November 2012, it will no longer be possible to authorise directed surveillance for the following offences:

- Dog fouling

- Littering
- Planning offences
- Noise abatement notices

As the courts **cannot** impose a maximum term of at least six months' imprisonment.

3.5.2 It will still be possible to authorise directed surveillance for the following offences:

- Fly tipping
- Benefit fraud
- Trading standards
- Financial offences
- Dangerous dogs
- Listed building offences

As the courts **can** impose a maximum term of at least six months' imprisonment.

4 CCTV

4.1 The Council operates a close circuit television system within certain towns in the New Forest District. Use of this system by the council or third parties such as the police for directed surveillance would require authorisation under RIPA.

4.2 Overt CCTV cameras which are permanently sited for the purposes of, for example, monitoring traffic flow or public safety will not generally require RIPA authorisation, since the public will be aware that such systems are in use. However, there may be occasions when the Council wishes to use such CCTV cameras for the purposes of a specific investigation or operation or to target a specific person. In such circumstances (unless as an immediate response to events) consideration must be given as to whether authorisation for directed surveillance is required.

4.3 For example, authorisation for directed covert surveillance is likely to be required if the Council wishes to make use of permanently sited overt CCTV cameras in circumstances where Officers have received reports of unlawful trading at a specific location, and wish to use those existing CCTV systems to keep watch for such activities.

4.4 If another agency – eg the Police – wishes to use the Council's CCTV cameras for one of their investigations, this must be agreed by the Head of Public Health and Community Safety, or by the Civil Contingencies and CCTV Manager. A copy of the other agency's RIPA authorisation form must be obtained and the details held with the Council's central register. In such circumstances, as long as there is a Police RIPA authorisation, there is no separate need for one of the Council's Authorised Officers to authorise the use of the cameras.

4.5 **Deployable CCTV**

The deployment of mobile surveillance cameras is likely to be directed surveillance in all cases and appropriate RIPA authorisation will be required. Additionally, applicants will be required to complete a "Mobile CCTV Deployment Form", in accordance with the Council's Deployable (Mobile) CCTV Camera Policy. This form should be submitted to the Council's CCTV Manager.

5 PRIVATE INFORMATION

5.1 The 2000 Act states that private information includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationships with others, including family and professional or business relationships. Private information may include personal data, such as names, telephone numbers and addresses.

5.2 Whilst a person may have a reduced expectation of privacy when in a public place, surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public. For example, two people holding a conversation on a public street or bus may have a reasonable expectation of privacy, even though they are in a public place.

5.3 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. For example, where an officer drives past a restaurant to take a photograph of the exterior, this is unlikely to require authorisation under RIPA, as the officer is not collecting private information. However, if the officer wishes to revisit the restaurant on a number of occasions to try to establish occupancy of the premises, this is likely to result in the obtaining of private information about the occupier, and authorisation for directed surveillance will usually be required.

6 CONDUCT AND USE OF COVERT HUMAN INTELLIGENCE SOURCES ("CHIS")

6.1 This paragraph should be read in conjunction with the Home Office Code of Practice "Covert Human Intelligence Sources" which can be found at http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-practice-human-intel?view=Binary

6.2 The conduct and use of covert human intelligence sources occurs when a person establishes or maintains a personal or other relationship with a person:

- For the covert purpose of using the relationship to obtain information or to provide access to any information to another person **or**
- To covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

A CHIS **does not** always need to be asked by the Council to exploit a relationship for a covert purpose for them to be classified as a CHIS (see paragraph 6.5 below).

6.3 The conduct or use of a CHIS may be authorised under RIPA where it is **necessary** for the **prevention or detection of crime**, or **for the prevention of disorder.**

6.4 A relationship is established or maintained for a covert purpose if it is conducted in a manner to ensure that one of the parties is unaware of its purpose. A relationship will only be used covertly and information will only be disclosed covertly if it is used or disclosed in a way which will ensure that one of the parties is unaware of the use or disclosure.

The use of such sources by the Council is essentially the manipulation of a relationship to gain information and can amount to the use of an informant. However, the Council is only likely to use a CHIS in very exceptional circumstances.

6.5 The CHIS will be the person who establishes or maintains the relationship as set out in paragraph 6.2 above.

- The provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the Council that is within their personal knowledge, without being induced, asked or tasked by the Council. Therefore, the public can continue to provide information as part of their normal civic duties, or to contact numbers set up by the Council to receive information.

- However, a member of the public providing information **may** be a CHIS if their information is obtained in the course of, or as a consequence of, the existence of a personal or other relationship and they covertly pass that information to the Council. For example, where a member of the public gives repeat information about a suspect and it becomes apparent that the member of the public may be obtaining that information in the course of a family or neighbourhood relationship, it should be considered by the Investigating Officer whether that person is in reality a CHIS.

- This is known as a "status drift". The Council accordingly needs to be alert to the fact that a public informant may in reality be a CHIS even if not tasked to obtain information covertly.

- Where such a "status drift" occurs, advice must be sought from Legal Services before any information received from this member of the public is relied on.

6.6 **Examples**

6.6.1 The following **will not** be a CHIS:

- A member of the public volunteers a piece of information to the Council regarding something he has witnessed in his neighbourhood. He will not be a CHIS as he is not passing on information as a result of a relationship which has been established or maintained for a covert purpose.
- A person complains about excessive noise coming from their neighbour's house and the Council ask them to keep a noise diary. They will not be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose.

6.6.2 The following **will** be a CHIS:

- Intelligence received by the Council suggests that a local public house will sell alcohol to minors if they are familiar with them. A person under the age of 18 is engaged and trained by the Council and deployed to attend the licensed premises on a number of occasions and then try and purchase alcohol. In this situation a relationship has been established and maintained for the covert purpose and therefore a CHIS authorisation will be required.
- Without being asked, a person provides regular information to the Council about their neighbours' working hours and income as they believe their neighbour is committing benefit fraud. The person regularly visits their neighbour and engages in conversations about their work for the purpose of obtaining this information and passing it to the Council.

6.7 If a CHIS is used, both the use of the CHIS and their conduct require prior authorisation.

- **Conduct** is 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** includes actions inducing, asking or assisting a person to act as a CHIS.

6.8 The Investigating Officer should apply for such authorisation as soon as the conduct or use of a CHIS is contemplated (see paragraphs 7,8 & 9 below, regarding authorisations and applications).

6.9 **Handling and Controlling the CHIS**

6.9.1 If an authorisation is provided the Investigating Officer must ensure that they are aware of the extent and limits of what the CHIS is allowed to do and make sure that the CHIS is advised of this.

6.9.2 The Investigating Officer will be responsible for the day to day handling of the CHIS (they will be the "handler"). This will involve dealing with the CHIS on behalf of the Council, directing the day to day activities of the CHIS, recording information supplied by the CHIS and monitoring the CHIS's security and welfare.

6.9.3 It will be good practice for the Investigating Officer to carry out a risk assessment on the use of the CHIS.

6.9.4 The safety and welfare of a CHIS both during the operation and after the authorisation has been cancelled should be taken into account by the investigating officer. Every application for authorisation should therefore include a detailed risk assessment of the risk to the CHIS and the likely consequences should the role of the CHIS become known.

6.9.5 The Authorising Officer will be responsible for the management and supervision of the "handler" and the general oversight of the use of the CHIS.

6.9.6 A record must also be made of the use made of the CHIS (see paragraph 16 below for the information which must be held in the Central Log).

6.10 **Records**

Records of relevant documentation relating to every CHIS should be kept for a period of at least three years in accordance with paragraph 16 of this Policy.

6.11 **Special considerations**

6.11.1 Special care should be taken where the use of CHIS may involve confidential information (see paragraphs 2.1 & 10).

6.11.2 Special safeguards should be put in place where the CHIS is under the age of 18. A child under the age of 16 may not be authorised to give information against his parents. The Regulation of Investigatory Powers (Juveniles) Order 2000 contains the special provisions which should be followed where the CHIS is a minor. In such cases the only Authorising Officer is the Chief Executive (or in his absence a Director).

6.11.3 Special safeguards should also be used where the CHIS is a vulnerable individual. A vulnerable individual is defined by the Code of Practice as "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." The use of a vulnerable individual is only permitted in exceptional circumstances. In such cases the only Authorising Officer is the Chief Executive (or in his absence a Director).

7 AUTHORISATIONS, RENEWALS, REVIEWS AND CANCELLATIONS

7.1 Prior authorisation is required for the use of directed surveillance or the conduct or use of a CHIS.

7.2 Procedure for Authorisations

7.2.1 Each officer who undertakes investigations on behalf of the Council must seek authorisation in **writing** for any directed surveillance or the conduct and use of a CHIS.

7.2.2 A full list of Authorising Officers, along with their functions, is shown at **Appendix 1.** Authorising Officers **must not** delegate their powers under RIPA.

7.2.3 A checklist for the respective duties of the Investigating Officer and the Authorising Officer is set out in **Appendix 2.** Further detail is provided on some of these duties in this Policy.

7.2.4 All applications for authorisations should be made on the applicable standard form (See paragraph 8).

7.2.5 The Authorising Officer must describe explicitly in the authorisation what is being authorised. This should be in the Authorising Officer's own words rather than merely by reference to the terms of the application.

7.2.6 The Authorising Officer may add a proposed activity to the application if it is deemed necessary, and the Authorising Officer may authorise only some of what is being requested by the Investigating Officer. Where only part of the application is being authorised, the Authorising Officer should state the reason for this decision.

7.2.7 Authorising Officers should not normally be responsible for authorising operations in which they are directly involved as the Authorising Officer should be independent of the investigations. Where this is unavoidable this must be highlighted on the authorisation.

7.2.8 Every authorisation must state the rank of the person providing it.

7.3 Authorisations Requiring Judicial Approval

7.3.1 With effect from **1 November 2012**, where an authorisation has been granted for directed surveillance or the conduct or use of a CHIS that authorisation shall not have effect until it has been **approved** by a justice of the peace at the local Magistrates Court. **No directed surveillance or the use of a CHIS can take place until this approval has been obtained.**

7.3.2 Legal Services should be instructed to prepare the application to the justice of the peace.

7.4 Urgent Cases

7.4.1 Where a case is urgent, different rules apply. However, a case will only be urgent if the time that would elapse before the authorisation could be made in the normal way would be likely to endanger life or jeopardise the operation or investigation.

7.4.2 In urgent cases authorisation may be granted or renewed orally.

7.4.3 Oral authorisation must be recorded in writing by the Investigating Officer as soon as possible after the authorisation is provided.

7.4.4 However, from **1 November 2012** it will not be possible to use the urgent, oral authorisation route, as Judicial Approval will be required before such authorisations can take effect. (see paragraph 7.3)

7.5 Duration

7.5.1 The time limit for a standard **written** authorisation for directed surveillance is 3 months from the day of the authorisation.

7.5.2 The time limit for a standard **written** authorisation for a CHIS is 12 months from the day of the authorisation.

7.5.3 The time limit for an **urgent oral** authorisation or renewal is 72 hours after it is issued.

7.5.4 It should be noted that even if an authorisation is only required for a limited time, it must still be for the statutory periods outlined above. However, the authorisation can be reviewed and/or cancelled if it is no longer necessary and proportionate.

7.5.5 No further operations can be carried out after the expiry of the relevant authorisation unless it has been renewed.

7.5.6 It will be the responsibility of the Investigating Officer to ensure that direct surveillance or the conduct or use a CHIS is only undertaken under an appropriate and valid authorisation. It will be the Investigating Officer's responsibility to diarise when the authorisation expires.

7.6 Reviews

7.6.1 The Authorising Officer will be responsible for reviewing each authorisation at regular intervals. The Authorising Officer shall determine how often a review should take place at the outset and each review should be conducted by the predetermined date. As a guide, reviews should take place on a monthly basis. However, the Authorising Officer may determine that they should take more or less frequently (if so, the reasons should be recorded).

7.6.2 Reviews should take place as often as necessary and practicable and this will need to be determined on a case by case basis. More frequent reviews should take place where surveillance results in collateral intrusion or access to confidential information. (see paragraphs 2.1, 2.2 & 10).

7.6.3 Reviews should also be held in response to changing circumstances and must take into account any subsequent action by the Council arising from the produce of the surveillance, which may be in the form of the issue of notices, orders, or determinations by the Council, or the bringing of criminal or civil proceedings, or any other action.

7.6.4 It will be the responsibility of the Authorising Officer to diarise when reviews should be held.

7.6.5 All reviews should be recorded on the correct form (See paragraph 8).

7.7 Renewal

7.7.1 An authorisation may be renewed **before** it ceases to have effect if an Authorising Officer considers it necessary for the authorisation to continue. The renewal takes effect at the time at which the authorisation would have ceased to have effect. If necessary a renewal can be made more than once.

7.7.2 Before a renewal of an authorisation for the conduct or use of a CHIS the Authorising Officer must be satisfied that a review has taken place of:

- the use made of the source in the period since the grant or, as the case may be, latest renewal of the authorisation; and
- the tasks given to the source during that period and the information obtained from the conduct or the use of the source.

7.7.3 With effect from **1 November 2012**, where renewal of an authorisation has been granted for directed surveillance or a CHIS that renewal shall not have effect until it has been **approved** by a justice of the peace at the local Magistrates Court.

7.7.4 Where the renewal relates to the conduct or use of a CHIS the Justice of the Peace will need to be satisfied that a review has taken place of the matters listed in paragraph 7.7.2.

7.7.5 All renewals must be made on the correct form. (See paragraph 8)

7.8 Cancellations

7.8.1 All authorisations must be cancelled **as soon as** they are no longer required.

7.8.2 Even if an authorisation has expired it will not lapse and should be formally cancelled.

7.8.3 The Authorising Officer who granted or last renewed the authorisation must cancel the authorisation if the grounds for granting the authorisation no longer apply e.g. the aims have been met; risks have changed and authorisation is no longer appropriate.

7.8.4 If the Authorising Officer is not available, this duty will fall one of the other Authorising Officers.

7.8.5 Authorisations may be cancelled orally and when and by whom this was done must be included on the cancellation form. However, best practice will be for the authorisation to be cancelled in writing.

7.8.6 When cancelling an authorisation, the Authorising Officer should (where applicable):

- Record the date and times (if at all) that surveillance took place, and that the order to cease the activity was made.
- Record reason for the cancellation.
- Ensure that surveillance equipment has been removed and returned.
- Provide directions for the management of the material obtained as a result of the investigation.
- Ensure that the detail of persons subjected to surveillance since the last review or renewal is properly recorded.
- Record the value of the surveillance and interference (i.e. whether the objectives as set out in the authorisation were met.)

7.8.7 The Authorising Officer should also advise those involved in the surveillance or the CHIS to stop their actions.

7.8.8 All cancellations must be completed on the correct form (See paragraph 8).

8 APPLICATION FORMS

8.1 The standard forms issued by the Office of Surveillance Commissioners can be found at www.homeoffice.gov.uk. The person completing the form is responsible for ensuring that the form used is the most up-to-date version issued by the Home Office.

8.2 The forms for applications, renewals, reviews and cancellations should be completed in as much detail as possible.

8.3 For guidance on what should be included in the application for authorisation the Investigating Officer should refer to paragraph 5.8 of the 2010 Covert Surveillance and Property Interference Revised Code of Practice (for direct surveillance) or paragraph 5.10 in the 2010 Authorisation Procedures for Covert Human Intelligence Sources Code of Practice (for CHIS).

8.4 Each investigation or operation should be given a unique reference number ("URN") on the application form by the Monitoring Officer. Any reviews, renewals or cancellation forms should be identified by the same URN.

8.5 The URN should be obtained from the Monitoring Officer (see paragraph 17).

8.6 Any application (or other) form which is not completed in full will be rejected by the Authorising Officer.

8.7 The role of the Investigating Officer is to present the facts and evidence to the Authorising Officer. They must also set out in detail why they consider the directed surveillance/use of a CHIS to be **necessary** and **proportionate** (see paragraph 9). The application should include consideration of any potential collateral intrusion (See paragraph 2.2) and measures taken to limit this. The application must state whether the Investigating Officer expects the investigation to result in the obtaining of confidential information (see paragraphs 2.1 &10).

8.8 Having reviewed the application, the Authorising Officer must decide whether they consider the activities applied for are **necessary** and **proportionate** (see paragraph 9). If so, they should decide whether to authorise some or all of the activities applied for. If they decide to authorise the application, they must record in detail the reasons that they have reached this decision, including the reasons that they have concluded the activities are necessary and proportionate.

9 THE NECESSITY AND PROPORTIONALITY TEST

9.1 No directed surveillance or use of a CHIS can be authorised under RIPA unless it can be demonstrated that it is necessary and proportionate.

9.2 The Authorising Officer must be satisfied that the proposed surveillance is **necessary and proportionate**.

9.3 Necessary

9.3.1 The use of the directed surveillance or conduct and use of a CHIS must be **necessary** for the **purpose of preventing or detecting crime** or **of preventing disorder.**

9.3.2 In order for the Authorising Officer to be satisfied that the surveillance is necessary, the Investigating Officer must clearly identify in the application the conduct that it is aimed to prevent or detect, and an explanation of why covert techniques are required.

9.4 **Proportionate**

9.4.1 The intrusion into the private and family life of the subject of the operation must be **balanced** against what the activity seeks to achieve. The intrusion must not be excessive or arbitrary.

9.4.2 The authorisation should therefore demonstrate how the Authorising Officer reached the conclusion that the act is proportionate

9.4.3 The activities will not be proportionate if the activities are excessive in the circumstances of the case or if the information could be obtained by a less intrusive means.

9.4.4 The following elements of proportionality must be considered by the Authorising Officer and should be addressed in the authorisation:

- 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.

9.4.5 When authorising a CHIS, the Authorising Officer must also:

- be satisfied that the conduct and/or use of the CHIS is proportionate to the objective sought to be achieved;
- be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS. These arrangements must address health and safety issues by the carrying out of a formal and recorded risk assessment;
- consider the likely degree of intrusion for all those potentially affected;
- consider any adverse impact on community confidence that may result from the use or conduct of the CHIS or the information obtained; and
- ensure that records contain the required particulars of the CHIS and that these are not available except on a 'need to know' basis.

9.4.6 **Risk of Collateral Intrusion**

The Authorising Officer should consider the likely effect of the use of the direct surveillance or the conduct and use of a CHIS on the private and family life of persons who are not the intended subjects of the activity. The Authorising Officer must consider the risk of collateral intrusion and have a plan for managing any such risk.

If the impact on other persons cannot be avoided altogether, then any collateral intrusion must be proportionate.

The person carrying out the surveillance must inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals not covered by the authorisation. The Authorising Officer must then consider whether the authorisation ought to continue or whether a new authorisation is required.

10 CONFIDENTIAL MATERIAL

10.1 Particular care should be taken where the subject of the investigation or operation might reasonably expect a high degree of privacy, for example in their home, and where it is envisaged that the investigation may cause the Council to come into possession of Confidential Information (see definition at paragraph 2.1). In these cases, the surveillance can only be authorised by the Chief Executive (or in his absence a Director). Applications which are calculated to obtain confidential information will only be authorised in very exceptional and compelling circumstances.

10.2 Where an Investigating Officer comes into possession of confidential material during the course of an investigation, s/he should seek legal advice from a member of the Council's Legal Services Section before taking any action in connection with that material.

10.3 Where it is envisaged that surveillance may cause the Council to come into possession of material which is subject to legal privilege, the Investigating Officer must seek legal advice from a member of the Council's Legal Services Section before the application for authorisation is made.

11 ACTIVITIES BY OTHER PUBLIC AUTHORITIES

The Investigating Officer must make enquiries of other public authorities whether they are carrying out similar activities, if he considers that there is such a possibility, in order to ensure that there is no conflict between the activities of the Council and those other public authorities.

12 JOINT INVESTIGATIONS

12.1 From time to time, Council officers may carry out investigations with officers from another public authority, for example:

- The police;
- The Department of Work and Pensions;
- The Environment Agency;
- The Food Standards Agency; or
- The Health and Safety Executive

12.2 Where one authority is acting on behalf of another, the tasking authority should normally obtain the RIPA authorisation. If an authorisation has been obtained by another agency, who wish the Council to carry out surveillance in accordance with that authorisation, an Authorising Officer must view that authorisation to ensure that Council officers, and the activities which they are being asked to carry out, are covered by that authorisation.

13 DATA PROTECTION

Private information collected as a result of surveillance may include personal data. It is the responsibility of the Authorising Officer to ensure that personal data is processed (including handling, dissemination, storage, retention and destruction) in accordance with the Data Protection Act 1998 and the Council's Data Protection Policy.

14 DESTRUCTION OF WHOLLY UNRELATED MATERIAL

14.1 Surveillance may result in officers obtaining the following categories of material:

i. material which is wholly unrelated to the investigation (for example, information about persons who are not the subject of the surveillance, and have no relevant involvement with the subject of the surveillance);

ii. material regarding the subject(s) of the surveillance, which is unlikely to be used in connection with the investigation or any subsequent proceedings;

iii. material which is relevant to the investigation, and may be used in connection with subsequent proceedings

14.2 Material which is **wholly unrelated** to the investigation (category **i.** above) should be destroyed promptly and securely. As the material will have been collected in connection with the investigation of a criminal offence, advice should be sought from the Council's Legal Services section prior to the destruction of evidence.

14.3 All other material should be retained until the investigation is concluded and a decision is taken regarding what action, if any, will be taken in connection with the investigation. At that stage, the Authorising Officer will determine which materials are to be retained, and for how long.

14.4 Where criminal proceedings are contemplated, all material (save for wholly unrelated material) is potentially relevant. It must therefore be retained and will be discloseable in those proceedings.

15 TRAINING

15.1 Each officer of the Council with responsibilities for the conduct of an investigation, operation or authorisation under RIPA, will undertake annual training to ensure that any such investigations, operations and authorisations undertaken are conducted according to the statutory requirements and the Codes of Practice.

15.2 Each officer who undertakes training in connection with their responsibilities under RIPA must keep a personal training record, and must send a copy of this training record annually to the Monitoring Officer.

16 RECORDS OF AUTHORISATIONS

16.1 A centrally retrievable record of all authorisations will be held by the Monitoring Officer. This will contain the following information:

- the URN
- the dates that the authorisation was granted, reviewed, renewed or cancelled and, with effect from 1 November 2012, the date of the Magistrates Approval.
- whether the authorisation was urgent.
- the name and rank of the Authorising Officer for the initial authorisation and any renews or cancellations.
- whether the Authorising Officer is involved in the investigation.
- the file reference for the investigation.
- whether the authorisation was likely to result in the obtaining of confidential material.

16.2 This centrally retrievable record will be stored in a manner which is confidential and secure and retained for a period of at least **three years** from the date of cancellation of the authorisation.

16.3 In addition, the Monitoring Officer will keep the following documents, where applicable, for a period of at least **three years** from the date of cancellation of the authorisation:

- The application, authorisation, reviews, renewals, cancellations and, with effect from **1 November 2012**, the approval from the Magistrates Court.
- The frequency of the reviews prescribed by the authorising officer.
- The date and time when any instruction to cease directed surveillance or use of a CHIS was given.
- The date and time when any other instruction was given by an authorising officer.

16.4 In relation to the use of a CHIS the Monitoring Officer will also maintain the following documents:

- Any risk assessment in relation to the CHIS.
- The circumstances in which tasks were given to the CHIS.
- The value of the CHIS to the Council.

16.5 Investigating Officers and Authorising Officers may keep copies of relevant documentation but any such copies should be stored in a manner which is confidential and secure.

17 MONITORING

17.1 The Head of Legal and Democratic Services will have responsibility for overseeing the authorising process to ensure good quality control of RIPA and will be referred to as the Monitoring Officer for the purposes of this Policy (see **Appendix 3**).

17.2 The Monitoring Officer will be responsible, along with the Senior Responsible Officer, for ensuring corporate awareness of RIPA.

17.3 The Monitoring Officer will be responsible for issuing each application with a URN.

17.4 All completed RIPA forms; applications (whether granted or refused), authorisations, reviews, renewals and cancellations and, with effect from **1 November 2012**, approvals from the Magistrates' Court should be forwarded to the Monitoring Officer within **five working days** of the relevant decision. The Monitoring Officer will hold these documents securely.

17.5 The Monitoring Officer will also be responsible for the day to day management of the authorising process and any initial queries from Investigating Officers or Authorising Officers should be addressed to the Legal Services Section.

18 SENIOR RESPONSIBLE OFFICER

18.1 The Senior Responsible Officer will be the Chief Executive (see **Appendix 3**).

18.2 The Senor Responsible Officer will be responsible for the following:

- The integrity of the process in place within the Council for the management of CHIS and Directed Surveillance.
- Compliance with RIPA and with the Codes of Practice.
- Ensuring all Authorising Officers are of an appropriate standard.
- Oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors.
- Engagement with the Office of Surveillance Commissioners (OSC) inspectors when they conduct their inspections, where applicable.
- Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.

19 POLICY AND IMPLEMENTATION

19.1 The Policy is operational from 9 October 2012 and replaces any previous policies and procedures relating to surveillance.

19.2 **The Monitoring Officer will report annually to** the Audit Committee regarding the use made by the Council of its powers under RIPA.

19.3 The Audit Committee will review the Council's Surveillance Policy annually.

20 APPENDICES

Appendix 1 – Functions that may be undertaken by Authorising Officers

Appendix 2 - Application and Authorisation Checklist

Appendix 3 – Monitoring and Senior Responsible Officers

APPENDIX 1

FUNCTIONS THAT MAY BE UNDERTAKEN BY AUTHORISING OFFICERS:

1. Authorise an **application** for authority to carry out directed surveillance or for the conduct or the use of a CHIS.

2. **Review** an authorisation to carry out directed surveillance or the conduct or use of a CHIS on or before the specified date.

3. Authorise **renewal** of an application for authority to carry out directed surveillance or for the conduct or use of a CHIS.

4. Authorise **cancellation** of an application for authority to carry out directed surveillance or for the conduct or use of a CHIS.

5. Authorise **destruction** of wholly unrelated material arising from surveillance or from the conduct or use of a CHIS, with advice from the Legal Services Section where appropriate.

6. **Monitor** the produce of the surveillance or from the conduct or use of a CHIS.

7. Authorise an application where the likely consequence of directed surveillance or conduct or use of a CHIS would be intrusion on another person other than the target **(collateral Intrusion).**

8. Authorise an application where the likely consequence of the directed surveillance or conduct or use of a CHIS would result in Council obtaining **confidential material.**

9. Authorise the use of a CHIS who is a minor.

10. Authorise the use of a CHIS who is a vulnerable person.

RANK/TITLE	AUTHORISED FUNCTIONS
Chief Executive	1-10
Executive Director	1-7 (8,9,10 in Chief Executive's absence)
Head of Service (Environment Services)	1-7
Head of Service (Housing)	1-7
Head of Service (Public Health and Community Safety)	1-7
Head of Service (Planning and Transportation)	1-7

APPENDIX 2

APPLICATION AND AUTHORISATION CHECKLIST

Investigating Officer must:

Read the Surveillance Policy document and be aware of any other relevant guidance.	
Determine that directed surveillance and/or a CHIS is required.	
For directed surveillance , assess whether the authorisation will be in accordance with Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 and be able to demonstrate that the suspected offence is subject to a custodial sentence of 6 months or more or that the surveillance is in connection with the sale of alcohol or tobacco to children (see paragraph 3.4 of this Policy).	
Assess whether authorisation is necessary under RIPA and whether the surveillance could be done overtly.	
Consider whether surveillance will be proportionate.	
Consider all less intrusive options which may be available and practicable **and use that option first.**	
If authorisation is **necessary and proportionate**, request a URN from the Monitoring Officer, prepare and submit an application to carry out directed surveillance or conduct or use of a CHIS to an Authorising Officer.	
REVIEW REGULARLY and submit to Authorising Officer on date set.	
If operation is no longer necessary or proportionate, complete **cancellation form** and submit to Authorising Officer.	

Authorising Officer must:

Consider in detail whether all options have been duly considered, including taking into account the Surveillance Policy document and any other relevant guidance.	

For directed surveillance, confirm that the offence is subject to a custodial sentence of 6 months or more or the surveillance is in connection with the sale of alcohol or tobacco to children (see paragraph 3.4 of this Policy).	
Consider whether surveillance can be considered to be in accordance with the law and is **necessary and proportionate** to the offence being investigated.	
Authorise **only** if an overt or less intrusive option is not practicable.	
Ensure the relevant judicial authority has made an order approving the grant of the authorisation.	
If surveillance is necessary and proportionate: • Review authorisation • Set review timetable (at least monthly)	
Cancel authorisation when it is no longer necessary or proportionate.	

ESSENTIAL:

- Officers must use the correct RIPA forms (which can be found on the Home Office website www.homeoffice.gov.uk).
- A URN must be obtained from the Monitoring Officer before submitting an application for authorisation.
- Once authorised, approval must be obtained from a Magistrates Court before any surveillance commences.
- All RIPA application forms (whether authorised or rejected) must be sent to the RIPA Monitoring Officer **within 5 working days**. This must include reviews, renewals and cancellations
- If in any doubt, seek advice from the Monitoring Officer or the Senior Responsible Officer **before** any directed surveillance and/or CHIS is authorised, renewed, cancelled, or rejected.

APPENDIX 3

MONITORING AND SENIOR RESPONSIBLE OFFICERS

Name	Job Title	RIPA Role
Grainne O'Rourke	Head of Legal and Democratic Services	Monitoring Officer
Dave Yates	Chief Executive	Senior Responsible Officer

New Forest
DISTRICT COUNCIL

POLICY FOR THE ACQUISITION OF COMMUNICATIONS DATA

Human Rights Act 1998,

Regulation of Investigatory Powers Act 2000

& Protection of Freedoms Act 2012

THIS POLICY MUST BE READ IN CONJUNCTION WITH THE CURRENT HOME OFFICE CODE OF PRACTICE: "ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA".

CONTENTS Page

1 BACKGROUND

1.1 When the Human Rights Act 1998 came into force in 2000 it made the fundamental rights and freedoms contained in the European Convention on Human Rights enforceable in UK Courts and Tribunals.

1.2 Article 8 of the Convention reads as follows: -

"Everyone has the right to respect for his private and family life his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of public safety, for the protection of order, health or morals, or for the rights and freedoms of others."

1.3 Investigating Officers of the Council may, from time to time, engage in activities which interfere with a person's right under Article 8 of the Convention to respect for their private and family life. Such interference is only permissible where it complies with the exceptions set out in Article 8.

1.4 The Regulation of Investigatory Powers Act 2000 ("RIPA") provides a statutory framework whereby certain investigations can be carried out in a lawful, regulated and proportionate manner so that an individual's Article 8 rights are not infringed.

1.5 This Policy is concerned with the provision in RIPA enabling certain communications data to be acquired by public authorities in a manner which is compatible with Article 8. This Policy sets out the relevant responsibilities of the Council and its officers, and is designed to ensure that any acquisition of communications data is conducted in a manner that will comply with the safeguards embodied in the Human Rights Act 1998 and RIPA. (The Council has a separate Surveillance Policy which deals with Directed Surveillance and Covert Human Intelligence Sources).

1.6 The acquisition of communications data can **only** be authorised by the Council under RIPA where the use of the surveillance is necessary for the **prevention or detection of crime** or for the **prevention of disorder**.

1.7 All officers who apply for communications data to be obtained or disclosed should be familiar with RIPA, this Policy, and the Home Office Code of Practice "The Acquisition and Disclosure of Communications Data" which can be found at http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-acquisition?view=Binary.

1.8 Acquiring communications data without authorisation or outside the scope of an authorisation will mean that the "protective umbrella" of RIPA is unavailable, and could expose the Council to the risk of legal action. It may also result in disciplinary action being taken against the officer/officers involved.

2 NATIONAL ANTI-FRAUD NETWORK

2.1 The Council currently uses the National Anti-Fraud Network ("NAFN") to deal with all applications for the acquisition of communications data. The application process, and NAFN's role in this process, is detailed below under "Applications and Authorisations".

2.2 NAFN provides a service whereby all applications are checked by an accredited individual (a "Single Point of Contact" or "SPoC") to ensure compliance with RIPA. NAFN has direct access to the databases of a number of Communications Service Providers ("CSPs"). This means that if an authorisation is granted to allow a person to engage in conduct required to obtain communications data (see paragraph 4.1.1 below), and NAFN has access to the database of the relevant CSP, the NAFN SPoC will be able to obtain that data directly.

2.3 In order to access the NAFN secure website to make an application for communications data, an Applicant will require a username, password and PIN.

2.4 Should a manager consider that it is necessary for a Council employee to use the NAFN secure website to make applications for communications data, this must be authorised in writing by the employee's Head of Service. Where the Head of Service has provided their authorisation, the manager should notify NAFN of the details of the employeewho requires log in details for the system.

3 WHAT TYPES OF DATA CAN BE ACQUIRED?

3.1 "Communications data" is generated, held or obtained by CSPs and may relate to use of the following services:-

3.1.1 Postal service

3.1.2 Email

3.1.3 Landline telephone

3.1.4 Mobile telephone

3.1.5 Internet

3.2 Local authorities may **NOT** acquire any information about the content of communications (eg, what was said, or what data was passed on), or the location of a mobile device used to make a call.

3.3 Local authorities may acquire communications data of the following types: -

3.3.1 **'Service information'**. This is information about the services provided to an individual. It will include information about:

a) the use made by any person of any postal service or communications service;

b) the use made by any person of any part of a telecommunications system, in connection with the provision to or use of any telecommunications service.

Service information might include, for example, information regarding itemised billing, use of call diversions/forwarding, itemised records of connections to internet services, information about selection of preferential numbers or discount calls, records of registered post and parcel consignment.

3.3.2 **'User information'**. This is information about the person who uses a service. It will include any information held by the provider of a postal or telecommunications service, regarding the persons to whom they provide the service.

This might include, for example, subscriber details, including names, addresses and other customer information.

3.4 The above examples are not exhaustive lists of the communications data which may be acquired. If officers are in any doubt about the types of data which they may be able to acquire, or the ways in which this might be acquired, they should seek advice from a SPoC (see paragraph 5.3 below).

3.5 Applicants and Designated Persons (see paragraph 5.4 below) should bear in mind that it may be appropriate to obtain subscriber information (ie, to check that the person who subscribes to a service is a person relating to their investigation) before they can determine whether it is necessary and proportionate to go on to acquire service information, such as itemised billing.

4 AUTHORISATIONS AND NOTICES

4.1 Communications data can be acquired in two ways: by Authorisation or by Notice:

4.1.1 An Authorisation enables the authorised person (generally the SPoC) to engage in conduct required to obtain the communications data;

4.1.2 A Notice requires a CSP to disclose the data in their possession, or to obtain and disclose the data.

4.2 The SPoC will be able to advise which of these methods will be most appropriate in relation to a particular investigation. In the majority of cases, the Council will use an Authorisation, authorising the SPoC to obtain the data required from the relevant CSP.

5 DIFFERENT ROLES

5.1 There are four key roles relevant to the acquisition of communications data:

- Applicant
- Single Point of Contact (SPoC)

- Designated Person
- Senior Responsible Officer

5.2 **Applicant**

The Applicant will generally be the investigating officer, who will complete the application form, setting out the necessity and proportionality of acquiring the communications data.

5.3 **Single point of contact**

A SPoC must have formal accreditation, and is trained to facilitate the lawful acquisition of communications data and effective cooperation between a public authority and CSPs. In this way, the SPoC provides a "guardian and gatekeeper" function. The SPoC provides objective judgement and advice to both the Applicant and Designated Person.

The Council does not have an internal Single Point of Contact (SPoC), but uses the SPoCs at NAFN, who hold the necessary accreditation.

5.4 **Designated Person**

The Designated Person is the person within the Council who reviews the application and authorises the grant of an Authorisation, or the giving of a Notice, where they consider the acquisition to be necessary and proportionate.

Designated Persons should not be involved in authorising Authorisations or Notices in relation to investigations in which they are directly involved. Where this is unavoidable, their involvement, and the reasons for which they have acted as the Designated Person in the particular case, must be set out in their recorded considerations.

The Council's Designated Persons are currently the Head of Public Health and Community Safety, the Chief Executive and Executive Directors.

5.5 **Senior Responsible Officer**

The Senior Responsible Officer is responsible for: -

5.5.1 Ensuring the integrity of the processes in place within the authority to acquire communications data;

5.5.2 Ensuring compliance with RIPA and with the Code of Practice;

5.5.3 Oversight of the reporting of errors to the Interception of Communications Commissioner's Office (IOCCO), the identification of the reasons for the errors, and the implementation of processes to minimise repetition of errors;

5.5.4 Engagement with IOCCO inspectors, and oversight of the implementation of any post-inspection plans.

The Council's Senior Responsible Officer is currently the Chief Executive.

6 NECESSITY AND PROPORTIONALITY

The obtaining or disclosure of communications data (by Authorisation or Notice) should only be authorised if the Designated Person is satisfied that:

6.1 The action is **NECESSARY** for the prevention or detection of crime or the prevention of disorder;

6.2 The action is **PROPORTIONATE.** It should: -

6.2.1 be no more than is required in the circumstances;

6.2.2 impair as little as possible on the rights and freedoms of the individual concerned and of innocent third parties;

6.2.3 be carefully designed to meet the objectives in question;

6.2.4 not be arbitrary, unfair or based on irrational considerations.

7 APPLICATIONS AND AUTHORISATIONS

7.1 APPLICATION FORM

7.1.1 The Applicant must complete the NAFN application form, which is a standard form approved by the Home Office. As the Council uses the NAFN application process, the Applicant will access the application form by logging onto the NAFN website using their username, password and PIN.

7.1.2 The Applicant should have reference to the Home Office document: "Acquisition and Disclosure of Communications Data; Guidance for the Layout of a Chapter II Application Form and Guidance for Applicants and Designated Persons Considering Necessity and Proportionality".

7.1.3 The application form must include the following information: -

i) name, rank and position of the Applicant;

ii) a unique reference number (which will be generated automatically by the NAFN website);

iii) the operation name, if applicable;

iv) specify that the communications data is required in connection with the purpose of **preventing or detecting crime or disorder**;

v) describe the communications data required, specifying the time periods for which the data is sought, including (where relevant) any historic or future dates. Any time period specified should be the shortest period in which the objective for which the data is sought can be achieved;

vi) explain why the acquisition of the communications data is **necessary** and **proportionate** (see paragraph 6 above);

vii) consider and, where appropriate, describe any collateral intrusion (ie, explain the extent to which the privacy of an individual not under investigation may be infringed, and why that infringement is justified in the circumstances);

viii) identify and explain the timescale within which the data is required.

7.2 SPoC REVIEW

7.2.1 Once the Applicant has completed the application form, this must be submitted electronically to the SPoC, who will check that the application is compliant with RIPA, that the acquisition intended is practical and lawful, and that the tests of proportionality and necessity have been properly considered and detailed.

7.2.2 If the SPoC considers that there are any problems with the application, or that further information is required, he will provide advice to the Applicant about the application. This may include, for example, advice about whether it is lawful, possible, or practical to obtain communications data of the nature sought by the applicant, and whether the tests of necessity and proportionality have been properly applied and explained. Where appropriate, the Applicant can make amendments to the application, and can re-submit the application to the SPoC.

7.2.3 Once the SPoC is satisfied with the application, he will complete the relevant sections of the application form, identifying the data to be acquired, and how it may be acquired. The SPoC will then notify the Designated Persons at the Council by email that there is an application pending which requires review.

7.3 AUTHORISATION BY DESIGNATED PERSON

7.3.1 The Designated Person must review the application in detail, before deciding whether to: -

a) authorise the application;

b) reject the application;

c) request further information.

7.3.2 Before deciding whether to authorise an application, the Designated Person should have reference to the Home Office document: "Acquisition and Disclosure of Communications Data; Guidance for the Layout of a Chapter II Application Form and Guidance for Applicants and Designated Persons Considering Necessity and Proportionality".

7.3.3 The Designated Person should consider the proportionality and necessity of the Authorisation/Notice applied for (see paragraph 6 above), and the potential for collateral intrusion. The Designated Person should not simply "rubber stamp" the application. Their reasons for authorising/declining the application should be clear and detailed, and demonstrate that they have considered the substantive merits of the application. If the Designated Person

requires further information in order to decide whether to approve an application, they should notify the SPoC that more information is required.

7.3.4 The standard form requires the Designated Person to tick a box to confirm whether they are authorising a person to engage in conduct to acquire communications data, or whether they are authorising a Notice to be served on a CSP, requiring them to obtain/disclose data. The Notice or Authorisation documents themselves will be completed by the SPoC.

7.3.5 The authorised or rejected Application is then submitted back to the SPOC via the NAFN secure website.

8 JUDICIAL APPROVAL

8.1 From 1 November 2012 a person may not engage in the conduct authorised, or serve a Notice on a CSP requiring them to provide communications data, unless and until the Authorisation/Notice has been approved by a Justice of the Peace.

8.2 Before approving an Authorisation or Notice, a Justice of the Peace must be satisfied that: -

At the time of granting the Authorisation, or giving the Notice: -

i) There were reasonable grounds for believing that the Authorisation/Notice was necessary and proportionate;

ii) The person who granted the Authorisation/Notice was an appropriate Designated Person; and

iii) At the time when the Justice of the Peace is considering the matter, there remain reasonable grounds for believing that the Authorisation/Notice is necessary and proportionate.

8.3 The procedure for obtaining judicial approval is as follows: -

i) After the Designated Person has completed the authorisation on the NAFN secure website, NAFN will send an application pack to the Applicant;

ii) The application pack should be forwarded to the Head of Legal and Democratic Services;

iii) A member of the Legal Services section will prepare the Magistrates' Court application, and will represent the Council at the Magistrates' Court hearing. The Applicant may be asked to prepare a witness statement and may be required to attend the hearing;

iv) If the Authorisation/Notice is approved, Legal Services will pass the approval to the Applicant. The Applicant will then liaise with the SPoC who will obtain the communications data from the CSP.

v) If the Authorisation/Notice is not approved, or is quashed by a Justice of the Peace, Legal Services will inform the Applicant. The Applicant must

inform the SPOC and Designated Person that the Authorisation/Notice was not approved, or was quashed.

8.4 **No action may be taken under the Authorisation or Notice unless and until it has been approved by a Justice of the Peace.**

9 DATA PROTECTION AND HANDLING THE DATA ACQUIRED

9.1 When the communications data has been acquired, it will be made available to the Applicant on the NAFN secure website.

9.2 Information collected through acquisition of communications data may include personal data. It is the responsibility of the Applicant to ensure that personal data is processed (including handling, dissemination, storage, retention and destruction) in accordance with the Data Protection Act 1998 and the Council's Data Protection Policy. In particular, the information obtained must be handled and stored securely. Any queries regarding an officer's obligations under the Data Protection Act should be directed to the Council's Data Protection Officer or Assistant Data Protection Officer.

10 DURATION, RENEWAL AND CANCELLATION

Duration

10.1 All Authorisations and Notices should specify the time period in relation to which the communications data are to be obtained. For example, it might authorise the SPOC to obtain information regarding all calls made from a specified number to another specified number in the two weeks immediately following the Authorisation. Or a Notice might require a CSP to confirm the subscriber details for a specific email account between two specified dates in the past. An authorisation: -

10.1.1 Cannot authorise or require any data to be obtained more than one month after the Authorisation or Notice is granted; and

10.1.2 In the case of a Notice, cannot authorise or require any disclosure of data not already in the possession of the CSP after the end of one month from the date of the grant of the Notice or Authorisation.

Renewal

10.2 RIPA provides that an Authorisation or Notice may be renewed for a period of up to one month by the grant of a further Authorisation or the giving of a further Notice. A renewed Authorisation or Notice takes effect upon the expiry of the Authorisation or Notice it is renewing.

10.3 Where the Applicant believes that a renewal is necessary and proportionate, they should complete an addendum to the original application, setting out their reasons for seeking renewal. They should then submit this to the SPoC, who will review it in the same way as a new application. Once the SPoC is happy with the application for renewal, they will notify the Designated Person that an application requires review.

10.4 Where a Designated Person is granting a further Authorisation or giving a further Notice to renew an earlier Authorisation or Notice, they should: -

10.4.1 consider and record in writing the reasons that it is necessary and proportionate to continue with the acquisition of the data being generated; and

10.4.2 record the date (and where appropriate the time) when the Authorisation or Notice is renewed.

10.5 A renewal **must** be approved by a Justice of the Peace before it will take effect. Any renewal must therefore be submitted to the SPOC in plenty of time to enable it to be reviewed and forwarded to the Designated Person for approval, and for approval to be sought from a Justice of the Peace. Where a renewal has been approved by a Designated Person, Legal Services must be notified at least 7 working days before expiry of the original Authorisation or Notice, so that they have sufficient time to seek approval from a Justice of the Peace.

10.6 In practice, given the requirement to obtain the approval of a Justice of the Peace and the time constraints this imposes, it will often be more practical to begin a new application, rather than to renew an existing Authorisation or Notice. Applicants who have not obtained, or do not expect to obtain, the data required within one month of grant of the Authorisation or Notice should discuss with the SPoC the best way to deal with this.

Cancellation

10.7 Where a Notice has been given to a CSP, and a Designated Person determines that it is no longer necessary or proportionate for the CSP to comply with the Notice, the Notice must be cancelled, and the CSP notified of the cancellation.

10.8 Where an Authorisation has been given and a Designated Person determines that it should cease to have effect because the conduct authorised is no longer necessary or proportionate, the Authorisation must be withdrawn, and the person authorised by the Authorisation must be informed.

10.9 The cancellation or withdrawal must: -

10.9.1 be in writing;

10.9.2 identify, by reference to its unique reference number, the Notice or Authorisation being cancelled;

10.9.3 record the date (and, where appropriate the time) when the Notice or Authorisation was cancelled;

record the name, office and rank/position held by the Designated Person.

10.10 Normally, it will be the Applicant who realises that a Notice or Authorisation is no longer necessary or proportionate (for example, because they have obtained the information required from elsewhere, or because the investigation has concluded for some reason). In this situation, the Applicant should notify the SPoC immediately. The SPoC will then alert the Designated Person that the Authorisation or Notice should be cancelled. The Designated Person should log on to the NAFN secure website to cancel the Authorisation or Notice. Where necessary, the SPoC will notify the CSP that the Authorisation or Notice has been cancelled.

10.11 Where the Designated Person who authorised the Application is unavailable, one of the other Designated Persons should cancel or withdraw the Authorisation or Notice so that no undue delay is caused.

11 RECORD KEEPING

NAFN keeps a full, electronic record of all applications on the Council's behalf, in accordance with the requirements of RIPA.

12 ERRORS

12.1 Where an error occurs in the grant of an Authorisation, the giving of a Notice, or as a consequence of any authorised conduct, or conduct undertaken to comply with a Notice, a record must be kept.

12.2 There are two types of error: -

i) an error which results in communications data being wrongly acquired or disclosed. This type of error is known as a "Reportable Error".

ii) an error which is identified after the Authorisation or Notice is given, but without data being wrongly obtained or disclosed. This type of error is known as a "Recordable Error".

12.3 If an Applicant or Designated Person identifies a Reportable or Recordable Error, they must notify the SPoC immediately.

12.4 A Reportable Error must be reported to the Interception of Communications Commissioner's Office (IOCCO). This report will be made by the SPoC at NAFN. It is **essential** that the SPoC is informed about any Reportable Error **immediately**, as the error must be investigated, the facts ascertained and the report made to the IOCCO within five working days of discovery of the error. If a SPoC requests assistance from the Applicant or another Council officer in connection with the investigation of an error, all reasonable assistance should be provided promptly.

12.5 If the Council receives material from a CSP which has no relevance to any investigation or operation by the Council, the material should be securely destroyed as soon as the report to the IOCCO has been made.

12.6 A record of all Recordable Errors will be held by NAFN, and made available for inspection by the IOCCO on request. The record will contain details of the error, how the error occurred, and an indication of what steps have been or will be taken to prevent the error from occurring again. The SPoC will notify the Designated Person and the Council's Senior Responsible Officer of all Recordable and Reportable Errors.

13 POLICY AND IMPLEMENTATION

13.1 The Policy is operational from 3rd April 2013 and replaces any previous policies and procedures relating to the acquisition of communications data.

13.2 The Monitoring Officer will report annually to the Audit Committee regarding the use made by the Council of its powers under RIPA.