REGULATION OF INVESTIGATORY POWERS ACT 2000

POLICY PRACTICE AND COMPLIANCE PROCEDURES FOR SOUTH KESTEVEN DISTRICT COUNCIL

COVERT SURVEILLANCE:

1. PURPOSE OF THIS POLICY

1.1 To assist investigating officers of the South Kesteven District Council in providing a procedure which is compliant with the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA).

1.2 This policy will be revised from time to time and should be read in conjunction with the Council's Human Rights Policy, current Enforcement Policies and CCTV operation Code of Practice plus any internal training materials produced in relation to RIPA and the Human Rights Act 1998 (HRA) that may be provided to relevant staff from time to time.

1.2. ACTIVITIES COVERED BY THIS POLICY

1.2.1 Since initial RIPA training in December 2001 and published guidance by Legal Services and Environmental Health Services, an audit of Council activities covered by RIPA has been carried out to identify those areas which could involve "directed surveillance" and "covert investigations" and could lead to the obtaining of "private information" about a person, the subject of the investigation and advertently or inadvertently forming part of that investigation. These specific concepts are explained, and guidance provided, in paragraph 3 below.

1.2.2 The following areas are considered to be the main Council functions requiring RIPA compliance:-

a) Housing Services – in particular tenant and neighbour disputes and/or antisocial behaviour investigations which might cover Council house tenants and their visitors.

b) Benefits Investigations – such as fraudulent claims which may require investigation of claimants which may reveal private information as defined in RIPA.

c) The Closed Circuit Television Services – whilst this is generally an overt system with signage indicating that CCTV monitoring is in operation there may be instances where the positioning of a camera to observe the subject of an investigation or the use of a

mobile camera for the same purpose may require a specific RIPA authorisation. This may be at the behest of one of the Council's own services or may originate from one of our partners such as the Police or Trading Standards.

d) Planning Enforcement – particularly involving investigations concerning the use of residential property which may reveal private information about a person.

e) Various licensing functions – such as taxi operations which may require investigations that reveal private information regarding a person and/or a licence holder.

f) Environmental Health Enforcement – concerning noise monitoring where prior notification may be required to ensure RIPA compliance if monitoring tests are to be carried out that could produce private information regarding a person.

1.3. IS RIPA AUTHORISATION REQUIRED?

1.3.1 An authorisation will be required if an investigation into an alleged regulatory breach of a Council function amounts to "directed surveillance" or is likely in carrying out the investigation to provide "private information" about a person either the subject of the investigation or forming part of the investigation and obtained either advertently or inadvertently. An authorisation can only be obtained from the Authorising Officers listed in paragraph 6 below.

1.3.2 "Directed surveillance" is defined by Section 26 (2) of the Act as covert surveillance undertaken:-

(a) For the purpose of a specific investigation or a specific operation.

(b) In such a manner as is likely to result in the obtaining of "private information" about a person (whether or not identified for the purposes of the investigation) and

(c) Otherwise by way of an immediate response to events occurring and as such it is not reasonably practical to obtain an authorisation.

1.3.3 "Private information" is defined by Section 26 (10) of the Act as "in relation to a person includes any information relating to his private or family life."

1.3.4 "Covert surveillance" is defined by Section 26 (9) of the Act as "if it is carried out in a manner that is calculated to ensure that persons who are the subject to the surveillance are <u>unaware</u> that it is or may be taking place."

1.3.5 A RIPA authorisation will also be required if in order to investigate an alleged regulatory breach it requires the use of a "covert human intelligence source." A covert human intelligence source occurs if an investigating officer uses either an informant or poses as an undercover officer and does not make clear to those he or she is investigating that he/she is an investigating officer of the Council and in posing as a covert human intelligence source attempts to maintain a relationship to obtain further information.

1.3.6 The Council does not, under any circumstances, have the power to undertake what is defined as "intrusive Surveillance".

Direct surveillance turns into intrusive surveillance if it is carried out on residential premises or any private vehicles and involves the presence of someone on the premises or in the vehicle or is carried out by means of a (high quality) surveillance device.

If the device is not on the premises or in the vehicle, it is only intrusive surveillance if it provides information of the same quality and detail as from a device actually present on the premises or in the vehicle.

1.3.7. The provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information, as part of their normal civic duties, or to contact numbers set up to receive information

CCTV cameras that are readily visible are not governed by RIPA. However, if the cameras are used as part of an operation to observe a known individual or group it is very likely that RIPA will apply and an appropriate authorisation will be required. Should an organisation such as the police request direct surveillance then the police authorise the action.

IF IN ANY DOUBT AS TO WHETHER A COURSE OF ACTION REQUIRES AUTHORISATION – GET IT AUTHORISED.

1.4. KEY QUESTIONS TO CONSIDER AT THE OUTSET OF AN INVESTIGATION

1.4.1 Does the investigation require some form of surveillance of a person or persons? If so is that surveillance likely to result in the obtaining of "private information" about a person?

1.4.2 Is the person being investigated unaware that the investigation or surveillance is taking place?

1.4.3 Is the investigation or surveillance an immediate response to events occurring or happening in front of you or a pre-planned operation?

1.4.4. If the answers to 4.1 or 4.2 are “yes” and the investigation is pre-planned then almost certainly an authorisation will be required before the investigation can commence.

1.5. WHEN SHOULD AN INVESTIGATION BE OVERT RATHER THAN COVERT?

1.5.1. In the majority of investigations carried out by the Council it is likely that the person being investigated will receive a letter at the commencement of the investigation confirming that a complaint has been received and that it is being investigated.

1.5.2 Unless you and your officer in charge of the investigation consider that a covert investigation is required then it should be normal practice to continue to write to the person being investigated setting out the nature of the complaint and the form of investigation that will follow.

1.5.3 In relation to noise investigations and complaints this procedure is particularly relevant. The person complained of should be informed of the nature of the complaint and the type of investigation including the noise monitoring that will be carried out and whether or not it will be time limited.

1.5.4 At the end of the investigation a letter should be sent to the person investigated advising them that the investigations are completed and either specific action or no further action will be taken in regard to the particular complaint.

1.6. AUTHORISATION PROCEDURE

An authorisation under RIPA will only be given if work is:
“for the purpose of preventing or detecting crime or of preventing disorder”

Prior to making an application for authorisation the investigator should first consider:-

(a) the possibility of a less intrusive method of investigation
(b) whether the surveillance could be done overtly and
(c) would the impact of direct surveillance justify the result?

1.6.1 An authorisation for a “directed surveillance” or “covert investigation” can be obtained from the following Authorising Officers:-

Chief Executive – Duncan Kerr
Monitoring Officer – Nick Goddard
Deputy Monitoring Officer – Lucy Youles
Housing Services – Phillip Doughty
Benefits – Kevin Legg
CCTV – Nick Goddard
Planning – Mike Sibthorp

Environmental Health – Bob Hadfield, David Price and Mike Brown

In the absence of a specified officer, any of the other officers can be contacted. The authorisation procedure should be a two person process so that the necessity for authorisation of an investigating officer can be tested and challenged by an Authorising Officer.

1.6.2. An application for an authorisation must be on one of the relevant forms which are annexed to this guidance. These forms are obtained from the Home Office website.

1.6.3 When making an application for an authorisation the investigating officer should seek a meeting with their authorising officer as soon as possible and provide a full explanation of the reasons why a "covert investigation/directed surveillance" is required in respect of the particular investigation. In deciding whether to grant an authorisation, the Authorising Officer must consider every application on its own merits and apply the tests of necessity and proportionality in relation to the Human Rights implications of the surveillance/investigation proposed as referred to in paragraph 8 below before deciding whether or not to grant an authorisation. This will include an assessment of the risk of collection of collateral information and/or third party information.

1.6.4 If an authorisation is granted then a copy of the authorisation must immediately be forwarded to Nick Goddard, Monitoring Officer who maintains a central record of all authorisations, each having a unique reference number.

1.6.5 If CCTV monitoring is required, they must be provided with a copy of the relevant authorisation whether it be internal or from an external agency to determine and abide by its terms and duration.

1.6.6 Authorisations must be cancelled as soon as they are no longer required, and, in any event, on or before the expiry date of the authorisation.

A written authorisation to use a Covert Human Intelligence Sources expires after 12 months from the date of last renewal or;

In all other cases (i.e. directed surveillance) 3 months from the date of their grant or latest renewal.

1.6.7 For urgent grants or renewals, oral authorisations are acceptable, but should be followed up with a written application as soon as possible thereafter. Urgent grants are those where authorisation would be needed but the circumstances are such that to obtain prior written authorisation would result in a missed opportunity for the gathering of information.

Any authorisation granted or renewed orally, (or by a person whose authorisation was confirmed to urgent cases) expires after 72 hours, this period beginning with the time of the last grant or renewal

1.7. REVIEW OF AUTHORISATIONS

1.7.1 The Authorising Officer should ensure that the authorisation is reviewed on a three monthly basis and that the outcome of each review is reported to Nick Goddard and retained for retention in the central record to ensure that authorisations are cancelled as soon as possible and are not maintained longer than is necessary nor proportionate for the investigation.

1.8. HUMAN RIGHTS ACT IMPLICATIONS

1.8.1 This policy acknowledges that any investigations undertaken by the Council should be subject to the Human Rights Act 1998 and Article 8 concerning a persons right to respect for private and family life.

1.8.2 This has been defined in the Courts to include the right to establish and to develop relationships with other human beings. Furthermore the Courts have now confirmed that the term “private life” must not be interpreted restrictively but as widely as possible. This policy aims to balance the rights of those persons within the Council’s jurisdiction afforded by Article 8 by ensuring that the investigation proposed is in relation to a lawful function of the Council. This will be the first consideration in determining whether to grant an application by an Authorising Officer.

1.8.3 Before issuing any authorisation, the Authorising Officer will then consider every case in accordance with the tests of necessity and proportionality in relation to the specific investigation proposed. This will take account of the circumstances of the investigations proposed and any relevant current Enforcement Policy of the Council. This will then be balanced against the necessity of a covert investigation to establish that an offence has or has not been committed. Likewise the same tests and procedure will be considered in carrying out a review and cancellation of any authorisation already granted.

1.9. THE USE OF CCTV FOR COVERT INVESTIGATIONS

1.9.1 If it is proposed to use the Council’s CCTV service for a covert investigation or directed surveillance and it is likely that in using the CCTV cameras that private information about a person may be obtained then an authorisation will be required. Furthermore any use of the Council’s CCTV Service must be subject to the existing Code of Practice which is attached to this policy document.

1.10. AGENCY ARRANGEMENTS

1.10.1 Some investigations may be shared with other agencies such as the Environment Agency, the Health and Safety Executive, the Police or other District Councils. If the investigation requires “directed surveillance” or a “covert investigation” to be carried out then the party that is the principal investigating authority will be required to obtain the authorisation. The investigating officer of this authority should obtain a copy of that authorisation which should be kept on file by the Authorising Officer and a copy sent to Nick Goddard for central recording purposes. If CCTV is involved then as indicated at 6.5 the CCTV control room also require a copy.

2. RIPA PART 1 CHAPTER II – THE ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

2.1 INTRODUCTION

Part 1 Chapter II (sections 21 – 25 of RIPA) came into force on 5th January 2004. It regulates the acquisition and disclosure of communications data. It provides powers for the Council to gain communications information when carrying out investigations. It also regulates information previously gained without regulations, which now has to be authorised.

The process is similar to that of the authorisation of directed surveillance and CHIS, but has extra provisions and processes.

The purpose of the introduction is the same, that is, to protect people's human rights. The effect of not gaining authorisation when needed is the same. The Council leaves itself open to a challenge under the Human Rights Act 1998 and the evidence gained without authorisation may not be admissible in court.

RIPA specifies that the only purpose for which the Council can gather communication data is in the:

'Prevention and detection of crime or preventing disorder'

There is a draft Code of Practice. It can be found at Appendix 2, on the public drive under RIPA and as an Appendix to the Policy and Guidance on the Intranet. It is also available on the Home Office website by clicking on this hyperlink.

www.homeoffice.gov.uk

Staff should refer to the Home Office Codes of Conduct for supplementary guidance

The Code does not have the force of Statute but are admissible in evidence in any criminal and civil proceedings.

2.2 WHAT IS COMMUNICATIONS DATA?

The definition of communications data includes information relating to the use of a communications service but it does not include the contents of the communication itself. It is broadly split into 3 categories:-

- Traffic data – where a communication was made from, to who and when
- Service data – the use made of a service by any person e.g itemised telephone records
- Subscriber data – any other information held or obtained by an operator on a person they provided a service to

The Council is restricted to subscriber and service use data and even then only for the purpose of preventing or detecting crime and disorder. For example a benefit fraud investigator may be able to get access to an alleged fraudster's mobile phone bills.

The word 'data' in relation to a postal item means anything written on the outside such as an address. Officers at the Council have previously been able to apply for the new address of a person that they were investigating, that is the redirection details. A request form was completed and the post office supplied the information. This activity is now regulated and authorisation needs to be gained.

THE CODE DOES NOT COVER THE INTERCEPTION OF COMMUNICATIONS (I.E. THE CONTENTS OF ANY COMMUNICATIONS INCLUDING THE CONTENT OF AN E-MAIL, OR INTERACTION WITH WEBSITES).

2.3 AUTHORISATIONS, NOTICES, RENEWALS AND DURATION

2.3.1 AUTHORISATIONS AND NOTICES

The Code states that a 'designated person', must decide whether authorisation is necessary and proportionate to the action to be taken. The designated person is in effect the Authorising Officer. The designated persons at this Council are Nick Goddard, Dave Marvin, Kevin Legg, Bob Hadfield, Richard Edwards, David Price, Mike Smith and Phillip Doughty.

There are two ways to authorise access to communications data:-

(a) Authorisation under 22(3). This allows the authority to collect the data itself. This may be appropriate where:

- The postal or telecommunications operator is not capable of collecting or retrieving the communications data;
- It is believed that the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- There is a prior agreement in place between the relevant public authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of data.

(b) By a notice under section 22(4). A notice is given to a postal or telecommunications operator and requires that operator to collect or retrieve the data and provide it to the authority.

The designated person decides whether or not an authorisation should be granted.

The designated person must take account of the following points when deciding whether to authorise the application or not:-

- Is the accessing of data for the prevention or detection of crime or disorder?
- Why is obtaining the data necessary for that purpose?
- Is obtaining access to the data by the conduct authorised proportionate to what is being sought to be achieved? That is what conduct are you authorising and is it proportionate?
- Is the accessing of the data likely to result in collateral intrusion? If so, is the access still justified?
- Is any urgent timescale justified?

The designated person will make a decision whether to grant the authorisation based upon the application made. The application form should subsequently record whether or not the application was approved or not, by whom and the date. A copy of the application must be kept by the officer until it has been inspected by the Commissioner.

If the application is authorised and the notice needs to be served, then only the notice is served upon the postal or telecommunications officer.

The application form and the authorisation itself are not served upon the holder of the communications data.

The postal or telecommunications service can change for providing the information.

2.3.2 PROVISIONS OF RIPA

Single Point of Contact (SPOC)

Notices and authorisations for communications data should be channelled through a SPOC. The Code states that this is to provide an effective system in that the SPOC will deal with the postal or telecommunications operator on a regular basis. Jeanette Strutt has been allocated the role of the SPOC. The SPOC will advise the Authorising Officer/designated person on whether an authorisation and/or notice is appropriate.

The single point of contact should be in a position to:-

- Where appropriate, assess whether access to communications data is reasonably practical for the postal or telecommunications operator;
- Advise applicants and designated persons on the practicalities of accessing different types of communications data from different postal or telecommunications operators;
- Advise applicants and designated persons on whether communications data falls under section 21(4)(a), (b) or (c) of the Act. That is traffic, service or subscriber data;
- Provide safeguards for authentication;
- Assess any cost and resource implications to both the public authority and the telecommunications operator.

Oral Authority

An oral application and approval can only be made on an urgent basis for the purpose set out in 22(2)(g) of the Act. That is:-

> "for the purpose, in emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health"

That is not a purpose under which the Council is able to collect communications data and therefore oral authorisations are not possible.

Duration

Authorisations and notices will only be valid for one month beginning from when it was granted. If the information can be collected in a shorter time period then that should be specified. This would accord with the proportionality element of the decision-making.

The postal or telecommunications operator need only comply with the request if it is reasonably practicable to do so.

Renewal

An authorisation or notice can be renewed at any point during the month that it is valid by following the same procedure as in obtaining a fresh authorisation.

Cancellations

The duty to cancel falls on the designated person who authorised it. The notice shall be cancelled as soon as it is no longer necessary or is no longer proportionate to what is being sort to be achieved.
Authorisations should also be cancelled.
In the case of a section 22(4) notice, the postal or communications operator shall be informed of the cancellation.

Retention

Applications, authorisations and notices will be retained by the authority until they have been audited by the Commissioner. The authority should also keep a record of the dates that the notices and authorisations were started and cancelled. A copy of each form should be kept by the Investigating Team and the originals kept in the Central Register. It shall be the responsibility of the designated person to ensure that the records are accurate and kept up to date.

Combined Authorisations

Applications for communications data may only be made by persons in the same authority as a designated person. There cannot, therefore, be any combined authorisations.

Errors

Where any errors have occurred in the granting of authorisations or the giving of notices, a record should be kept and a report and explanation sent to the Commissioner as soon as practical.

3. BENEFITS OF OBTAINING AUTHORISATIONS UNDER RIPA

Authorisation of surveillance, human intelligence sources and the acquisition and disclosure of communications data.

RIPA states that:

"if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it shall be "lawful for all purposes".

However, the opposite is not true – i.e. if you do not obtain *RIPA* authorisation it does not make any conduct unlawful (e.g. use of intrusive surveillance by local authorities). It just means you cannot take advantage of any of the special RIPA benefits and you may have to justify infringing a person's Human Rights and any evidence you place before the courts may be subject to challenge in respect of the processes used to obtain the evidence (s78 Police and Criminal Evidence Act 1984).

RIPA states that a person shall not be subject to any civil liability in relation to any conduct of his which –

a) is incidental to any conduct that is lawful by virtue of an authorisation; and

b) is not itself conduct for which an authorisation is capable of being granted under a relevant enactment and might reasonably be expected to have been sought in the case in question.

However **IF YOU ARE IN ANY DOUBT** about whether a course of action requires an authorisation, **GET IT AUTHORISED.** (If you are unable to secure an authorisation it is likely that your application does not comply with the law).

4. SCRUTINY AND TRIBUNAL

RIPA set up the Office of the Surveillance Commissioner to regulate the conduct of public bodies and to monitor their compliance with *RIPA.* The

Chief Surveillance Commissioner will keep under review, among other things, the exercise and performance of duties, imposed in *RIPA* by the persons on whom those duties are conferred or imposed. This includes authorising directed surveillance and the use of covert human intelligent sources.

A tribunal has been established to consider and determine complaints made under *RIPA* if it is the appropriate forum. Persons aggrieved by conduct, e.g. directed surveillance, can make complaints. 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 period.

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.

5. AUTHORISATION FORMS

Authorisation forms can be found at Appendix 1 and should be used in conjunction with this Policy but will be updated as necessary from time to time.

January 2005
SG/COR 09796