SOUTH LAKELAND DISTRICT COUNCIL

GUIDANCE ON SURVEILLANCE UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000

June 2018

CONTENTS

1. INTRODUCTION

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) regulates covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that law enforcement and security agencies have the powers they need to do their job their effectively.

1.2 South Lakeland District Council ("the Council") is therefore included within the RIPA framework with regard to the authorisation of both Directed Surveillance and of the use of Covert Human Intelligence Sources.

1.3 The purpose of this guidance is to explain the scope of RIPA and the circumstances where it applies and provide guidance on the authorisation procedures to be followed. This guidance also includes details relating to the Investigatory Powers Act 2016, which came into force on 30th December 2016.

1.4 The Council has had regard to the Codes of Practice produced by the Home Office in preparing this guidance and the Solicitor to the Council has copies to which staff can refer. The relevant codes of practice and associated guidance that relate to authorised Council activity are:

(a) Home Office Code of Practice – Covert Surveillance;
(b) Home Office Code of Practice – Covert Human Intelligence Sources
(c) Guidance from the Office of Surveillance Commissioners
(d) Protection of Freedoms Act 2012-changes to provisions under the Regulation of Investigatory Power Act 2000 Home Office Guidance for Magistrates' Courts in England and Wales for a local authority application seeking an order approving the grant or renewal of a RIPA authorisation or notice
(e) Guidance on Investigatory Powers Act 2016

1.5 In summary RIPA requires that when the Council undertakes directed surveillance or uses "covert human intelligence source" these activities must only be authorised by an officer with delegated powers when the relevant criteria are satisfied. RIPA states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it should be "lawful for all purposes". The Council has nominated officers ("Authorising Officers") who can grant authorisations. The Authorising Officers are The Chief Executive, the Director (People and Places), the Assistant Director (Resources) and the Assistant Director Neighbourhood Services.

1.6 Chapter 2 of Part 2 of the Protection of Freedoms Act 2012 ("the 2012 Act") amends RIPA so as to require the Council to obtain judicial approval for the use of covert investigatory techniques available to them under RIPA.

1.7 Part 2 of the 2012 Act specifies the grounds for which authorisations can be granted for carrying out both Directed Surveillance and of the use of Covert Human Intelligence Sources. Furthermore the 2012 Act provides that use of RIPA to authorise directed surveillance will have to be confined to cases where the offence under investigation carries a maximum custodial sentence of 6 months or more, save in cases in relation to the sale of alcohol and tobacco to minors where the new threshold would not apply and offences under sections 146, 147 or 147A of the Licensing Act 2003

1.8 The Council has to apply to the Magistrates' Court for an Order approving the use of the authorisation.

1.9 Subject to the need for approval from the Magistrates Court as referred to above, authorisation under RIPA gives lawful authority to carry out surveillance and the use of a source. Obtaining authorisation helps to protect the council and its officers from complaints of interference with the rights protected by Article 8(1) of the European Convention of Human Rights, by the Human Rights Act 1998. This is because the interference with the private life of citizens will be "in accordance with the law", provided activities undertaken are also "reasonable and proportionate."

1.10 There are two types of surveillance:

Directed Surveillance – This is surveillance undertaken for the purpose of a specific operation and in a manner which is likely to result in the obtaining of private information about a person (whether or not that person is the target of the investigation or operation); and is carried out in a planned manner and not by way of an immediate response; and

Intrusive Surveillance – This is surveillance that takes place on residential premises or any private vehicle and involves the presence of an individual on the premises or in the car, or by the use of a surveillance device that although not in the car/premises, provides data as though it was.

1.11 Under RIPA the Council cannot authorise any form of "Intrusive Surveillance".

1.12 Deciding when an authorisation is required involves making a judgment. For example, environmental health officers might covertly observe and then visit a shop as part of their enforcement functions. Such observations may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras. Where this does not involve systematic surveillance of an individual, it forms a part of the everyday functions of law enforcement authorities or other public bodies. This low-level activity will not usually be regulated under the provisions of RIPA.

1.13 Conversely where systematic covert surveillance is undertaken then an authorisation will be required. Neither the provisions of RIPA nor the Codes of Practice cover the use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use around Council car parks and in the public parts of Council buildings in order to prevent crime. However use of CCTV cameras to target a person would require an Authorisation and this is dealt with in Section 5 of this document. If you are in doubt, seek the advice of an Authorising Officer, if they are in doubt they will seek advice from the Solicitor to the Council.

1.14 There may be a necessity on occasions for the Council to undertake surveillance which does not meet the criteria for the use of RIPA. For example

- certain types of criminal behaviour which the 2012 Act states cannot be the subject of a RIPA authorisation; and
- certain serious disciplinary or audit investigations which may merit surveillance.

1.15 The Council must still meet its obligation under the Human Rights Act 1998. Any surveillance which is carried out outside of RIPA must still be necessary and proportionate taking into account the issue of intrusion into a person's privacy. The decision making process and the management of such surveillance must be well documented.

1.16 There is a requirement for the Council's Senior Responsible Officer to regularly monitor surveillance outside of RIPA. Therefore before any such surveillance takes place, advice must be sought from the Solicitor to the Council.

2. DIRECTED SURVEILLANCE

2.1 Surveillance is 'Directed' for the purposes of RIPA if it is covert, but not intrusive and is undertaken:

(a) for the purposes 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 one is specifically identified for the purposes of the investigation or operation); and

(c) 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.

2.2 Before any officer of the Council undertakes any surveillance of any individual or individuals they need to assess whether the activity comes within RIPA. In order to do this the following key questions need to be asked:

(a) Is the surveillance covert? Covert surveillance is that carried out in a manner calculated to ensure that subjects of it are unaware it is or may be taking place. If activities are open and not hidden from the subjects of an investigation, the RIPA framework does not apply;

(b) Is it for the purposes of a specific investigation or a specific operation e.g. car park CCTV cameras which are readily visible to anyone walking around the area covered? The answer is not if their usage is to monitor the general activities of what is happening in the vicinity. However, if that usage changes, RIPA may apply. If CCTV cameras are targeting a particular known individual, and are being used in monitoring his/her activities, that has turned into a specific operation which will require authorisation.

(c) Is it in such a manner that is likely to result in the obtaining of private information about a person e.g. if part of an investigation is to observe a person's home to determine their comings and goings then that would be covered. If it is likely that observations will not result in the obtaining of private information about a person, then it is outside the RIPA framework. However, the use of 'test purchasers' may involve the use of Covert Human Intelligence Sources. If in doubt, it is safer to get authorisation;

(d) Is it by way of an immediate response to events or circumstances? The Home Office gives the example of anything happening as an immediate response to something occurring during the course of an observer's work which is unforeseeable. If so it is likely that an authorisation is not required. However, if as a result of an immediate response, a specific investigation subsequently takes place, that brings it within the RIPA framework.

3. COVERT USE OF HUMAN INTELLIGENCE SOURCE

3.1 A person is a Covert Human Intelligence Source ("a CHIS") if he/she establishes or maintains a personal or other relationship with a person for the covert purpose of using such a relationship either to obtain information or provide access to information about another person. A relationship is covert, if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose.

3.2 The above clearly covers the use of professional witnesses to obtain information and evidence. It can also cover "entrapment" cases.

3.3 Special safeguards apply to the granting of authorisations where the CHIS would be a juvenile (under 18 years of age). Authorisations cannot be granted unless the provisions within The Regulation of Investigatory Powers (Juveniles) Order 2000 are satisfied. Only the Chief Executive (or in his absence, the Director-People and Places) can authorise the use of a juvenile CHIS. If any Council officer intends to use juvenile CHIS, advice and guidance should be sought from the Solicitor to the Council before any steps are taken.

4. AUTHORISATIONS, RENEWALS, DURATION AND CANCELLATION

4.1 No officer shall grant an authorisation for the carrying out of Directed Surveillance unless he/she believes that an authorisation is necessary and proportionate to what is sought to be achieved by carrying it out.

4.2 The 2012 Act provides that an authorisation is necessary only if it is for the purpose of preventing or detecting crime. The onus is therefore on the person authorising such surveillance to satisfy themselves it fulfils this criteria.

4.3 In order to ensure that Authorising Officers have sufficient information in order to make an informed decision and so that a sound case is presented when seeking the approval of the Magistrates Court, it is important that detailed records are maintained. As such the standard forms in the Appendix 2 are to be completed where relevant. It is also sensible to make any authorisation sufficiently wide enough to cover all the means required as well as being able to prove effective monitoring of what is done against that is authorised.

4.4 Authorisations must be in writing using the appropriate standard form RIPA 1 (Directed Surveillance) or RIPA 5 (CHIS). Appendix 2 to this guidance contains copies of all the standard forms which are to be used by all Council Directorates.

4.5 Although it is possible to combine two authorisations in one, the Council's practice is for separate forms to be completed to maintain the distinction between Directed Surveillance and the use of a CHIS.

4.6 Authorisations lapse, if not renewed:-

(a) in the case of Directed Surveillance 3 months from the date of the Magistrates' Court approval of either an authorisation or the latest renewal.

(b) in the case of a CHIS 12 months, from date of approval of an authorisation or the latest renewal by the Magistrates' Court.

4.7 As is the case with an Authorisation, renewal needs the approval of the Magistrates Court.

4.8 Forms RIPA 2 (Directed Surveillance) and RIPA 7 (CHIS) must be used for all renewals. The following should also be noted:-

(a) All authorisations must be reviewed every 4 weeks and Form RIPA 3 (Directed Surveillance) or Form RIPA 7 (CHIS) completed;

(b) When an authorisation is cancelled a Form RIPA 4 (Directed Surveillance) or RIPA 8 (CHIS) must be completed.

4.9 Subject to approval by the Magistrates Court, an authorisation can be renewed using the Renewal Form RIPA 2 (Directed Surveillance) or RIPA 6 (CHIS) at any time before it ceases to have effect by any person entitled to grant a new authorisation in the same terms. In the case of a CHIS, a person should not renew (using form RIPA 6) unless a review has been carried out (using Form RIPA 7) and that person has considered the results of the review when deciding to renew or not. A review must cover what use has been made of the CHIS, the tasks given to them and information obtained.

4.10 Authorising Officers are responsible for ensuring that authorisations undergo timely reviews for which a RIPA 3 (Directed Surveillance) or RIPA 7 (CHIS) form must be completed. Also that they are cancelled promptly if the Directed Surveillance activity (using Form RIPA 4) or use of a CHIS (using form RIPA 8) is no longer necessary.

4.11 Cancellation of the authorisation and completion of Form RIPA 4 (Directed Surveillance) or RIPA 8 (CHIS) must be carried out in all cases as soon as the actual surveillance activity for which authorisation was specifically granted ceases. Authorisations must not be allowed to continue in force until they reach the stated expiry date without cancellation if the surveillance activity or use of a source is no longer in operation. However should this occur formal cancellation must be carried out and evidenced by the completion of Form RIPA 4 (Directed Surveillance) or RIPA 8 (CHIS) as soon as this is detected even though this will result in a cancellation date after the expiry date.

4.12 Cancellation should wherever possible be carried out by the same person that granted the original request or renewal. If that person is no longer available to do this then it should be completed by the person appointed to replace them or by one of the other Authorising Officers.

4.13 A copy of the Form RIPA 4 (Directed Surveillance) or RIPA 8 (CHIS) completed to evidence the cancellation must be sent to the Solicitor to the Council to be recorded on the central register and the original held securely within the originating unit.

4.14 Any person giving an authorisation should give particular consideration to collateral intrusion i.e. interference with the privacy of persons other than the subject(s) of surveillance. Such collateral intrusion or interference would be a matter of greater concern in cases where there are special sensitivities, for example in cases of premises used by lawyers or for any form of medical or professional counselling or therapy.

4.15 An application for an authorisation should include an assessment of the risk of any collateral intrusion or interference. This will be taken into account by the Authorising Officer, particularly when considering the proportionality of the surveillance.

4.16 Those carrying out the Covert Surveillance should inform the Authorising Officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

4.17 Any person giving an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place or of similar activities being undertaken by other public authorities which could impact on the development of the surveillance.

4.18 No operations will be undertaken in circumstances where investigators believe that surveillance will lead to them to intrude on spiritual counselling between a Minister and a member of his/her faith. In this respect, spiritual counselling is defined as conversations with a Minister of Religion acting in his/her official capacity where the person being counselled is seeking or the Minister is imparting forgiveness, or absolution of conscience.

4.19 RIPA refers to 'confidential material' namely:

(a) matters subject to legal privilege;
(b) confidential personal information; or
(c) confidential journalistic material.

4.20 RIPA does not provide any special protection for 'confidential material'. Nevertheless, such material is particularly sensitive, and is subject to additional safeguards under the code. In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of confidential material, the deployment of the source should be subject to special authorisation. In such circumstances only the Chief Executive or in his absence the Director–People and Places can grant an authorisation.

4.21 In general, any application for an authorisation which is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Special care should be taken where the target of the investigation is likely to be involved in handling confidential material. Such applications should only be considered in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

4.22 The following general principles apply to the acquisition of confidential material:

(a) Confidential material should not be retained or copied unless it is necessary for a specified purpose;
(b) Confidential material should be disseminated only where an appropriate officer is satisfied that it is necessary for a specific purpose;
(c) The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature; and appropriate safeguards as to its security must be implemented;
(d) Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

4.23 In cases of joint working, for example, with other agencies on the same operation only one authorisation is required. Duplication of authorisations does not affect the lawfulness of the activities to be conducted, but may create an unnecessary administrative burden on the agencies.

4.24 Applications for Directed Surveillance or the use of a source are to be retained by the Authorised Officer, for a period of 5 years. Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period commensurate to any subsequent review.

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

4.26 There is nothing in RIPA that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However, the use outside the authority that authorised surveillance, of any material obtained by means of Covert Surveillance and, other than in pursuance of the grounds on which it was obtained, should be authorised only in the most exceptional circumstances.

4.27 The Council will not use an external or professional source for the purpose of obtaining information. It is not the Council's general practice to seek, cultivate or develop a relationship with a potential external or professional source. It is possible, though highly unlikely, that the role of a Council employee may be that of a source, for example in 'entrapment cases'

4.28 The Authorising Officer must consider the safety and welfare of an employee acting as a source, and the foreseeable consequences to others of the tasks they are asked to carry out. A risk assessment should be carried out before authorisation is given. Consideration from the start for the safety and welfare of the employee, even after cancellation of the authorisation, should also be considered.

4.29 The Council's practice is not to use an employee acting as a source to infiltrate existing criminal activity, or to be a party to the commission of criminal offences, even where this is within the limits recognised by law.

Further details about the Council's Procedures for seeking authorisations are set out in Appendix 1.

5 The Investigatory Powers Act 2016

5.1 The Investigatory Powers Act 2016 which came into force on 30th December 2016 sets out, amongst other things, how communications data can be obtained. Section 61 specifically excludes local authorities from being able to obtain internet connection records (ICRs). However, sections 73-79 define local authorities as a relevant public authority for the purposes of Part 3 of the Act and set out the circumstances in which a local authority authorisation for obtaining communications data (other than ICRs) can be granted. In order to obtain communications data, proposed conduct must be proportionate to what is sought to be achieved and judicial approval from a justice of the peace obtained and the following tests must be satisfied:-

- It must be for the purpose of preventing or detecting crime or of preventing disorder.
- The local authority must be part of a collaboration agreement that has been published and has been certified by the Secretary of State
- The authorisation must be granted by a designated senior officer, which means a director, head of service, service manager, or equivalent or a higher person.
- It must be granted to an officer of a local authority that is either a 'supplying' or 'subscribing' authority under the collaboration agreement. (The Council have not entered into a collaboration agreement. Should the need arise in the future, arrangements could be made to enter into such an agreement)
- A person who is acting as the single point of contact must be consulted, unless the circumstances are exceptional, i.e. an imminent threat to life.

6 CCTV

6.1 The Council has no responsibility for any town centre CCTV systems. It does have CCTV at Town View Fields Hostel, car parks and public areas within its offices. Given the limited scope of its CCTV coverage, the use of CCTV in Directed Surveillance is unlikely. Use of the Council owned or operated CCTV cameras to target a person would be Directed Surveillance. Before an officer of the Council undertakes such activity, an Authorisation is required in accordance with the procedures set out in this document.

6.2 Similarly, given the limited scope of the Council's CCTV coverage, proposals for the use of the Council's CCTV by external organisations for Directed Surveillance are also unlikely to be forthcoming.

6.3 When there is a proposal for the use of the Council owned or operated CCTV cameras by an external organisation to target a person, it is for that organisation to obtain their own RIPA authorisation. A copy of this Authorisation must be passed to the appropriate responsible Council officer before such activity can be carried out. If the request is urgent, the appropriate responsible Council officer can authorise the use of the Council's CCTV cameras but only upon receiving a written assurance from an officer of the external organisation that authorisation will be obtained. Details of the request should be then be recorded by the appropriate responsible Council officer and a copy of the authorisation sought as soon as is reasonably practicable.

6.4 Please note that the 2012 Act removes from Local Authorities the ability to obtain urgent authorisations. The CCTV operator therefore must not allow purported use of an "urgent authorisation" to enable access to Council owned or operated CCTV by any other Local Authority. The Council's CCTV Policy has been reviewed to take into account the Data Protection Act 2018 and GDPR.

7 SOCIAL AND BUSINESS NETWORKING SITES AND INTERNET SITES

7.1 Although social and business networking sites and internet sites are easily accessible if they are going to be used during the course of an investigation, consideration must be given to whether authorisation under RIPA should be obtained.

7.2 Care must be taken to understand how the social or business networking site or internet site works. Officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

7.3 It is the responsibility for an individual to set privacy settings to protect against unsolicited access to their private information on a social or business networking site. Unprotected data may be deemed published and no longer under the control of the author. The author has a reasonable expectation of privacy if access controls are applied. Where privacy settings are available but not applied the data may be considered open source and authorisations are not usually required.

7.4 Relevant members of staff who make use of social media and internet sites for investigative purposes must appreciate that what they may begin as an entirely legitimate use by them of social media and internet sites can sometimes develop into surveillance which falls within the protective ambit of the legislation. The use of such media to build a profile of a person or regular use to monitor a person's activities might

be an infringement of their privacy and may meet the criteria for authorisation under RIPA if the ground for necessity is met, i.e. prevention or detection of crime. Advice and guidance can be obtained from the Solicitor to the Council before embarking on use of such sites for investigative purposes.

7.5 Any use of social media sites for investigative purposes must be accessed by a Council enforcement account and staff should never use their own personal accounts for this purpose.

7.6 If it necessary and proportionate for the Council to covertly breach access controls, an authorisation for Directed Surveillance will be required. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by the officer. This could be in circumstances where the activity is more than a mere reading for the site's content. This could occur if an officer covertly asks to become a "friend" or be "connected" on someone's social or business networking site.

7.7 A CHIS authorisation may be required when using an internal trading organisation in circumstances when a covert relationship is likely to be formed. However the use of disguised purchaser details in a single overt electronic purchase is not likely to require a CHIS authorisation because no relationship is usually established at this stage.

8 IMPACT OF General Data Protection Regulation (GDPR) and Data Protection Act 2018

8.1 The Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR) came into force on 25 May 2018. The general rules applicable to employee surveillance as espoused by the DPA and the employment code will remain the same.

Impact assessments

One of the main recommendations of the Information Commissioners Office code is that employers should undertake an impact assessment before undertaking surveillance. This is best done in writing and should, among other things, consider whether the surveillance is necessary and proportionate.

The Council must demonstrate and record its general obligation of data protection by design and default as detailed under Chapter 4, Section 57 of the Data Protection Act 2018. Chapter 4 of the Data Protection Act 2018 and Article 35 of the GDPR introduces the concept of a Data Protection Impact Assessment (DPIA) (also known as a Privacy Impact Assessment) as a tool, which can help data controllers (in this case employers) identify the most effective way to comply with GDPR obligations. A DPIA is required when the data processing is 'likely to result in a high risk to the rights and freedoms of natural persons'.

The Article 29 Working Party recently published its data protection impact assessment guidelines for comments. It sets out the criteria for assessing whether data processing is high risk. This includes processing involving:

1. Evaluation or scoring, including profiling and predicting, especially from aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements;
2. Automated decision-making with legal or similar significant effects;
3. Systematic monitoring of
4. individuals;
5. Sensitive data;
6. Personal data on a large scale;
7. Datasets that have been matched or combined;
8. Data concerning vulnerable data subjects;

9. Innovative use or application of technological or organisational solutions;
10. Data transfers across borders outside the EU;
11. Data that prevents data subjects from exercising a right or using a service or a contract.

Employee monitoring is very likely to satisfy a number of the above criteria (particularly 3, 7 and 10) and so will be considered as high-risk processing under article 35 requiring a DPIA.

Chapter 4, Section 64 of the Data Protection Act 2018 and the GDPR sets out the minimum features which must be included in a DPIA:

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the data controller;
- An assessment of the necessity and proportionality of the processing in relation to the purpose;
- An assessment of the risks to individuals; and
- The measures in place to address risk, including security, and to demonstrate that the data controller is complying with GDPR.

Before doing a DPIA, the data protection officer's advice, must be sought as well as the views (if appropriate) of data subjects or their representatives. The views of the ICO may also have to be sought. In all cases the data controller is obliged to retain a record of the DPIA which may be reviewed by the ICO at a later date in the event of an audit or investigation arising from the data controller's use of personal data.

Article 6 – lawfulness

All forms of processing of personal data (including employee surveillance) have to be lawful by reference to the conditions set out in article 6 of the GDPR (equivalent to Chapter 2, Section 8 of the Data Protection Act 2018.) One of these conditions is consent. Article 4(11) states: '"Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'

Consent is more difficult under the Data Protection Act 2018 and GDPR. This is especially so for employers conducting employee surveillance. Part 1, Section 2(1)(a) of the Data Protection Act 2018 makes specific regard to the lawful and fair processing of personal data on the basis of the 'data subject's consent or another specified basis. According to ICO draft guidance on consent under GDPR: 'Consent will not be freely given if there is imbalance in the relationship between the individual and the controller – this will make consent particularly difficult for public authorities and for employers, who should look for an alternative lawful basis.'

Public authorities

Article 6 states that the legitimate interest's condition shall not apply to processing carried out by public authorities in the performance of their tasks. Such organisations will have to consider the applicability of the legal obligation and public interest/official authority conditions (articles 6(1)(c) and 6(1)(e) respectively) to justify surveillance.

9 NON RIPA SURVEILLANCE

9.1 RIPA does not grant powers to carry out surveillance. It simply provides a framework that allows the Council to authorise and supervise surveillance in a manner that ensures compliance with the Human Rights Act 1998. Equally RIPA does not prevent surveillance from being carried out or require that surveillance may only be carried out under RIPA.There may be times when it will be necessary to carry out covert Directed Surveillance or use a CHIS other than by using RIPA. For example there may be a serious internal investigation that may lead to criminal proceedings. In such circumstances RIPA procedures may be appropriate. However in relation to an investigation that for example a member of staff or a contractor is not carrying out their work as contracted, then a RIPA authorisation is not usually available as in such circumstances criminal proceedings are not normally contemplated.

9.2 Similarly there may be serious cases of neighbour nuisance or involving anti-social activity which involve potential criminal offences for which the penalty is below the thresholds which would enable use of a RIPA authorisation. Nonetheless there may be strong grounds for carrying out Directed Surveillance or use of a CHIS. Indeed there may be circumstances in which Directed surveillance or use of CHIS is the only effective means of efficiently obtaining significant information to take an investigation forward.

9.4 In the circumstances outlined above a RIPA application may be completed in accordance with this Policy and the application must be clearly endorsed in red "NON_RIPA SURVEILLANCE" along the top of the first page. The application must be submitted in the normal fashion to the Authorising Officer who must considered it under the necessity and proportionality test in the same way they would a RIPA application. The normal procedure of timescales, review and cancellations must also be followed.

9.5 The authorisation, regular review, the outcome of any review, renewal applications and eventual cancellation must be notified to the Solicitor to the Council in the normal way and using the same timescales as would be applicable to a RIPA investigation. However for non RIPA surveillance the requirement to seek approval from the Magistrates Court is inapplicable. The Authorisation for non RIPA surveillance takes effect from the date that it is authorised by the Authorising Officer.

10. CENTRAL REGISTER OF AUTHORISATIONS

10.1 RIPA requires a central register of all authorisations to be maintained. The Solicitor to the Council maintains this register.

10.2 Whenever an authorisation is granted the Authorising Officer must arrange for a copy of the authorisation to be forwarded to the Solicitor to the Council. In addition copies of any other forms completed, as listed in Appendix 2, must also be so forwarded. Copies of the orders of the Magistrates Court approving or refusing the grant or renewal of an authorisation will also be placed on the Central Register of Authorisations.

10.3 It is the responsibility of each Directorate to arrange for the secure retention of all authorisations that are generated by them. Authorisations should only be held for as long as they are necessary. Once the investigation is closed (bearing in mind cases may be

lodged some time after the initial work) the records held by the Directorate should be destroyed.

11. CODES OF PRACTICE

11.1 There are Home Office Codes of Practice referred to in paragraph 1.4 above, that expand on this guidance. The codes do not have the force of statute, but are admissible in evidence in any criminal and civil proceedings.

12. BENEFITS OF OBTAINING AUTHORISATION UNDER RIPA

12.1 The Home Office Codes of Practice say councils should appoint a Senior Responsible Officer. This person is responsible for the integrity of the surveillance process, ensuring the Council complies with RIPA and relevant legislation, and also engaging with the Inspectors when they conduct their inspections. The Council's Senior Responsible Officer is the Director of Policy and Resources (Monitoring Officer)

12.2 The Codes of Practice also say elected members should review the Council's use of RIPA and review the policy once a year. In addition to this, internal quarterly reports on the use of RIPA should be provided, including any 'nil returns' to ensure consistency and compliance with Policy. These quarterly reports are submitted to the Cabinet Member for Council Organisation, People and Wellbeing. Details of any non RIPA surveillance will also be reported annually and quarterly in the same way.

12.3 Consideration should also be given to appropriate liaison with the Local Magistrates Court with a view to reviewing consistency of approach and any training needs of the court clerks and magistrates.

13. SCRUTINY AND TRIBUNAL

13.1 To effectively "police" RIPA, Commissioners have been appointed to regulate conduct carried out under RIPA. The Chief Surveillance Commissioner will keep under review, among others, the exercise and performance by the persons on whom are conferred or imposed, the powers and duties under the Act. This includes authorising Directed Surveillance and the use of CHIS.

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

13.3 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.

APPENDIX 1- PROCEDURE FOR APPLYING FOR AUTHORISATIONS

Applications

1. Applications for authorisation to carry out directed surveillance must be made in writing and should describe any conduct to be authorised and the purpose of the investigation or operation. The application should also include:-
   - The reasons why the authorisation is necessary in the particular case and on the relevant ground-this is for the purpose of preventing or detecting crime or of preventing disorder;
   - The reasons why the surveillance is considered proportionate to what it seeks to achieve;
   - The nature of the surveillance;
   - The identities where known, of those to be the subject of the surveillance;
   - An explanation of the information which it is desired to obtain as a result of the surveillance;
   - The details of any potential collateral intrusion and why the intrusion is justified;
   - The details of any confidential information that is likely to be obtained as a consequence of the surveillance;
   - The level of authority required (or recommended where that is different) for the surveillance; and
   - A subsequent record of whether authority was given or refused, by whom and the time and date

Renewals

2. Applications for renewal should record the above information together with details of:-
   - Whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
   - Any significant changes to the information previously provided;
   - The reason why it is necessary to continue with the directed surveillance;
   - The content and value to the investigation or operation of the information so far obtained by the surveillance;
   - The result of regular reviews of the investigation or operation.

Covert Human Intelligence Source Records

3. The following information is included in records relating to each covert human intelligence source:-
   (a) the identify of the source;
   (b) the identify, where known, used by the source;
   (c) any relevant investigating authority other than the authority maintaining the records;
   (d) the means by which the source is referred to within each relevant investigating authority;
   (e) any other significant information connected with the security and welfare of the source;
   (f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

(g) the date when, and the circumstances, in which the source was recruited;
(h) the identities of all persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) or in any order made by the Secretary of Sate;
(i) the periods during which those persons have discharged those responsibilities;
(j) the tasks given to the source and the demands made of him in relation to his activities as a source;
(k) all contacts or communication between the source and a person acting on behalf of any relevant investigating authority;
(l) the information obtained by each relevant investigatory authority by the conduct or use of the source;
(m) any dissemination by that authority of information obtained in that way; and
(n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

Covert Human Intelligence Source Applications

4. Applications for authorisation for the use or conduct of a source should be in writing and record the information laid down within the relevant code of practice. Applications for renewal of covert human intelligence sources should record:-
   - whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
   - any significant changes to the information previously provided;
   - the reasons why it is necessary to continue the use of the source;
   - the use made of the source in the period since the grant, or, as the case may be, latest renewal of the authorisation;
   - the tasks give to the source during that period and the information obtained from the conduct or use of the source;
   - the result of regular reviews of the use of the source

Duration and Cancellation of Authorisations

5. For Direct surveillance the written authorisation will cease to have effect (unless renewed) at the end of a period of three months beginning with the day on which it took effect, being the date on which it was approved by the Magistrates Court.

6. In a case in which the authorisation is for the conduct of a covert human intelligence source, the authorisation shall cease to have effect after the period of 12 months beginning with the day on which the grant takes effect, being the date on which it was approved by the Magistrates Court.

7. A person shall not renew an authorisation for a covert human intelligence source unless a review has been carried out as to the use made of the source, and tasks given during that period, and considered the same. Any such renewal takes effect subject to approval by the Magistrates Court.

8. Authorisations should be cancelled if the criteria for the authorisation is no longer met. A separate authorisation is required for each investigation.

9. Reviews should be undertaken following any significant occurrence and the results of a review should be recorded on the central register of authorisations.

Magistrates Court

10. No authorisation or renewal relating to Directed Surveillance or CHIS can be acted upon unless approval is given by the Magistrates Court. An application for such approval will be made by a representative of Legal Services accompanied by the Authorising Officer and the applicant.

APPENDIX 2

Standard forms to be used in connection with applications to authorise surveillance under the Regulation of Investigatory Powers Act 2000

The standard forms are also published on the Intranet.

1	Form RIPA 1	Authorisation Directed Surveillance
2	Form RIPA 2	Renewal of a Directed Surveillance authorisation
3	Form RIPA 3	Review of a Directed Surveillance authorisation
5	Form RIPA 4	Cancellation of a Directed Surveillance authorisation
6	Form RIPA 5	Application for authorisation of the conduct or use of a Covert Human Intelligence Source (CHIS)
7	Form RIPA 6	Application for renewal of a Covert Human Intelligence Source (CHIS) Authorisation
8	Form RIPA 7	Review of a Covert Human Intelligence Source (CHIS) Authorisation
9	Form RIPA 8	Cancellation of authorisation for the use or conduct of a Covert Human Intelligence Source (CHIS)

South Lakeland District Council
CCTV Policy

Document Control	
Organisation	South Lakeland District Council
Title	CCTV Policy
Author	Paul Mountford
Filename	CCTV Policy.docx
Owner	Principal Performance & Intelligence Officer
Subject	CCTV Policy
Protective marking	NOT PROTECTED
Review date	May 2019

Revision History			
Revision Date	**Revised By:**	**Previous Version**	**Description**

Document Approval		
Approval	**Name**	**Date**
Senior Information Risk Officer (SIRO)	Debbie Storr	
Deputy Senior Information Risk Officer (DSIRO)	Simon McVey	
Solicitor to the Council	Anthea Lowe	
Community & Leisure Manager	Jim Maguire	
Corporate Asset Manager	Sion Thomas	
Public Protection Manager	Fiona Inston	
Shared ICT Service Manager	Ben Wright	
HR Services Manager	Kerry Wallace	
Lake & Parking Services Officer	Frankie Flannigan	
Senior Communications Officer	Richard Machin	

KEY MESSAGES

- guidelines on the Council's use of CCTV
- protect the organisation from allegations of misuse of the system
- protect staff and the public from any abuse of the CCTV system

1, Statement

South Lakeland District Council uses Closed Circuit Television (CCTV) systems in public spaces, within car parks and at a number of the organisation's owned sites. The Council has installed a number of separate systems on a number of its operational vehicles. The Council's Civil Enforcement (Parking) Officers operate body worn video recording devices.

2, Purpose

The purpose of this policy is designed to give clear guidelines on the Council's use of CCTV and to protect the organisation from allegations of misuse of the system and to protect staff and the public from any abuse of the CCTV system.

3, Scope

This policy covers the use of CCTV equipment and the gathering, storage, use and disposal of visual data. This policy applies to all staff employed by the Council and should be the standard expected from any external agencies or persons who operate CCTV systems on its behalf.

4, Definition

The Council has installed a comprehensive public realm CCTV surveillance system which covers key Council assets in Bowness-on-Windermere, Kendal, Troutbeck and Ulverston. In addition, the Council has installed a number of separate systems at key Council premises, on a number of its operational vehicles and operates a body worn video system in the operation of its Civil Enforcement duty. The Council also supports Cumbria Constabulary's county wide CCTV scheme. The following CCTV systems are in use by the Council:

Ferry Nab, Bowness-on-Windermere CCTV System - this system provides external CCTV coverage of the Council's operations. Live images are visible to staff on site; recorded images are accessible to duly authorised officers in accordance with this policy.

Kendal Town Hall CCTV System - this system provides internal CCTV coverage within Kendal Town Hall. Live images are visible to staff on site; recorded images are accessible to duly authorised officers in accordance with this policy.

South Lakeland House CCTV System - this system provides internal CCTV coverage within South Lakeland House. Live images are visible to staff on site; recorded images are accessible to duly authorised officers in accordance with this policy.

Westmorland Shopping Centre Car Park, Kendal CCTV System - this system provides internal and external CCTV coverage of Westmorland Shopping Centre Car Park. Live images are visible to staff on site; recorded images are accessible to duly authorised officers in accordance with this policy.

North Lonsdale Road Depot, Ulverston CCTV System - this system provides external CCTV coverage of the Council's operations depot. Live images are visible to staff on site; recorded images are accessible to duly authorised officers in accordance with this policy.

Ecclerigg Depot, Troutbeck CCTV System - this system provides external CCTV coverage of the Council's operations depot. Live images are visible to staff on site; recorded images are accessible to duly authorised officers in accordance with this policy.

Town View Fields Hostel, Kendal CCTV System - this system provides internal and external CCTV coverage of the Council's emergency homeless hostel. Live images are visible to staff on site; recorded images are accessible to duly authorised officers in accordance with this policy.

South Lakeland House Car Park, Kendal CCTV System - this system provides internal and external CCTV coverage of South Lakeland House Car Park. Live images are visible to staff on site; recorded images are accessible to duly authorised officers in accordance with this policy.

Operational Vehicle CCTV System - the Council has fitted a number of its operational vehicles with CCTV cameras. Live images are visible within the vehicle; recorded images are accessible to duly authorised officers in accordance with this policy.

Body Worn Portable CCTV System - the Council's Civil Enforcement (Parking) Officers operate body worn video recording devices. Recorded images are accessible to duly authorised officers in accordance with this policy.

5, Risks

It is important that everyone and especially those charged with operating the CCTV systems on behalf of the Council understand exactly why each of the systems has been introduced and what the cameras will and will not be used for.

The primary objectives of the Council's CCTV systems are to provide a safe environment for the benefit of those who live, work, trade, visit, service and enjoy local facilities. Their collective purpose is to:

- Reduce the fear of crime and provide reassurance to the public through provision of a CCTV System.
- Assist in the detection and prevention of crime, anti-social behaviour and the maintenance of public order.
- Facilitate the apprehension and prosecution of offenders in relation to crime, public order and anti-social behaviour.
- To collect and provide evidence for the purpose of criminal and civil litigation by the police or other bodies with a responsibility for enforcing law, licensing regimes and other regulatory functions.
- To protect Council assets, resources, staff, land and other public facilities and ensure reasonable, justified and proportionate compliance with Council Policy and Procedure.
- To assist in improving the environment of the area.
- To provide assistance to emergency services.
- To assisting in staff disciplinary, grievance, formal complaints and Health and Safety Investigations.

Individuals will only be monitored if there is reasonable cause to suspect that a criminal offence or serious breach of discipline (potentially amounting to misconduct) has been, or may be about to be committed. This will only be permitted when authorised and may require the use of a RIPA authorisation. Duly authorised officers must consult the Senior Information Risk Officer (SIRO), Solicitor to the Council, Human Resources Manager and Data Protection Officer before any such action is taken.

In any event, a comprehensive incident log will be recorded giving a reason for the monitoring of the individual. All duly authorised officers must be able to justify their actions at all times.

6, Applying the Policy

In addition to Council policies, procedures, guidelines and Codes of Practice, CCTV and its operation are subject to legislation under:

- The Data Protection Act 2018 (DPA).
- The EU General Data Protection Regulation (2016/679) (GDPR).
- The Human Rights Act 1998 (HRA).
- The Freedom of Information Act 2000 (FOIA).
- The Regulation of Investigatory Powers Act 2000 (RIPA).
- The Protection of Freedoms Act 2012.

It is important that the operation of all the Council run CCTV systems comply with these Acts, policies, procedures, guidelines and Codes of Practice. This is to ensure that staff running the CCTV systems, the public and the Council itself are protected from abuses of the CCTV systems. Authorised officer's will be responsible for reviewing all CCTV documentation relating to their system annually (or as changes occur) and ensuring the information in those documents is up to date**.** The Council's Data Protection Officer will assist in this process.

The Council also takes proper regard to the Surveillance Camera Code of Practice 2013 issued by the Secretary of State and will work to develop the good practice advice set out in *'In the picture: A data protection code of practice for surveillance cameras and personal information'* published by the Information Commissioner's Office in May 2015.

Where any doubt exists about the lawful and proper use of any of the Council's CCTV Systems, the data they capture or data gathered by way of any monitoring contract, legal advice or advice from the Surveillance Commissioner's Office will be sought.

6.1, Privacy

The CCTV systems are included as part of the Council's Data Protection Registration with the Information Commissioners Office (ICO) in accordance with all data protection requirements. Every consideration will be given to the right of the general public to go about their daily business with minimum loss of privacy. Whilst total privacy cannot be guaranteed within a CCTV area, the cameras and their recordings will not be used to unduly monitor persons going about their lawful business.

It is a requirement under the Information Commissioners Code of Practice and the National CCTV Strategy that any equipment purchased is fit for purpose and will meet the objectives set down for the scheme. There is also a clear requirement for all CCTV schemes to have an effective maintenance schedule and Code of Practice. Officer's purchasing new CCTV equipment need to ensure these requirements are met.

Audio recording should only be used where the Council:

- has identified a need or issue which can be characterised as a pressing social need and can evidence that this need must be addressed
- has considered other less privacy intrusive methods of addressing the need; and
- having reviewed the other less privacy intrusive methods, the Council has concluded that these will not appropriately address the identified issue and the only way to address the issue is through the use of audio recording.

If a decision is made to use audio recording, the Council will make it clear that audio recording is taking place, over and above any visual recording which is already occurring.

Prior to any decision to use audio recording, a Data Protection (Privacy) Impact Assessment must be undertaken to inform the decision making process. The Data Protection Officer will support the Lead Authorised Officer in this process.

6.2, Code of Practice

The casual viewing or trawling of images is strictly forbidden. Viewings must only be undertaken for a specific legitimate purpose.

In accordance with the Surveillance Camera Code of Practice (2013), the following 12 guiding principles have been adopted within the Council CCTV system. They are:

- Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
- The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
- There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
- Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
- No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
-

- Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
- Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
- There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
- When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
- Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

6.3, Signage

All areas where CCTV is in use should be clearly signed to comply with the Data Protection Act 2018. This is to warn people that they are about to enter an area covered by CCTV cameras or to remind them that they are still in an area covered by CCTV. The signs will also act as an additional deterrent. CCTV signs should not be displayed in areas, which do not have CCTV cameras.

Where covert cameras have been authorised for deployment, signage will not normally be erected. The sign should carry the CCTV camera and SLDC Logo. The information on the sign should explain why the CCTV cameras are there, who runs them and a contact number. The signs, position and the message needs to be big enough to enable people to easily read the information on it.

6.4, CCTV Ownership

South Lakeland District Council is the data controller. The Lead Officer and other Officers duly authorised are defined by the Policy (see paragraph 6.9) to review recorded images captured by the relevant CCTV systems. The duly appointed officers are supported by the Council's Data Protection Officer.

6.5, Control and Operation of CCTV Systems

Only staff with responsibility for using CCTV equipment shall access the systems operating controls (other than those under supervised training). All use of cameras and control equipment shall be in accordance with the purposes and primary objectives of this policy.

6.6, Recorded material and still images

All recorded material produced from the Council's CCTV systems remain the property of the Council and are protected by copyright. Recorded material is held for a maximum of 30 days unless retained for evidential or training purposes. Recorded material shall only be used for the purposes defined in the Policy. Access to recorded material will only take place as defined in this Policy, and by duly authorised officers.

The release of recorded material to the public will only be allowed in accordance with the law. Recorded material will only be used in accordance with the primary objectives as set out in this Policy and in accordance with the Data Protection Act 2018 and EU General Data Protection Regulation (2016/679) (GDPR).

In accordance with Schedule 2 Part 1 of the Data Protection Act 2018 Enforcement Agencies may apply for access where the agency reasonably believe that access to specific recordings is necessary for the proper investigation and detection of a particular offence or offences or for the prevention of crime and disorder.

In accordance with Schedule 2 Part 1 of the Data Protection Act 2018 agencies and organisations may apply where access is necessary for the purpose of, or in connection with, legal proceedings, is necessary for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

No other access to data will be allowed unless approved by a duly authorised officer
Still images should not be taken as a matter of routine. The taking of each still image must be for justifiable reasons.

All still images will remain the property of the Council. A record will be kept of the reason for production of the photograph, date and time, the particulars of production, and information identifying those responsible for producing the photograph.

At no time should a still image be used for anything other than the purpose specified and identified when released to Enforcement or other agencies or organisations. Still images may be sent electronically via secure email to named officers.

6.7, Enforcement agency contact and the use of the Council's CCTV Systems

Enforcement agencies such as the police have a legal requirement to seize any relevant evidence when investigating a crime and the Council has a duty to comply with their request. But the enforcement agencies are bound by the same rules as everyone else.

Enforcement agencies are not permitted to trawl the CCTV system on the off chance of detecting a crime or wrong doing. They are required to provide the duly appointed Officer with a Crime or Incident number of other such proof that they are conducting a legitimate investigation.

The release of evidence or permission to view images may only be authorised by the duly appointed Officer or in their absence, the Data Protection Officer or Departmental Director**.** Where an enforcement agency requests copies of an image, one copy is to be made but there is no requirement for the duly appointed Officer to retain or produce any further copies.

The control of cameras and their monitoring is, unless covered by RIPA or other authorisation, the responsibility of duly authorised staff only. Enforcement Agencies may request assistance in order to:

- Assist with the deployment of resources.
- Monitor potential public disorder or other major security situations.
- Assist in the detection of crime.
- Facilitate the apprehension and prosecution of offenders in relation to crime and public order.
- Assist with the detection of moving traffic offences where it is considered that the public safety is at risk.

6.8, Civil Contingencies

Use of the Council's CCTV Systems are integrated into the Council's Emergency Planning Procedures for major civil emergencies.

6.9, Duly Appointed Officers

The Lead Duly Authorised Officer for each system is set out below and is the Information Asset Owner. Duly Authorised Officers within each function are also identified.

In addition to staff viewing live images, duly authorised officers with reasonable, justified and proportionate grounds can view recorded images in order to undertake audit checks, system checks and checks to ensure compliance with Council Policy and Procedure.

Prior to any decision to procure additional cameras or new CCTV systems, a Data Protection (Privacy) Impact Assessment must be undertaken to inform the decision making process.

CCTV System	Lead Duly Authorised Officer (Information Asset Owner)	Duly Authorised Officer(s)
Ferry Nab, Bowness-on-Windermere	Community and Leisure Manager	Lake and Parking Services Officer Lake Warden(s)
Kendal Town Hall	Corporate Asset Manager	Facility Manager Halls Officer (Kendal)
South Lakeland House, Kendal	Corporate Asset Manager	Facility Manager Senior Communications Officer Contact Centre Team Leader
Westmorland Shopping Centre Car Park, Kendal	Community and Leisure Manager	Lake and Parking Services Officer Parking and Cash Collector Supervisor Parking Assistant (Westmorland Shopping Centre)
North Lonsdale Road Depot, Ulverston	Community and Leisure Manager	Principal Street Scene Officer Street Scene Team Leader (North Lonsdale Road)
Ecclerigg Depot, Troutbeck	Community and Leisure Manager	Principal Street Scene Officer Street Scene Team Leader (Ecclerigg)
Town View Fields Hostel, Kendal	Public Protection Manager	Hostel Team Leader Housing Options Manager Hostel Support Officer(s)
South Lakeland House Car Park, Kendal	Community and Leisure Manager	Lake and Parking Services Officer Parking and Cash Collector Supervisor Parking Assistant (Westmorland Shopping Centre)
Operational Vehicles	Community and Leisure Manager	Principal Street Scene Officer Street Scene Team Leader(s) Street Scene Operative(s)
Body Worn Portable Devices	Community and Leisure Manager	Lake and Parking Services Officer Parking and Cash Collector Supervisor Civil Enforcement Officer(s)

7, Policy Compliance

Tampering with or misuse of cameras, monitoring or recording equipment, images or recorded data by staff may be regarded as misconduct and could lead to disciplinary action, which may result in dismissal or criminal prosecution.

Any Council Officer found to have breached this policy may be subject to South Lakeland District Council disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If Council Officers do not understand the implications of this policy or how it may apply to them they can seek advice from the Council's Data Protection Officer.

8, Policy Governance

The following table identifies who within South Lakeland District Council is Accountable, Responsible, Informed or Consulted with regards to this policy.

The following definitions apply:

Responsible - the person(s) responsible for developing and implementing the policy.
Accountable - the person who has ultimate accountability and authority for the policy.
Consulted - the person(s) or groups to be consulted prior to final policy implementation or amendment.
Informed - the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Data Protection Officer
Accountable	SIRO
Consulted	Senior Management Team (SMT), Shared ICT Services, Human Resources, Solicitor to the Council, Asset Management, Community and Leisure, Public Protection
Informed	All Council Employees, All Temporary Staff, All Contractors

9, References

The following South Lakeland District Council documents are directly relevant to this policy, and are referenced within this document:

Framework Structure			
Information Governance Framework			
	CCTV Policy		✓
		SLDC CCTV System - Operational Protocol	