Lancashire County Council

Scrutiny Committee

Friday, 11th December, 2015 at 10.00 am in Cabinet Room 'B' - The Diamond Jubilee Room, County Hall, Preston

Agenda

Part I (Open to Press and Public)

No. Item

1. Apologies

2. Disclosure of Pecuniary and Non-Pecuniary Interests

Members are asked to consider any Pecuniary and Non-Pecuniary Interests they may have to disclose to the meeting in relation to matters under consideration on the Agenda.

3. Minutes of the Meeting held on 13 November 2015 (Pages 1 - 10)

4. Regulation of Investigatory Powers Act 2000 Report (Pages 11 - 48)

5. Superfast Broadband Roll Out (Pages 49 - 50)

A presentation will be delivered by Sean McGrath (External Investment and Funding) to update the Committee regarding Superfast Broadband Roll Out.

6. Request for Sub-Committee of the TAMP Task Group (Pages 51 - 52)

7. Workplan and Task Group Update (Pages 53 - 56)

8. Urgent Business

An item of urgent business may only be considered under this heading where, by reason of special circumstances to be recorded in the Minutes, the Chair of the meeting is of the opinion that the item should be considered at the meeting as a matter of urgency. Wherever possible, the Chief Executive should be given advance warning of any Member's intention to raise a matter under this heading.

Lancashire County Council

9. Date of Next Meeting

The next meeting of the Scrutiny Committee will be held on Friday 15 January 2016 at 10:00am at the County Hall, Preston in Cabinet Room 'B'.

I Young
Director of Governance,
Finance and Public Services

County Hall
Preston

Lancashire County Council

Scrutiny Committee

Minutes of the Meeting held on Friday, 13th November, 2015 at 10.00am in Cabinet Room 'B' - The Diamond Jubilee Room, County Hall, Preston

Present:

County Councillor Bill Winlow (Chair)

County Councillors

D Clifford	M Parkinson
C Crompton	J Shedwick
C Henig	V Taylor
Mrs L Oades	C Wakeford
D O'Toole	G Wilkins

County Councillor Alyson Barnes was replaced by County Councillor Darren Clifford and County Councillor Richard Newman-Thompson was replaced by County Councillor Chris Henig for this meeting.

1. Apologies

Apologies were received from County Councillor David Watts

2. Disclosure of Pecuniary and Non-Pecuniary Interests

None were disclosed.

3. Minutes of the Meeting held on 16 October 2015

The minutes of the meeting held on 16 October 2015 were agreed to be an accurate record.

4. Report of the Fire Suppression Measures Task Group

The Chair introduced Jason Homan, Assistant Director of Property (Building Design & Construction) to the meeting who delivered the Task Group's report.

It was explained that the Task Group was convened following a request from the Cabinet Member for Children and Young People to consider the installation of further fire suppression measures in all new schools in Lancashire. It was elucidated that the Task Group used a report to the All-Parliamentary Discussion Group presented in 2013, and that this report had been provided as an appendix.

The issues analysed by the Task Group were outlined to be; financial aspects, community impacts, technical issues and the thoughts of the Fire and Rescue

Service. The aforementioned were considered in the formulation of recommendations.

Jason Homan stated that Government developed a risk assessment tool for fire safety within schools, and the County Council had built upon this by incorporating further assessments to analyse specific issues within Lancashire.

It was emphasised to the Committee that fire suppression focussed upon mitigating psychological impacts of fires within schools, rather than specifically saving lives as other measures sought to ensure pupil safety.

The Committee were informed that the Task Group had given consideration to existing schools within the county as the proportion of new schools to be built was anticipated to be low in number in the coming years, with schools more likely to have building extensions within their existing grounds. Therefore, the Task Group suggested that particular criteria be developed to determine thresholds for size expansions that triggered the requirement to install sprinkler systems.

Regarding schools within Lancashire that the county council did not control, it was stressed to be of importance that measures the county council considered appropriate for their own schools should be encouraged in schools not under the county council's control.

Members noted that the Task Group analysed alternative forms of fire suppression, for example misting systems. It was explained that fire safety was determined by various factors, for example; the layout of a school, direct access to outside from classrooms, the fire properties of building materials, limiting roof voids and the space above ceilings. Therefore, it was conveyed that the installation of a sprinkler system was not the only measure that could be implemented to suppress fire.

The Task Group, it was conveyed, also considered schools that currently had sprinkler systems installed and, specifically, the extent the systems were examined, inspected and maintained as there had been issues with sprinkler systems deploying, however it was highlighted this was due to poor maintenance rather that system failure. Furthermore, the issue of unanticipated sprinkler system triggering was discussed with the Task Group, and it was explained that sprinklers only triggered in the area of a fire/heat source which was contrary to common misconceptions.
Discussions within the Task Group had taken place around who was responsible for sprinkler systems, e.g. with the county council or with individual schools.

Finally, in the instances that it was not felt appropriate for sprinkler systems to be installed, discussions taken place regarding mitigating fire damage and therefore prevent psychological impacts.

Jason Homan elucidated that as a result of the discussions outlined above, the following five recommendations had been formulated;

1) All brand new schools developed by LCC shall have a sprinkler system installed as part of their fire safety strategy. With regard to the extension of an existing school, where the capacity of a school is to increase by 50% or more, based on pupil numbers, then a sprinkler system shall be installed into the resultant new facility (both the new and existing elements).

   Once installed the responsibility to correctly inspect, service and maintain the sprinkler system shall rest with the governing body of that school.

2) All schools that currently have a fire suppression system installed shall have an initial assessment carried out by LCC to establish the condition of the system. Any remedial work required to ensure the correct operation of the system shall be carried out by the individual school within 6 months of them being notified of these requirements.
   Upon completion of the initial assessments and resultant remedial works where necessary, the responsibility for the future inspection, servicing and maintenance of the system shall rest with the governing body of that school.

3) 4. All schools under the control of LCC and which do not have a fire suppression system installed shall seek to provide a fire retardant storage facility suitable for their needs as assessed by themselves.

4) All other organisations that are responsible for the provision of school premises within Lancashire shall be encouraged to adopt the same recommendations as will apply to those schools under the direct control of LCC.

5) In order to ensure this policy remains consistent with future changes in building legislation it is to be reviewed every 5 years.

Members were invited to ask questions and to raise any comments in relation to the report, a summary of which is provided below:

The Committee sought clarification on recommendation 4, stating that the lexical choice suggested there was a storage facility for fire retardant materials. It was clarified that the recommendation was for schools to create a fire retardant space within a school and consequently, it was agreed that the lexis would be changed to aid understanding.

CC G Wilkins expressed surprise at the emphasis upon mitigating the impact on pupil's work rather than lives. It was explained that many schools had direct access to outside from classrooms and were therefore safe, and that many fires occurred at night.

CC G Wilkins requested that, as many County Councillors were school governors, the report be distributed to all Members.

It was agreed that the report would be sent to all Members following the remainder of the Task Group process and following amendments to the recommendations as requested above.

CC C Henig noted that within the Task Group report reference was made to painted sprinklers, and that it was the school's responsibility to maintain sprinkler systems. Jason Homan explained that the policy did not differ from other systems within a school building, and therefore it did not add any new responsibility and that painted sprinklers should be picked up via the annual inspections. It was emphasised that it had been incorporated in the recommendation to state clearly who held the responsibility.

CC Chris Henig enquired whether the installation of a sprinkler system impacted insurance costs for a school. Jason Homan stated that the installation of sprinkler systems in a small number of schools would not significantly impact on insurance costs as the county council were insured for the entire portfolio of its schools as one entity. However, for schools In Lancashire that were outside of the county council's remit who insured themselves, this would have an impact on their insurance costs, and therefore would be attractive to them.

CC C Henig expressed that there was possibly scope for savings for schools insuring themselves individually. The Chair expressed that discussions around this could take place at a later date.

CC V Taylor queried whether sprinkler systems that were painted over would impact insurance claims. Jason Homan explained that the recommendations sought to address this issue. It was noted that, going forward, it was going to be a more prominent issue that they are maintained and inspected correctly.

CC V Taylor expressed concern that it may take time to determine the condition of sprinkler systems. Therefore, it was suggested that the county council contact Head Teachers and/or governing bodies of schools to seek assurance that their sprinkler systems were fully operational.

Jason Homan explained that the county council sought assurance via the annual statement of compliance, which referred to whether the systems within a school were fully functioning.

The Chair requested that schools be contacted requiring that sprinkler systems are checked.

CC J Shedwick asked who replaced faulty sprinkler heads within schools. Jason Homan explained that the school would remedy issues via the arrangements they had in place, which were either through the county council's property services or external contractors.

CC L Oades expressed that when she was a chair of governors at a school she had been informed it would be prohibitive for the county council to insure each

individual school, rather than the current arrangement of generic insurance for all schools it was responsible for. Therefore, caution was urged with this approach.

The Chair stated that clarity was required regarding insurance for schools and a report could be required to be presented to the Committee. Jason Homan explained that he would speak to insurance officers to take the request forward.

CC Carl Crompton explained that most schools had a health and safety committee who inspected fire suppression measures, and therefore it was an automatic responsibility for the school to report any issues.

CC G Wilkins asked what the thoughts of Lancashire Fire and Rescue Service were regarding a sprinkler system and also the thoughts of Head Teachers. Jason Homan explained that the thoughts of Lancashire Fire and Rescue Service were that all school buildings should have sprinkler systems installed and that this position was consistent nationwide. Regarding Head Teachers, it was explained that when fire risk assessments resulted in suggestions for the installation of a sprinkler system Head Teachers did not have an issue.

CC D O'Toole stated that if any of the recommendations were implemented it should be done in collaboration with Lancashire Fire and Rescue Service. It was explained that their knowledge could help to reduce the cost of sprinkler system installations, as premium sprinkler systems may not be necessary.

Resolved;

i. That the Committee accept the Task Group's recommendations following the suggested amendments outlined above.

ii. That schools be contacted requiring that sprinkler systems are checked.

5. Lancashire Safeguarding Children Board Update

The Chair introduced Jane Booth (Independent Chair Lancashire Safeguarding Children Board), Paul Hegarty (Business Manager of Lancashire Safeguarding Children and Adult Board) and Louise Taylor (Corporate Director, Operations and Delivery) to the meeting who delivered the Lancashire Safeguarding Children Board (LCSB) report.

The Committee were informed that LSCB considered the county council to be a key player in safeguarding children and therefore, the report was before the Committee. It was noted that a shorter more accessible version of the report would be available on the LSCB website in the near future.

Members were informed that, following their audit and inspection, the LSCB had identified some areas of concern regarding the experiences of some children and young people and that these had been presented on page 4 of the report.

Jane Booth noted that, despite some concerns, there were many positives. For example, a significant increase in early-help activity. It was elucidated that the increase was mirrored by a decrease in children on child protection plans and therefore there may be a connection between the two, although the connection would not be confirmed without further analysis. It was explained to the Committee that there had not been a similar impact upon the number of looked-after children and the referrals received, however with the increase in early-help activity there could be movement on this position going forward.

It was explained that a supplementary document would be produced over the coming months which focussed upon data-analysis and that this would be shared with the Scrutiny Committee.

It was conveyed that the childcare structure was particularly complex in Lancashire due to a large number of Clinical Commissioning Groups, 12 District Councils, a number of health care providers, a mixed picture of poverty/deprivation and a large cohort of schools.

The Committee were informed that LSCB reviewed all child deaths and, through their work, there had been issues identified that required work with agencies.

Members noted that LSCB had completed two inspections, one around early-help and one locality inspection in Burnley, along with a number of individual case audits. It was also conveyed that LSCB had improved data collection and consequently performance analysis across agencies, and work was ongoing to increase capacity.

Jane Booth highlighted that a decision had been made to align the business units that supported the LSCB and Lancashire Safeguarding Adults Board (LSAB) as many issues span across the age bands, and through aligning business, the service could be more effective.

Members were invited to ask questions and to raise any comments in relation to the report, a summary of which is provided below:

CC D O'Toole queried the differentiation in funding to LSCB from local authorities, for example Blackpool Council. Jane Booth explained that there were separate LSCB's for each of Lancashire, Blackburn with Darwen and Blackpool. Some core functions such as the development of policies and procedures were shared and a joint Child Death Overview Panel was in place to which the other LSCB's made financial a contribution. It was noted that there was not a national formula to determine the level of contributions by agencies. In addition, Jane Booth noted that LSCB had approached Health Trusts for contributions, with one positive response and efforts were continuing.

The Chair queried if a funding formula could be developed for Lancashire and whether the Committee could formulate any recommendation to aid the LSCB. It was explained that with the alignment of the LSCB and LSAB it would be difficult

to organise until the financial implications were understood. However, Members were reassured that agencies were prepared to increase contributions based on any increase in budget following the changes. Jane Booth also expressed that a review commissioned by the LGA who performed a recent quality assurance exercise had recommended in a report that Government should take on-board issues about resource in general and the National Serious Case Review Panel had also recommended that the government address the funding of the production of serious case reviews.

CC G Wilkins queried the impacts of immigration for LSCB. Jane Booth explained that there had not been identification of specific issues with abuse with particular communities. However, for example, some migrants may possess different opinions around the Police service due to fears from another culture and could therefore refrain from reporting concerns or seeking help.

CC G Wilkins queried if it was anticipated that LSCB's 15/16 report would differ from the 14/15 report. Jane Booth expressed that she anticipated it would be significantly different as financial and other resource pressures were being felt by all agencies and there was a risk that performance would deteriorate.

CC C Henig made reference to 'key areas for professionals to consider and challenge themselves' present within Appendix 'A' of the report and expressed that they should be innate for a social worker following their training. Jane Booth noted that she agreed that they were an integral part of a social worker's training. It was conveyed that the 'key areas' were outlined to avoid slippage via good supervision and challenge as some social workers had been seen to stray from the key areas in some instances. It was explained that the methodology for a serious case review had changed and practitioners were now brought together and asked questions as opposed to paper based reviews. Paul Hegarty elaborated stating that learning briefs were distributed to all professionals, and although very simple, it was noted that going back to basics allowed for a comprehensive picture to be devised.

CC C Henig queried how far investigative work into agencies could go regarding serious case reviews. Jane Booth expressed that LSCB needed to increase its capacity to audit in order to perform more investigative work as this aided understanding of where issues lay.

CC L Oades noted that often Fylde and Wyre were associated with Blackpool Council despite being in Lancashire. Jane Booth outlined that this was also an issue with districts bordering Blackburn with Darwen Council and discussions were taking place around information sharing. It was highlighted that issues arisen as, for example, residents of Fylde and Wyre often used Blackpool based hospitals and therefore crossed the boundaries.

CC L Oades expressed concern that there were an increasing number of children from other authorities coming into Lancashire and asked if there was a recommendation the Committee could devise to help LSCB and consequently the county council from the point of view of funding. Jane Booth noted that Lancashire had a large number of such children whose responsibility lay outside of its boundaries and that they utilised Lancashire's services such as schools and

health services, however Lancashire agencies were not responsible for the child's care plan. It was emphasised to be a complex picture with work ongoing to address the issue. For example, LSCB were currently performing an audit around children placed in Lancashire by other authorities, and once completed, an audit of Lancashire children placed elsewhere in the country would be undertaken.

Louise Taylor explained that the county council tried hard to avoid placing children outside of the county boundaries, however in some instances, this did occur. This, it was outlined, occurred when it was felt a child was at genuine risk of harm remaining in the county, when there was a specific and complex needs that independent providers could not cater for within the county, when educational needs could not be met in the county and various other reasons. It was noted that Bob Stott, Director of Children's Services, reported the numbers of Lancashire children placed outside of the county boundaries to LSCB.

CC L Oades stated that Government needed to look at the placement of children outside of a local authorities boundaries in some instances when it did not have good reason, with specific reference to some private children home providers utilising cheaper accommodation in Lancashire.

CC V Taylor asked for more information about concerns around 'achieving successful engagement by the LSCB with schools and early years settings' outlined on page 22 of the report. Jane Booth explained the complexities of engaging with schools to the Committee and noted that it was not a reluctance on the part of the schools but more a capacity issue for the LSCB.

CC C Henig made particular reference to an unsuccessful bid to obtain funds from the innovation fund and therefore it was queried if Lancaster University had been approached around research. Jane Booth explained that the LSCB was keen to progress the research and were prepared to utilise reserves to support it. It was highlighted that there was potential for funding from the Police & Crime Commissioner, and other funding streams.

CC C Crompton queried if other local authorities were surcharged if a child's care package exceeded outlined requirements by a local authority outside of Lancashire. Louise Taylor explained that a mechanism did not exist for local authorities to be recompensed if the above scenario occurred. It was noted that it created particular issues for health colleagues as they were not consulted prior to placements, and therefore inherited costs as a consequence.

The Chair thanked Jane Booth, Paul Hegarty and Louise Taylor for presenting the report and answering queries.

The Chair suggested that a letter be sent to Government regarding national funding for Children's Boards. The Committee agreed that this be penned.

Resolved:

i. That the Committee note the report.
ii. That the Committee write to Government regarding national funding for Children's Boards.

6. Transforming Care and Calderstones NHS Foundation Trust - Notice of Motion

The Chair explained that the letters provided had been shared with the Committee to give the opportunity to note the result of the Notice of Motion which was approved at Full Council.

Resolved; That the Committee notes the letters sent to Government and the CEO of NHS England.

7. Workplan and Task Group Update

Resolved; That the work plan and task group update be noted.

8. Urgent Business

The Chair introduced Wendy Broadley (Scrutiny Officer) who attended to request approval from the Committee for a Task Group to be convened to explore the shortage of nurses within the NHS system.

It was explained to the Committee that Health Scrutiny Committee liaised with Acute Trust providers in Lancashire and a common theme from discussions was a shortage of Doctors and Nurses, and therefore Trusts had a heavy reliance of agency staff and nurses from overseas. It was conveyed that members of Health Scrutiny Committee wanted a better understanding of the reason behind the shortages and therefore the Task Group request had been devised.

CC D Clifford stated that the Task Group should consider the work of Community Nurses when assessing nursing levels of Acute Trusts. Wendy Broadley explained that the Task Group would be endeavouring to receive as a wide a picture as possible around these issues. For example, Health Steering Group would be meeting with Chorley & South Ribble CCG around their workforce planning project and the information from this meeting would be fed into the Task Group to aid their work.

CC M Parkinson noted that nursing, previously, had been a vocation, however this had changed in recent times with the requirement for qualifications and therefore could be a contributing factor.

CC C Henig suggested that nurses could be consulted by the Task Group. Wendy Broadley stated that it would be useful to speak to nurses.

CC G Wilkins asked that the Task Group investigate if the NHS required non-EU nurses to fill quotas.

CC D O'Toole suggested that the Task Group investigate the level of training nurses received and attitudinal issues.

CC C Crompton stated that an issue was nurses seeking employment via agencies rather than direct employment and suggested that the Task Group analyse this. Wendy Broadley stated that this was an area the Task Group would be endeavouring to understand.

Resolved: That the Committee support the Task Group request.

9. Date of Next Meeting

The next meeting of the Scrutiny Committee will be held on Friday, 11 December, 2015, at 10:00am at the County Hall, Preston in Cabinet Room 'B'.

I Young
Director of Governance, Finance
and Public Services

County Hall
Preston

Scrutiny Committee: 11 December 2015

Report of the Director of Governance, Finance and Public Services

Electoral Division affected:
None

Regulation of Investigatory Powers Act 2000 Report
(Appendix 'A' refers)

Contact for further information:
Ian Young, 01772 533531, **Director of Governance, Finance and Public Services**,
Ian.young@lancashire.gov.uk

Executive Summary

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a framework for certain public bodies, including local authorities, to use "covert surveillance" to gather information about individuals without their knowledge for the purposes of undertaking statutory functions in connection with the prevention or detection of crime.

RIPA activity and authorisations are governed by Codes of Practice and Guidance issued by the Office for Surveillance Commissioners (OSC) and the Home Office.

Local authorities are also subject to regular inspections from the OSC.

Members are required to review the use of RIPA and set the policy at least once a year.

Recommendation

That the Scrutiny Committee note the use of RIPA referred to in the content of this report.

Background and Advice

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a framework for certain public bodies, including local authorities, to use "covert surveillance" to gather information about individuals without their knowledge for the purposes of undertaking statutory functions in connection with the prevention or detection of crime.

RIPA is permissive legislation, that is to say that it is not mandatory for a Local Authority to authorise covert surveillance under RIPA, but if it does so then RIPA provides the local authority with a defence if the individual brings a claim against the local authority alleging that the surveillance breaches their Human Rights, specifically Article 8, the right to respect for private and family life, home and correspondence.

The Regulation of Investigatory Powers Act covers directed surveillance, use of a Covert Human Intelligence Source (CHIS) and the acquisition, disclosure and retention of communications data.

Within the County Council, covert surveillance authorised pursuant to RIPA is used very infrequently and only in connection with Trading Standards activities, typically against rogue traders, counterfeiters or individuals engaged in selling tobacco or alcohol products to children. It is used in cases where it is important to obtain information to support potential criminal proceedings, and only where that information cannot be obtained by any other means.

RIPA activity and authorisations are governed by Codes of Practice and Guidance issued by the Office for Surveillance Commissioners (OSC) and the Home Office.

Local authorities are subject to regular inspections undertaken by OSC, the most recent Lancashire County Council inspection having taken place on 3 February 2014. The resulting report was considered in June 2014 by Cabinet following the inspection and a number of changes to procedure were subsequently adopted, including an update to the RIPA Corporate Policy; designation of the Head of Trading Standards and two Trading Standards Managers to authorise RIPA applications; and agreement to a response to the OSC in relation to the authorisation of directed surveillance of underage sales test purchasing activities.

In December 2014 some key changes were made to the Code of Practice for Covert Surveillance and Property Interference, and the Covert Human Intelligence Sources Code of Practice, the main revisions being:

- To take account of the requirement under the Protection of Freedoms Act that local authorities should seek approval for authorisations from a magistrate,
- To extend the length of time for which records must be kept in the central record to 5 years,
- To clarify the need for consideration of relevant authorisation for the use of third party individuals or organisations (for example private investigators and internet researchers)
- Making it clear that the need for authorisation for directed surveillance or CHIS should be considered prior to the use of the internet in investigations, and that such use should be both necessary and proportionate.
- To clarify the information required to be provided on a review of an authorisation.

Where necessary these revisions have been incorporated into the revised policy, attached at Appendix A.

Directed surveillance and CHIS activity 1 April 2014 – 26 November 2015

Directed surveillance is covert but not intrusive, (local authorities cannot be authorised to carry out intrusive surveillance) and is undertaken
a) for the purpose of a specific investigation/operation,
b) is likely to result in the obtaining **private information** about a person (whether or not one specifically identified for the purposes of the investigation or operation)
c) Otherwise than by way of an immediate response to events or circumstances and it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

A **CHIS (Covert Human Intelligence Source)** is a person who establishes or maintains a personal or other relationship with another person for the covert purpose of:
(a) Using such a relationship to obtain information or to provide access to information to another person, or
(b) Disclosing information obtained by the use of such a relationship or as a consequence of such a relationship.

There have been three authorisations for the use of a CHIS and no Directed Surveillance authorisations during this period. All applications under RIPA are authorised by one of the three officers in Trading Standards to whom this function has been delegated, and then approved at magistrate's court. In practice approval is now routinely carried out by a District Judge.

Authorisation 1: The case involved the investigation of the supply of counterfeit goods via social media in contravention of the Trade Marks Act 1994.

As the investigation was drawing to a close it came to our knowledge that another investigation was taking place in parallel with the LCC Trading Standards case, and the defendants were all successfully prosecuted by this third party, with goods seized by Lancashire being signed over for disposal.

The first defendant was sentenced to 8 weeks imprisonment, suspended for 12 months with 60 hours unpaid work. A curfew was imposed from 6pm to 7am for 12 weeks, the second defendant was sentenced to 8 weeks imprisonment, suspended for 12 months. A curfew was imposed from 6pm to 7am for 12 weeks. The third defendant was sentenced to a community order with supervision for 6 months.

Authorisation 2: The case involved investigations into the supply of counterfeit goods via social media in contravention of the Trade Marks Act 1994. The authorisation was given, approval received from the District Judge in Preston, and investigations are ongoing.

Authorisation 3: The case involved investigations into the supply of counterfeit goods via social media in contravention of the Trade Marks Act 1994. Authorisation and approval from the District Judge has only just been obtained so investigations are at a very early stage. A review is scheduled for mid-January 2016.

All of the above authorisations are in connection with investigations into contraventions of the **Trade Marks Act 1994.**

These are serious offences with a maximum penalty of 10 years imprisonment at crown court.

- Counterfeiting Costs Industry £9 Billion Per Annum in UK
- Treasury loses £1.7 Billion in revenue p.a.
- Directly responsible for 4100 job losses in UK and 17120 in EU p.a.
- 7-9% of all world trade is in counterfeits

It is in the public interest to pursue such cases, since counterfeit sales affect genuine retailers, deprive rights-holders of revenue, and deprive the economy of taxes. In some cases this can influence others to also begin selling such goods in contravention of the law and thus enter into criminality. Counterfeiting may also often be linked to organised crime.

Consultations

N/A

Implications:

This item has the following implications, as indicated:

Risk management

If local authorities undertake covert surveillance activities without having first gone through an appropriate RIPA authorisation process there is a risk that the Council may face Human Rights challenges.

List of Background Papers

None

Reason for inclusion in Part II, if appropriate

N/A

LANCASHIRE COUNTY COUNCIL

Corporate Policy and Guidance
On
The Regulation
Of Investigatory Powers Act 2000

Contents

7. Communications Data
7.1 Accessing Communications Data
7.2 What is Communications Data?
7.3 Who are Communication Service Providers?
7.4 What information can be obtained from Communications Service Providers?
7.5 How can this information be obtained
7.6 Contact with the Communications Industry
7.7 The Role of the Single Point of Contact (SPOC)
7.8 The Role of the Authorising Officer
7.9 The Application Process
7.10. Records and Errors
7.11 Further Relevant Documentation

8. Seeking JP approval for authorisations
9. Lancashire County Council Auditing of Authorisations and Records
10. Inspections by the Office of the Surveillance Commissioner and the Interception of Communications Commissioner
11. Complaints
12. Management Records

General Statement of Policy

This policy document relates to use by Lancashire County Council officers of directed surveillance, covert human intelligence sources and access to telecommunications information.

- **The County Council is committed to upholding human rights**

- **As a public body and responsible employer, the County Council wants to conform to the letter and spirit of the requirements of the Regulation of Investigatory Powers Act 2000 and associated regulations and draft codes of practice relating to the use of covert surveillance, the use of covert human intelligence sources, and interception**

- **County Council officers will only undertake surveillance work when it is both necessary and proportionate to the ends it seeks to achieve**

- **From 1 November 2012 local authorities have been required to obtain judicial approval prior to using covert techniques. Local authority authorisations and notices under RIPA are only be given effect once an order has been granted by a justice of the peace in England and Wales, a sheriff in Scotland and a district judge (magistrates' court) in Northern Ireland.**

- **Additionally, from this date local authority use of directed surveillance under RIPA will be limited to the investigation of crimes which attract a 6 month or more custodial sentence, with the exception of offences relating to the underage sale of alcohol and tobacco.**

Corporate Guidance

1.1 Foreword

1.1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) provides a framework for certain bodies (including local authorities) to undertake their duties aimed at preventing or detecting crime, which may interfere with a citizens normal human rights in respect of privacy by the use of 'covert surveillance', Covert Human Intelligence Sources (CHIS) i.e. undercover officers/informants and to obtain certain limited communications data.

1.1.2 The use of these techniques must be "necessary" and "proportionate" to the investigation i.e. simple, overt methods of gathering information are not available and the matter under investigation should not be trivial.

1.1.3 RIPA establishes detailed requirements in respect of the seniority, training awareness of Authorising Officers (referred to as 'Designated Officers' in the Act) and also the formal assessment and recording processes before undertaking any surveillance activity.

1.1.4 The Authorising Officer is required to be an officer at least at the following level within the authority:

- Director
- Head of Service
- Service Manager or equivalent

The Authorising Officers for the Council are the Head of the Trading Standards Service and Trading Standards Managers in Trading Standards authorised by the Director of Governance, Finance and Public Services.

1.1.5 This guidance addresses the detailed requirements of RIPA and its codes of practice in relation to:

- the covert surveillance of individuals,
- the use of covert human intelligence sources, including undercover Officers/agents/informants,
- the recording of telephone conversations
- for obtaining communications data.

This guidance provides a summary and overview of the legislation and codes of practice. DO NOT seek to rely on it alone. In the event of any doubt, any senior managers, or applicants, should refer to the relevant legislation or code and consult the Director of Governance, Finance and Public Services, the Director of Legal and Democratic Services or the Head of Trading Standards before any action is taken.

1.1.6 The Act and relevant Codes of Practice(as amended in December 2014) had effect from 1 October 2000 and impose requirements as regards authorisation,

procedures and records, which must be followed by Public Authorities undertaking investigations which fall within the scope of the Act

1.1.7 Appropriate staff should familiarise themselves with the guidance and procedures, the legislation and the Codes of Practice. If in any doubt advice and guidance should be sought from an appropriate officer before undertaking any enforcement activities which may fall within the scope of the Act.

1.1.8 Lancashire County Council is committed to carrying out its enforcement functions in an equitable, practical and consistent manner. We are committed to these aims and to maintaining a fair and safe environment. This guidance demonstrates our desire to carry out our criminal investigations in a fair and equitable manner that respects all human rights and contributing to this commitment.

1.1.9 Enforcement activities of the Council that fall within the remit of the RIPA are subject to monitoring and oversight by the Surveillance Commissioner and the Interception Commissioner.

1.1.10 Complaints made regarding activities of the Council, which are within the scope of RIPA, can be investigated by an independent tribunal.

1.1.11 The Council may be liable to claims alleging breaches of an individual's rights under the Human Rights Act 1998 if officers fail to follow the requirements of RIPA and Codes of Practice.

1.1.12 Failure to follow RIPA and Codes may also adversely affect the admissibility of any evidence obtained using methods covered by RIPA. The safety of members of the public supplying information to the Council may also be compromised where an authorisation is not in place.

1.1.13 When undertaking any covert investigation, officers should have regard to the health and safety of persons affected by the activity. This may include themselves, colleagues and members of the public and the person you are being asked to observe. A risk assessment of the investigation technique being proposed should be undertaken, having regard to Corporate Health and Safety Policy and any supplemental guidance issued.

1.1.14 The monitoring of Internet and e-mail use is regulated by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, made under RIPA.

1.2 Employee or Non-RIPA Surveillance

1.2.1 RIPA does not apply where surveillance is undertaken otherwise than for ‘the detection or prevention of crime’ for example as part of an internal investigation into possible employee misconduct where the investigation is not primarily aimed at detecting criminal offences. However, as such surveillance may infringe an individual's Human Rights in respect of privacy, then similarly to RIPA, the procedures of authorisation and assessment should be followed with the Authorising Officer using

RIPA criteria in considering the surveillance request. Assessment and Approval forms, similar to RIPA, must be used in considering surveillance activity.

1.2.2 Similarly, child custody/protection investigations requiring surveillance should follow the same principles and use the non-RIPA Assessment forms. Copies of appropriately complete forms should be kept with the investigation file and the original sent to the Central Register in Legal and Democratic Services, but these will not be logged on the corporate RIPA database.

1.3 CCTV Use

1.3.1 CCTV surveillance systems are not normally caught by the Act where signs or cameras are visible or members of the public are aware that such systems are in use. However there may be occasions when public authorities use CCTV systems for the purposes of a specific directed investigation or operation. In such cases, authorisation for directed surveillance may be necessary. A protocol has been produced to protect those officers responsible for such systems from being pressured into carrying out directed surveillance without an appropriate authorisation.

1.4 Lancashire County Council Auditing

1.4.1 For appropriate corporate reporting and auditing of activities to ensure awareness and ongoing compliance with RIPA policies. Contact: Director of Legal and Democratic Services

2 **Definitions**

2.1 Surveillance and Covert Human Intelligence Sources

The Regulation of Investigatory Powers Act 2000

Authorising Officer Means the person(s) designated under Sections 28 and 29 of the Act to grant authorisations for directed surveillance and the use and conduct of a Covert Human Intelligence Source, respectively. The Head of Trading Standards and Trading Standards Managers in Trading Standards are designated as authorising officers by the Director of Governance, Finance and Public Services.

Conduct of a Source Any action of that source falling within the terms of the Act or action incidental to it. (ie what they do)

Confidential Material Matters of legal privilege, confidential personal
Includes: information (eg medical records), confidential journalistic material

Controller Means the person or designated managerial officer responsible for overseeing the use of the source.

Covert Human Intelligence Sources Commonly known as Agents, Informants, Undercover Officers. (NB. See RIPA and the Codes of (CHIS) Practice for the definition)

Covert Surveillance Means surveillance carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is taking place.

Directed Surveillance - Surveillance is directed if it is covert but not intrusive and is undertaken:

a) for the purpose of a specific investigation/operation
b) is likely to result in the obtaining **private information** about a person (whether or not one specifically identified for the purposes of the investigation or operation)
c) Otherwise than by way of an immediate response to events or circumstances and it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

Handler An investigating officer having day to day responsibility for:

- dealing with the source on behalf of the authority
- directing the day to day activities of the source
- recording the information supplied by the source
- monitoring the security and welfare of the source.

Intrusive Surveillance Means Covert Surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle **and** involves the presence of any individual **on** the premises or **in** the vehicle or is carried out by means of a surveillance device.

Private Information In relation to a person or business, this includes any information relating to an individual's private, business or family life.

Senior Responsible Officer (Surveillance)
An officer responsible for the integrity of RIPA processes for the authority and compliance with Part II of the Act. The Senior Responsible Officer for Surveillance and CHIS is the Director of Governance, Finance and Public Services.
(Note: See Senior Responsible Officer for Communications Data)

Surveillance includes: - monitoring, observing or listening to persons, their movements, their conversations, or their activities or communications.

- recording anything monitored, observed or listened to in the course of surveillance.

- Surveillance by or with the assistance of a surveillance device (any apparatus designed or adapted for use in surveillance eg cameras and microphones.

2.2 Communications Data

Communications Service Provider (CSP)
These include telecommunications, Internet (including e-mail) and postal service providers.

Designated Person
This is the authorising officer for the purposes of obtaining communications data, currently the two Trading Standards Managers.

Senior responsible Officer (Communications Data)

An officer responsible for the integrity of RIPA processes in relation to the Acquisition of Communications data under the Act, currently the Head of Trading Standards.

Single Point of Contact (SPOC)

This is a nominated officer within a public authority who has completed a training course and is accredited by the Home Office to make enquiries with communication service providers. SPOC's will oversee the forwarding and receipt of notices and authorisations sent to and returned by CSPs.
(CSPs will not deal with enquires to obtain communications data from an officer who is not listed with them as being a nominated SPOC).

SPOCs: The SPOC role is carried out by the National Anti Fraud Network on behalf of Lancashire County Council, and access can be arranged by approaching the Head of Trading Standards.

3. Covert Surveillance Policy and Procedures

3.1 Introduction

3.1.1 Covert Surveillance means **surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.**

3.1.2 An authorisation provides lawful authority for a Public Authority to carry out covert surveillance.

3.1.3 Any /Service seeking to use covert surveillance techniques must seek authorisation from the Director of Governance, Finance and Public Services or nominated deputy using the appropriate forms.

3.1.4 Whenever surveillance takes place and is for the purpose of obtaining, or is likely to obtain private information about a person (whether or not they are the target of the operation) an authorisation should be obtained.

3.1.5 By obtaining an authorisation, the surveillance operation is carried out in accordance with the law and the safeguards that exist.

3.1.6 Prior to granting an authorisation the Authorising Officer must be satisfied that the proposed surveillance is **necessary** on specific grounds and is **proportionate** to what it seeks to achieve.

3.1.7 Careful consideration must also be given to any Community sensitivities that may be exacerbated by any individual surveillance operation.

3.1.8 Before applying for an authorisation, the Investigating Officer should consider whether or not the evidence sought could be obtained by alternative possibly non covert methods.

3.1.9 The Authorising Officer must also believe that the surveillance is proportionate to what it seeks to achieve and is not excessive.

Note for All Applications for Authorisations

Necessity
For interference with an individual's private, family or business life to be necessary, the action must be for the purpose of detecting crime or prevention of disorder, be necessary to secure best evidence and that less covert or intrusive action would not serve the appropriate purpose.

Proportionality

The test for proportionality goes far beyond selecting the least intrusive method of investigation. The activity to be observed must not be trivial and must warrant the surveillance to be instigated

The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair. Proportionality should contain a consideration of four elements

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

3.2 Collateral Intrusion

3.2.1 The officer seeking the authorisation should also consider the possibility of collateral intrusion (this is where interference with the privacy of others not subject to the original surveillance may occur). Steps should be taken to assess the risk and where possible reduce the risk of collateral intrusion. Where unforeseen collateral intrusion occurs during an operation, the Authorising Officer must be notified and consideration given to amending the authorisation following a review. A separate Lancashire County Council CCTV protocol exists which also refers to avoiding collateral intrusion.

3.2.2 Consideration must also be given as to whether or not the surveillance activities of the Service take place where similar activities are also being undertaken by another agency e.g. the Police, Benefits Agency, Environment Agency and liaison with other enforcement agencies should be considered where appropriate.

3.3 Records of Authorisations

3.3.1 A record of all authorisations must be maintained for five years following the end of the authorisation for Covert Surveillance and CHIS. Records relating to Communications Data should be retained until they have been inspected by the Interception of Communications Commissioner. The record should include not only those authorisations granted, but also those which are refused.

3.3.2 All CHIS and Directed Surveillance records including JP authorisations must be supplied electronically by email to the Director of Governance, Finance and Public Services for the Central Record of authorisations. For the Acquisition of Communications data the record is maintained by the National Anti Fraud Network (NAFN). Nominated Authorising Officers may retain copy records for their own reference. Copies of all relevant documents should be returned electronically to the applying officer. An officer from the central record will advise Authorising Officers of the status of authorisations when renewals, cancellation etc are required.

3.3.3 Due to the sensitive nature of **all documentation** covered by the Act, consideration **must** be given to the means by which copies are forwarded to the central record to ensure confidentiality. Records of authorisations, renewals and cancellations should be forwarded by email to the Director of Governance, Finance and Public Services.

3.4 Authorisations for Directed Surveillance

3.4.1 An authorisation is required for covert surveillance undertaken:

(a) for a specific investigation or operation; and

(b) where the surveillance is likely to result in obtaining private information about any person (whether or not they are the subject of the surveillance).

3.4.2 Directed surveillance is conducted where the observation is for the purpose of gathering private information to produce a detailed picture of a person's life, activities and associations.

3.4.3 An authorisation is not required for covert surveillance carried out as an immediate response to events or circumstances which could not be foreseen. However, if this surveillance continues for a substantial period of time, or is recommenced after some time has elapsed, an authorisation may be required.

3.4.4 **Local Authorities cannot undertake intrusive surveillance**. Therefore Authorisations will not be granted for cover covert surveillance on residential premises

or in any private vehicles where an individual or surveillance device is present on such premises or vehicle.

3.4.5 Where the surveillance activity is likely to result in **confidential material** beingobtained, the Authorising Officer within Lancashire County council will be **the Chief Executive, or in his absence the person acting as Head of Paid Service** (see paragraph 4.3 of the Code of Practice on Covert Surveillance). In practice, advice should be sought from the Director of Governance, Finance and Public Services.

3.5 Covert Video Camera and Audio Recording Equipment

3.5.1 This type of equipment may be considered for the purpose of recording the transaction/activity and obtaining photographic evidence of individuals or activities eg Trading Standards test purchases etc. Concealed cameras and voice recorders may be used to record activities and conversations without the knowledge of the other party.

3.5.2 The deployment of such equipment clearly has the potential for not only obtaining personal information in relation to the suspect, but also collateral intrusion into the activities of other persons in the vicinity of the operation.

3.5.3 Whilst the use of such equipment does not automatically require an authorisation, consideration should be given to safeguard against any challenge as to Human Rights infringements. The manner in which such equipment is used may also invoke the requirements relating to **Covert Human Intelligence Sources.** Prior to such covert use of equipment, advice should always be sought from an Authorising Officer.

3.6 Grounds for Granting Authorisations

3.6.1 Surveillance **must** be shown to be necessary on specific grounds. Investigations undertaken by Local Authorities can only be authorised:

For the purposes of preventing and detecting crime or for preventing disorder

3.6.2 The Council operates parallel procedures for Non-RIPA investigations/surveillance (Ref paragraph 1.2)

3.6.3 Local Authorities are not able to issue urgent oral authorisations.

3.6.4 Officers should normally be able to prepare investigations in advance to enable a written authorisation to be obtained.

3.7 Duration of Authorisation

3.7.1 An authorisation is valid for three months, unless cancelled.

This begins on the day on which the Authorising Officer grants the application, the expiry date will be considered to be three months minus one day (authorisation ceases at 23:59) from the date of signature by the Authorising Officer.

3.7.2 The Authorising Officer should ensure that a system is in place to review authorisations before it ceases to have effect. It is a matter for the Authorising Officer to determine how frequently a review is necessary and practicable. This is stated within the authorisation as a control measure. The authorisation should also be reviewed prior to expiry to determine whether or not a renewal is required and can be justified. It is a requirement that review forms are maintained by the Central Record.

3.8 Renewal

3.8.1 An authorisation may be renewed for a further period of three months. It may be renewed more than once provided that the renewal continues to meet the criteria for authorisation. The number of occasions it has been renewed should be recorded.

3.8.2 A record should also be made of the following:

- Any significant changes to the previous authorisation
- Why it is necessary to continue the surveillance
- The value to the investigation of the information obtained so far by surveillance
- An indication of the length of time further surveillance may be necessary

3.9 Cancellations

3.9.1 The Authorising Officer who granted or who last renewed the authorisation must cancel it if satisfied that the directed surveillance no longer satisfies the criteria outlined in this procedure.

3.9.2 An authorisation should also be cancelled once the activity which was the subject of the authorisation has been completed. **The authorisation should not be left to lapse as a result of the time limit expiring.**

3.9.3 The reason for cancellation of the authorisation must be detailed on the cancellation form. The cancellation form should be sent to the Central Record by the Authorising Officer.

3.10 Records

3.10.1 Material obtained as a result of surveillance activities should be recorded on the “Record of Product obtained by Directed Surveillance Form”.

3.10.2 A copy of this form should be forwarded to the Authorising Officer to be filed with the Authorisation form. The original should be retained by the Investigating Officer as part of the case file. Internal procedures within some services may require that all authorisations and case materials are held within a specific secure location. A copy should be retained on the case file.

3.10.3 A record must also be maintained of the period over which surveillance has taken place.

3.11 Handling Product from Surveillance Activities

3.11.1 "Product" from Covert Surveillance activities may consist of:

- Photographs
- Video film
- Voice recordings
- Surveillance log
- Officer's notes

3.11.2 The above may be required as evidence in current or future criminal proceedings. Officers must have regard to the provisions of the Criminal Procedure and Investigations Act 1996 in relation to unused material. Product obtained via an authorisation may be used by the authority in other investigations.

3.11.3 Although specific legislation and the Data Protection Act 1998 provide for the disclosure of information in certain circumstances, additional controls are introduced by RIPA.

3.11.4 The use of any product obtained by authorised surveillance activities outside of the local authority or the Courts should only be authorised in the most exceptional circumstances. This requirement seeks to prevent product from being used for grounds other than that for which it was obtained. **Joint operations should make reference to the potential use of evidence by each agency.**

3.11.5 Officers may receive requests from other agencies for product, which may include photographs of suspects, descriptions and vehicle details. Where this information has been obtained under an authorisation, further guidance should be sought from the Authorising Officer since disclosure may not be permitted under the provisions of the Code of Practice.

3.12 Storage of Product

3.12.1 Officers should ensure that evidential protocols are observed to ensure the integrity, security and confidentiality of material. This will ensure that the requirements of the Data Protection Act are addressed.

3.13 Disposal of Product

3.13.1 Officers should ensure that personal data is not kept for longer than necessary for the purpose for which it was obtained as follows:
Product which is not required as evidence should not be retained any longer than necessary. It will be necessary to retain product for a sufficient time to safeguard the Council against any civil claims against infringement of an individual's Human Rights. **A period of five years** ensures that all of the retention period requirements are addressed.

3.13.2 Product which has been destroyed should have this fact recorded on the record of product obtained by Directed Surveillance and be signed by the officer

3.13.3 An amended copy of this Record form should be forwarded to the Authorising Officer indicating destruction of the product obtained from the surveillance activity.

4 Guidance Notes for the Authorisation of Directed Surveillance

4.1 Activity Involved

Does the activity involve:

The necessary and proportionate systematic covert surveillance of an individual which is likely to gather personal information?

If so, an authorisation is required

4.1.1 Low-level activity for example, to determine whether a premise is still trading, will not require authorisation. Surveillance carried out in response to immediate events will also not require authorisation. However, if the surveillance activity continues for any period of time, an authorisation will be required.

4.1.2 The Authorising Officer must be satisfied that:

The authorisation is:

Necessary for the purposes of preventing and detecting crime or for preventing disorder or is pursuant to Council Policy for Non-RIPA surveillance (Ref Paragraph 1.2)

4.1.3 **The Authorising Officer must also believe that the surveillance is proportionate to what it seeks to achieve, and is not excessive**.

Where the identity of the subject is known to the officer, measures should also be taken to verify (where appropriate) the address under surveillance (e.g. electoral register, business rates, utility suppliers). The Authorising Officer must include some control measures within the authorisation e.g. reviews, circumstances in which the surveillance must be stopped.

4.1.4 The application should provide the background to the investigation and details of other methods which have failed to provide the information being sought or why other methods are not appropriate.

4.1.5 The description of the activity to be undertaken should be as comprehensive as possible describing how the surveillance will be undertaken, where it will occur and any equipment (e.g. cameras, video camera) which will be used. The investigating officers must not employ techniques which are not permitted by the authorisation.

4.1.6 The information being sought should be described and how this may provide evidence of the offence or other matter being investigated. The potential for collateral intrusion should be identified and plans to avoid/minimise such intrusion.

4.1.7 A statement must also be included as to the likelihood of obtaining confidential material/religious material e.g. the premises are a residential property, not located near any medical, religious or legal establishments, therefore there is no likelihood of obtaining any confidential/religious material.

4.1.8 If confidential material is being sought, or is likely to be obtained, a higher level of authorisation is required. This authorisation can only be given by the Chief Executive (or in his absence by the Head of Paid Service). Further guidance should be sought from the Director of Governance, Finance and Public Services if confidential material becomes relevant to the investigation.

4.1.9 Where applications for authorisations are refused, records of the refused application must also be maintained stating the reasons for the refusal and a service number. Copies of these refusals must be sent for inclusion in the central record.

4.2 Directed Surveillance via Recording of Telephone Conversations

4.2.1 The interception of communications sent by post or public telecommunications systems or private telecommunications systems attached to the public network may only be authorised by the Secretary of State (Part I RIPA).

4.2.2. The attachment of a general surveillance device e.g. "wiretapping" to a telecommunications system can only be undertaken under a warrant issued under Section 5 of RIPA (this is not available to the Council).

4.2.3 However an exception to the rule requiring a warrant exists, where one party to a telephone conversation consents and where an authorisation for directed surveillance is obtained. See Section 48(4) of RIPA.

4.2.4 For example, a member of the public may consent to the recording of a telephone conversation made by or to him/her. An officer may seek to record such a conversation to assist with an investigation into another person's activities.

4.2.5 An officer may also request a colleague to telephone another person as part of an investigation or may make the call himself or herself. These situations may require an authorisation to be granted depending on the nature of the information to be obtained. Where the call is a simple call to enquire about the availability or description of goods or services on offer for supply as any consumer would enquire, an authorisation will not be required.

4.2.6 Where the person giving consent is not present and a recording made, this activity is deemed to be intrusive surveillance and is beyond the scope of activities authorised for the Council.

4.2.7 Where the Officer acts in an overt capacity, i.e. clearly identifying the fact that they represent the Council, the activity will not require a directed surveillance authorisation.

4.2.8 Where the Officer makes/receives the call acting covertly, with the possibility of private information being obtained and a relationship being entered into, both a directed surveillance and CHIS authorisation will be required.

4.2.9 Similarly if a member of the public or another person acting as a covert source is asked to record a telephone conversation made/received by them, both authorisations will be required to be in place.

4.3 Test purchasing of age restricted products

4.3.1 Juveniles may only be authorised as a CHIS by the Head of Paid Service.

4.3.2 Officers should have regard to the Better Regulation Delivery Office code of Practice in determining whether directed surveillance authorisation will be necessary in the context of the planned operations.

4.3.3 Where the information obtained relates only to whether a sale is made or not, and no other information is likely to be obtained which is not already known to the officer directed surveillance authorisation is not necessary.

5 Covert Human Intelligence Sources (C.H.I.S.)

5.1 Introduction

5.1.1 This section of the guidance document deals with Covert Human Intelligence Sources (CHIS), more commonly known as:
Undercover Officers
Informants/Agents
Authorisation is a two-stage process:

(a) to use a source
(b) an authority for the conduct of a source

NB Juvenile surveillance CHIS – normally no-one under 18 years or any vulnerable individual should be considered as a CHIS (see 5.6 – 8)

5.1.2 A CHIS is a person who establishes or maintains a personal or other relationship with another person for the covert purpose of:

(a) Using such a relationship to obtain information or to provide access to information to another person, or

(b) Disclosing information obtained by the use of such a relationship or as a consequence of such a relationship.

In addition, a person who covertly provides information to a public authority is potentially a CHIS if he has obtained that information in the course of or as a consequence of the existence of a personal or other relationship, whether or not the relationship has been established or maintained for that purpose. A repeat informant if and when it becomes apparent that he obtains his information in that way is a CHIS to whom a duty of care is owed, if the information is acted upon. Legal advice should be taken before acting on the information provided by such a source.

5.1.3 The relationship is used covertly if, and only if, it is conducted in a manner calculated to ensure that the person is unaware of its purpose.

5.1.4 The Council receives complaints/information routinely from the public and traders regarding the alleged activities of individuals. The actions of these complainants do not generally fall within the definition of a covert source since they are a one off provision of information. However, a person may become a covert source if an ongoing relationship with the Council develops and activities described in paragraph 5.1.2 above are carried out.

5.1.5 Where the nature of the complaint relates to a matter where an officer requests the complainant to obtain further information covertly via a relationship with another individual, this activity is likely to fall within the scope of RIPA. An authorisation will therefore be required before seeking such information. By following the authorisation procedures, the Council will also be in a position to seek to safeguard the identity of the source in any subsequent legal proceedings. Further guidance should be sought from the Director of Governance, Finance and Public Services Group on this issue to ensure that the identities of any such individuals are safeguarded in the event of any legal proceedings, tribunals or disciplinary hearings.

5.1.6 The Code of Practice on Covert Human Intelligence Sources relates not only to sources (which may commonly be referred to as informants) but also the activities of sources, which consist of undercover officers who establish or maintain a covert relationship to obtain information and evidence.

5.1.7 Before a source may be engaged or an undercover officer deployed the use must be authorised. A separate authorisation for the conduct is also required. The use authorisation effectively registers the source with the Council. The conduct will address each separate operation/investigation in which that source may be involved.

5.1.8 In most cases, the use and conduct of a source will be restricted to a single investigation. However, situations may arise where different conducts are required which can be done once the use authorisation is in place. An example would be officers of a Service who undertake investigations which require different undercover stories to be adopted. The use authorisation enables them to undertake such covert activities. The conduct authorisation addresses each different cover story and activity within a different investigation/operation.

5.1.9 The same authorisation form is used for both use and conduct, with the deletion of Use*/Conduct* as appropriate. A conduct authorisation should be traceable back to the original use authority. A handler and controller must also be designated as part of

the authorisation process and detailed records of the use, conduct and tasking of the source maintained.

5.1.10 An Authorising Officer is a person entitled to give an authorisation for the use or conduct of a source in accordance with Section 29 of the RIPA. The Head of Trading Standards and Trading Standards Managers have been designated as authorising officers.

5.1.11 The use of a CHIS should be **necessary** and **proportionate** to the matter being investigated (see para 3.1.9).

5.1.12 Failure to obtain an authorisation may render the Council liable to a claim of infringing the human rights of an individual and may adversely affect the admissibility of any evidence obtained by the use of covert methods employed by a source. It is also established that a public authority owes a duty of care to a CHIS. Failure to undertake a robust risk assessment and authorisation may also adversely affect the position of the Council in the source suffering any harm as a result of the activity in which they have been engaged.

5.1.13 Careful consideration must be given to any potential sensitivities which may exist before deciding whether to use a CHIS in a particular community or against a particular individual.

5.1.14 A separate directed surveillance authorisation is not required where any surveillance device (technical equipment) is used in the presence of the covert source.

5.1.15 A CHIS carrying surveillance equipment can be invited to enter residential premises or a private vehicle. However the CHIS cannot install surveillance equipment in residential premises or a private vehicle since this activity constitutes intrusive surveillance and is not available for use by local authorities.

5.2 Further Guidance on the C.H.I.S Process.

5.2.1 When seeking an authorisation for an individual to act as a CHIS, consideration needs to be made of their potential role in the investigation. Are they prepared to be a witness? Do they need to be given protection as a result of providing information? The source may also be in a position to provide information relating to a number of different matters worthy of investigation.

5.2.2 The motives of potential sources need to be considered as part of the evaluation process. Could they be motivated by possible rewards or revenge? The aim could be to deflect attention away from themselves towards other individuals.

5.2.3 Has consideration been given to building up a detailed profile of the potential source and their associates? In all cases, a face-to-face meeting with the complainant or any other person considered as a potential source should take place. Please be aware that the individual may have needs in respect of language, hearing or sight.

5.2.4 Directed surveillance may be needed to evaluate the source. Consideration should be given in certain circumstances to carrying out checks on the source with the

Police. A thorough risk assessment must be carried out on the potential source and the proposed conduct.

5.3 Management of Sources

5.3.1 Tasking is the assignment given to the source by the handler/controller asking him/her to obtain information or to take action to obtain information.

5.3.2 All authorisations should be in writing and in place before tasking a source. Every source must have a designated handler and controller. RIPA provides for urgent oral authorisations to be granted. However, Authorising Officers should bear in mind the potential risks and liabilities of authorising a CHIS without a risk assessment being undertaken. Such authorisations should therefore only be considered in exceptional circumstances.

5.4 Designated Handlers and Controllers for the Use of Covert Human Intelligence Sources

5.4.1 Where the CHIS is a complainant or an informant, the Handler will be the Investigating Officer and the Controller will be their line manager. Where the CHIS is employed by the Council acting in an undercover capacity, the Handler will be the officer's line manager and the Controller will be another manager within the Service. This arrangement will ensure that an officer does not act as a Controller and Authorising Officer thereby ensuring a level of independent scrutiny.

5.5 Security and Welfare of Sources

5.5.1 A source has no licence to commit crime. In certain circumstances it may be advisable to provide written guidance to the source explaining what is being requested of them and the limits of the tasking. The source should be asked to sign such a document to confirm that they understand the terms of reference.

5.5.2 A public authority deploying a source should take into account the safety and welfare of the source when carrying out any actions in relation to the authorisation or tasking. The foreseeable consequences of the tasking should also be considered.

5.5.3 A Risk Assessment should be undertaken to evaluate the source and to determine the risk to the source of any tasking and the likely consequences should the identity and role of the source become known to the subject or others involved with the subject.

5.5.4 The handler should draw to the attention of the controller:

- The Risk Assessment
- The Conduct of the Source
- The Safety and Welfare of the Source
- A Handler is responsible for:
- Dealing with the source on behalf of the Council
- Directing the day to day activities of the source
- Recording the information supplied by the source

Monitoring the security and welfare of the source

5.5.5 Where a source is known or suspected of being involved in crime, consideration should be given to their motives in supplying information. It may also be a prudent step in the management of such a source to have two officers present during any meetings with the source. Background checks on the potential source via the Police Local Intelligence Officer should also be considered.

5.5.6 Special provisions exist for the conduct in use of juvenile sources (Under 18).
A source under 16 cannot be engaged to use a relationship with any person having parental responsibility for them. A source under 16 must have an appropriate adult present during any meetings and a risk assessment must also take place before granting or renewing an authorisation for the conduct and use of a source under 18. This will take account of physical and psychological risks.
See the Regulation of Investigatory Powers (Juveniles) Order 2000 for detailed guidance.

5.5.7 Special consideration should also be given to the use of vulnerable individuals as a source. This will require the highest level of Authorising Officer (see the code of practice for further guidance).

5.5.8 Authorisations for juvenile sources ie a source under the age of 18, when the authorisation is granted, have effect for one month. **Juvenile and vulnerable source authorisations can only be issued with the authorisation of the Head of Paid Service.**

5.6 The Application for Authorisation

Must include:

5.6.1 The ground on which the authorisation is sought:

- Preventing, detecting crime or preventing disorder (or other Lancashire County Council Non-Ripa policy circumstances)

- An explanation of the necessity and proportionality of the Use/Conduct.

- Where the matter relates to a specific investigation, details of that investigation or operation.

- Details of the purpose for which the source will be tasked.

- Details of what the source will be tasked to do.

- Details of the level of authority required having regard to any confidential material that might be obtained as a consequence of the authorisation. (This will invoke the requirement to be authorised by the Chief Executive if confidential material is being sought or is likely to be obtained).

- Details of who will be affected and plans to avoid/minimise collateral intrusion. Where this changes, the Authorising Officer must be informed and the authorisation reviewed.

- A detailed Risk Assessment must have been undertaken. A review may also be required if the assessment is not current.

- The Authorising Officer may wish to impose control measures on the authorisation that is granted.

5.6.2 Unless renewed or cancelled, an authorisation remains in force for:

12 months from the date of issue (Juveniles - one month). The authorisation should be given a unique operation reference number and be recorded in management record file. Conduct authorisations should be referenced to the original use authorisation.

A duplicate/copy of the authorisation should be issued to the officer. This will ensure that the officer has a record of the scope of the activity authorised.

5.6.3 Applications which are refused should also be recorded together with the reasons for the refusal and a service number. Copies of these refusals must be sent for inclusion in the central record.

5.7 Duration of Authorisations

5.7.1 Authorisations have effect for a period of twelve months. It is suggested that the authorisation to use the source has effect for up to 12 months (other than juveniles, see above), however the conduct may be restricted to a shorter period or be made subject to reviews set as a control measure by the Authorising Officer.

5.7.2 Records of authorisations to be retained for a minimum period of one year to comply with the code. However, it will be policy to retain the records for a period of five years to safeguard against any civil claims against the Council under the Human Rights Act 1998.

5.7.3 Destruction of the authorisation form should be documented in the Authorising Officers Management Record file.

5.8 Renewals and Reviews

5.8.1 An authorisation may be renewed after the Authorising Officer reviews the use made of the source having regard to:

a) The tasks given to the source
b) The information obtained from the source.

If satisfied that the original authorisation criteria are met, a renewal may be granted.
5.8.2 Since an authorisation for a CHIS may remain in force for a period of twelve months, regular reviews should be undertaken to ensure the ongoing validity of the

activity and the ongoing welfare and security of the source. Any changes to circumstances may require that further risk assessments are undertaken.

5.8.3 The reviews should be undertaken at intervals of no longer than three months and documented. Additional control measures may also be introduced as a result of a review. The Authorising Officer should implement a system to identify appropriate review dates.

5.9 Cancellations

5.9.1 An Authorising Officer must cancel an authorisation where:

The use or conduct of the source no longer meets the original authorisation criteria.

The procedures for managing the source are no longer in place.

Where possible the source should be informed of the cancellation, and this fact noted on the cancellation. The authorising officer should give directions on the handling, storage or destruction of the product of surveillance.

5.9.2 Where an investigation no longer requires the authorisation to be in place eg the evidence has been obtained, it should be cancelled promptly rather than allowed to expire through time, and the reason for cancellation documented.

5.10 Source Records

5.10.1 Records of Use of the source and the product provided by the sourceshould be maintained by the service for a period of five years. Records should not be destroyed without the authority of the Authorising Officer. Destruction of records should be documented in the Central Records file.

5.10.2 The following information must be recorded:

- Authorisation Reference Number
- Authorising Officer
- Identity used by Source (If any)
- Identity of Source
- Reference used in the authority to refer to Source (If any)
- Information relating to security and welfare of Source
- A record that any risks to the security and welfare of the Source have been explained to and understood by the Source
- Records of reviews conducted on the continuing use and welfare of the Source

- The date when the Source was recruited
- The circumstances of the recruitment
- Identity of the Handler and Controller (and details of any changes)
- A record of the tasks and activities given to the Source
- A record of all contacts or communications between the Source and a person representing the Council
- The information obtained through the Source
- How the information is used
- A statement as to whether any payment, benefit or reward is provided by or on behalf of any investigating authority and details of it***.**
- Reasons for cancelling/not renewing the authorisation and the date and the time of such a decision.

*(Please seek guidance regarding any payment, benefit or reward you may wish consider from an Authorising Officer).

Notes:

Necessity
For interference with an individual's private, family or business life to be necessary, the action must be for the purposes of preventing and detecting crime or of preventing disorder, be necessary to secure best evidence and that less covert or intrusive action would not serve the appropriate purpose.

Proportionality

The test for proportionality goes far beyond selecting the least intrusive method of investigation. The activity to be observed must not be trivial and must warrant the surveillance to be instigated.

The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair. Proportionality should contain a consideration of three elements:

a) that the proposed covert surveillance is proportional to the mischief under investigation;

b) that it is proporational to the degree of anticipated intrusion on the target and others and;

c) it is the only option, other overt means having been considered and discounted

6 Risk Assessments for All RIPA/Surveillance Activities

6.1 Whenever undertaking covert directed surveillance or engaging in the conduct and use of a CHIS, the proposed activity must be the subject of a risk assessment and evaluation of the proposed Source.

6.2 Directed Surveillance activities clearly have the potential to expose staff to hazards should their activities become known to the subject or even to others during the operation. The use of a CHIS has the potential to expose handlers, undercover officers, agents/informants and the public to health and safety risks. A duty of care may also lie with officers and the Council in managing sources.

6.3 Authorising Officers, Controllers, Handlers Undercover Officers and Investigating Officers must all have regard to the Council's Corporate Policy on Health and Safety. This addresses issues such as lone working and violence to staff.

6.4 It is a matter for each Service to determine the training required to ensure that staff are competent to undertake risk assessments of proposed operations/use of covert sources. All incidents/dangerous occurrences during the course of operations should be reported in accordance with the relevant Health and Safety Procedures.

6.5 Consideration should also be given to staff training requirements to engage in covert activities, surveillance and acting in an undercover capacity.

6.6 This section of this guidance document is intended to provide an overview which must be borne in mind when undertaking activities within the scope of RIPA.

6.7. Further Guidance on Health and Safety issues is available from Corporate HR/ Health and Safety sources.

6.8 Risk assessments for directed surveillance operations should be undertaken by the officer in charge of the proposed activity and submitted with the authorisation application.

6.9 Risk assessments for the use of a CHIS should be undertaken by the Handler and considered by the Controller as part of a risk management process. The assessment should then be forwarded to the Authorising Officer with the application. The assessment should consider the Ethical, Personal and Operational Risks of the proposed activity. The evaluation of a potential source is an important part of the application process.

6.10 Risk assessment is not a one off activity but an ongoing process throughout the operation and use of the source, since circumstances may change and a review may be required.

6.11 The nature of the risks surrounding the deployment and management of individual sources, handlers and operational activities will vary according to a wide

range of factors on a case by case basis. Risk assessment allows the handler and controller to advise the Authorising Officer of the plan for managing the risks.

6.12 Authorising Officers will **not** authorise a Directed Surveillance operation or the use of a source without the evidence that the risks have been considered and a plan for their management exists.

7 Communications Data

7.1 Accessing Communications Data

7.1.1 The relevant provisions of Part I Chapter II of RIPA 2000 came into force on 5 January 2004. This established a formal legal framework, by which public authorities can obtain communications data by a lawful method, consistent with article 8 of the Human Rights Act 1998.

7.1.2 This section of the guidance document details the systems in place to ensure compliance with RIPA when an investigating officer seeks to obtain communications data within the scope of their enquiries.

7.1.3 In a similar manner to the existing provisions of RIPA relating to directed surveillance and the use of a CHIS, a process of submitting an application and securing an authorisation is established by the legislation and code of practice.
For this part of the Act the lead Service for the Authority is the Trading Standards Service. The Senior Responsible Officer for this Part of the Act is the Head of Service for Trading Standards.

7.1.4 Under Section 22(2) of RIPA, communications data which local authorities are entitled to access can only be sought for the purpose of:

The prevention and detection of crime or preventing disorder Section 22(2)(b)

The application is also put to the two tests under RIPA of necessity and proportionality.

7.1.5 This activity cannot be undertaken by an officer as communications service providers will only accept requests for information form accredited officers registered with the Home Office and termed **Single Points of Contact (SPOC).**

7.1.6 The National Anti Fraud Network acts as the SPOC on behalf of Lancashire County Council. Applications are made by officers via a secure network, and forwarded to the designated persons in the Trading Standards Service for authorisation by means of this network.

7.1.7 Records of all applications, authorisations, notices, cancellations and refusals are maintained by NAFN. These are subject to periodic inspection by the body appointed to have an overview of this Part of the Act, the Interception Commissioner. As with other parts of RIPA there is a Central Record. For this part of the Act it is maintained by NAFN on behalf of Lancashire County Council.

7.2 What is Communications Data

7.2.1 Communications data is information held by communication service providers such as telecom, Internet and postal companies relating to the communications made by their customers.

7.2.2 Communications data includes the detail of the user, the use and the content (Traffic) of the communication. (Note: Local Authorities do not have the right to access traffic information).

7.3 Who are Communication Service Providers

7.3.1 Communications data is obtained from Communications Service Providers (CSPs)
These include:

Telecommunications Providers

- Mobile Phone service providers eg Orange, Vodafone, T Mobile, O2
- Landline telephone service providers eg BT, NTL, Cable and Wireless
- International Simple Voice Resellers eg One-Tel

Internet Service Providers (ISPs)

Examples: AOL, BT, NTL

Virtual ISP's: Freeserve

Portals: Hotmail, Yahoo, Lycos

Postal Providers

- Royal Mail, Parcelforce, DHL
- Small parcel courier services
- Accommodation agencies, which forward mail to clients

7.4 What Information can be Obtained from Communications Service Providers

7.4.1 **Information about communications service users**
Section 21(4)(c)

This category mainly includes personal records supplied to the CSP by the customer/subscriber. For example, their name and address, payment method, contact number etc.

- Name of account holder/subscriber
- Installation and billing address
- Method of payment/billing arrangements
- Collection/delivery arrangements for PO Box (but not where from or to)

- Other customer information such as any account notes, demographic information or sign up data (not passwords or personalised access information)

7.4.2 **Information about the use of the Communications Service**
Section 21(4)(b)

This category mainly includes everyday data collected relating to the customer's use of their communications system. For example, details of the dates and times they have made calls and which telephone numbers they have called.

- Outgoing calls on landline or contract or prepay mobile
- Timing and duration of service usage
- Itemised connection records
- Internet log on history
- Emails log (sent)
- Information on connection, disconnection and reconnection of services
- Information on the provision of conference calling, call messaging, call waiting and call barring
- Information about the provision and use of forwarding/redirection services (postal and telecom)
- Records of postal items, such as records of registered, recorded or special delivery postal items, records of parcel consignments, delivery and collection

7.4.3 **Information about Communications (Traffic Data)**
Section 21(4)(a)

Local authorities are not permitted to obtain 'traffic' data (ie the actual content of the communication or more detailed information or tracking)

This category mainly includes data generated by the CSP (network data) relating to a customer's use of their communication system (that the customer may not be aware of) for example, cell site data and routing information.

- Information identifying the sender and recipient (including copy recipients) of a communication
- Information identifying any location of a communication (such as mobile phone cell site locations data)
- Routing information identifying or selecting any apparatus through which a communication is transmitted – for example dynamic IP address allocation, web postings and e-mail headers
- Call detail records for specific calls (such as calling line identity – incoming calls)
- Web browsing information (only the web site name is disclosed and not the pages visited on the web site)
- Information written on the outside of a postal item (such as a letter or parcel)
- Online tracking of communications (including postal)

- Signalling information and dialling sequences that affects the routing of a communication (but not the delivery of information) in the investigation of “dial thru” fraud

Please note that these lists are not exhaustive and the CSPs cannot all provide the same information.

7.5 How can this Information be Obtained

7.5.1 Under Section 22(2) of RIPA, communications data which local authorities are entitled to access can only be sought if it for the purpose of:

The prevention and detection of crime or preventing disorder Section 22(2)(b)

7.5.2 The application is also put to the two tests under RIPA of necessity and proportionality.

7.5.3 RIPA establishes two methods by which communications data may be obtained:

Notices
Authorisations

7.5.4 A Notice under Section 22(4) of RIPA requires the CSP to collect or disclose the data on behalf of the public authority.

7.5.5 An authorisation under permits the public authority to collect the information. This may be where the CSP is not capable of colleting the data or a prior agreement is in place to allow the authority to access the data.

7.5.6 A CSP only has to provide the data in a reasonable time and if practical to do so. Different CSPs will have different types of data and differing retention periods.

7.5.7 When it becomes clear that a witness statement is required to formally produce the data which has been provided by the CSP, it should be requested without undue delay.

7.5.8 CPSs are entitled to recover reasonable costs incurred in providing the data and supplying witness statements. These vary from one CSP to another.

7.5.9 Where the notice or authorisation is approved by the Designated Person (Authorising Officer), it remains in force for a period of one month.

7.5.10 Notices and authorisations which are no longer required are no longer necessary or proportionate and must be cancelled.

7.6 Contact with the Communications Industry

7.6.1 Notices and, where appropriate, authorisations for communications data can only be channelled through single points of contact officers (SPOCs) within each public authority.

7.6.2 Similarly, requests for a witness statement following receipt of data from a CSP should also be via a SPOC.

7.6.3 SPOCs have been trained via a course accredited by the Home Office and the details of nominated SPOCs within each public authority are held by each CSP.

A CSP will therefore not deal with any request received from another un-accredited source of enquiry.

7.7 The Role of the SPOC

7.7.1 SPOCs will enable a more efficient regime to be developed as they will deal with CSPs and become aware of the data which they hold.

7.7.2 The SPOC plays an important role in the self-regulation and internal quality control of a public authority in ensuring that the requirements of RIPA are adhered to in requesting and obtaining communications data.

7.7.3 SPOCs reduce the demands upon CSPs from a great number of sources within a public authority.

7.7.4 A SPOC will be able to advise the applicant officer of the nature and practicalities of obtaining the data which is being requested.

7.7.5 The SPOC will advise the applicant on the content of the application request prior to submission to the Authorising Officer and where necessary refuse the application at that point for stated reasons.

7.7.6 The SPOC provides a safeguard for CSPs in ensuring that applications and notices are genuine.

7.7.7 SPOCs will retain a list of contact points with relevant CSPs.

7.7.8 NAFN provide a SPOC service on behalf of Lancashire County Council, and access details are maintained within the Trading Standards Service.

7.8 The Role of the Authorising Officers

7.8.1 This officer considers the necessity and proportionality of any application for communications data (see earlier sections of this Guidance Document which provide further information on these tests).

7.8.2 Consideration should also be given to the issue of collateral intrusion where other persons may be affected by the granting of the notice or authorisation.

7.8.3 The Authorising Officer is required to be an officer at least at the following level within the authority:

- Director

- Head of Service
- Service Manager or equivalent

An Authorising Officer should have the necessary training and experience to be competent to authorise activity. A record of Authorising Officers will be kept within the Trading Standards Service.

7.9 The Application Process

7.9.1 The investigating officer should log in to NAFN and complete the relevant online form.

7.9.2 The application should then be submitted to the SPOC via NAFN who will give consideration to the following:

- Whether the data being requested is capable of being provided by the CSP

- The reasons for the data being required in terms of the investigation being conducted and the offence being investigated

- The grounds for necessity and proportionality being addressed

- Should the application be deemed satisfactory, a Notice or authorisation form will be completed, this together with the application form will be submitted to the Authorising Officer for authorisation or refusal.

Should the SPOC, however, consider there are grounds refusing the application, the form will be returned to the officer via the network.

When a Notice or authorisation is approved by the Authorising Officer, the SPOC will send it to the relevant CSP.

A Notice is only valid for a period of one month.

When, during the life of a Notice or authorisation, it is no longer necessary or proportionate or is no longer required by the investigation it must be cancelled.

.

7.10 Records and Errors

7.10.1 NAFN will retain records of all applications, refusals and authorisations passed to the designated person. Copies of all Notices/authorisations and refusals from the Authorising Officer will be retained.

7.10.2 This will allow a full audit trail for an application for obtaining communications data.

7.10.3 Documentation will be maintained by NAFN for inspection by the Interception Commissioner and complaints falling within the remit of the Complaints Tribunal.

7.10.4 Where any errors have occurred in granting authorisations or notices (eg subscriber details of an incorrect telephone number being obtained), a record must be kept and the matter explained by means of a report to the Commissioner as soon as practicable. NAFN or the authorising officers will notify the Trading Standards Head of Service of any errors as soon as possible so a report can be sent to the Interception Commissioner.

8 Seeking JP approval for authorisations

8.1 In all cases involving authorisation of Directed Surveillance, use of CHIS, and access to Communications Data, officers must seek prior approval from a JP before undertaking the activity.

8.2 If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

8.3 The officer will make an appointment at the relevant magistrates' court and will provide the JP with a copy of the original RIPA authorisation or notice and the supporting documents setting out the case. This forms the basis of the application to the JP and **should contain all information that is relied upon**. For communications data requests the RIPA authorisation or notice may seek to acquire consequential acquisition of specific subscriber information. The necessity and proportionality of acquiring consequential acquisition will be assessed by the JP as part of his consideration.

8.4 The original RIPA authorisation or notice should be shown to the JP but will be retained by the local authority so that it is available for inspection by the Commissioners' offices and in the event of any legal challenge or investigations by the Investigatory Powers Tribunal (IPT). The court may wish to take a copy.

8.5 In addition, the local authority will provide the JP with a partially completed judicial application/order form.

8.6 The order section of this form will be completed by the JP and will be the official record of the JP's decision. The local authority will need to obtain judicial approval for all initial RIPA authorisations/applications **and renewals** and the local authority will need to retain a copy of the judicial application/order form after it has been signed by the JP. There is no requirement for the JP to consider either cancellations or internal reviews.

8.7 Further more detailed guidance and documentation should be accessed via the Home Office Guidance available on the www.gov.uk website.

8.8 Where JP approval is granted, this should be forwarded to the Director of Governance, Finance and Public Services for the Central record, and directed surveillance and CHIS activity can commence. For Communications Data, the approval needs to be returned to NAFN for the SPOC to contact the relevant CSP.

9 Lancashire County Council Auditing of Authorisations and Records

9.1 Each Service must annually undertake a review of their activity within the scope of RIPA and complete the annual RIPA and non RIPA return form which must be returned to the Director of Governance, Finance and Public Services.

9.2 A cross Council officer working group meets four times a year to monitor activity under the Act, arrange training and provide guidance. The Senior Responsible Officer is a member of the group and reports activity under RIPA to the Crime and Disorder Overview and Scrutiny Committee.

9.3 Part of the Audit will focus on a review of Projected Service activity and that all relevant staff have had sufficient training.

9.4 The following will also fall within the scope of the audit:

- Applications
- Authorisations
- Risk assessments
- Reviews and Renewals
- Cancellations
- Records of Product of Directed Surveillance
- Source Records
- Staff Awareness

9.5 The audit will seek to establish compliance of the authorisations/renewals/cancellations and records with the following:

- RIPA
- Statutory Instruments made under RIPA
- The Code of Practice on Covert Surveillance
- The Code of Practice on Covert Human Intelligence Sources
- The Code of Practice on Accessing Communications Data
- https://www.gov.uk/government/collections/ripa-codes
- Lancashire County Council RIPA Guidance Document and work instructions
- Guidance material issued by the OSC and IOCCO.

9.6 Non-conformities identified as a result of the audit will be reported to the relevant Service Management Team. Action taken by local management should be reported back to the Audit team.

9.7 The cross Council audit report will be held within the Central Record.

9.8 The processing of prosecution reports by a service should have regard to compliance with RIPA where investigations include covert surveillance and/or the use of a CHIS and/or obtaining communications data.

10 Inspections by the Office of the Surveillance Commissioner (OSC) and the Interception of Communications Commissioner (IOCCO)

10.1 The Codes of Practice include a section dealing with inspection by the Commissioners. They impose a requirement to comply with requests and to disclose or provide information requested by the Commissioner to allow him to carry out his functions.

10.2 During inspection visits, the codes require certain authorisations to be drawn to the Inspector's attention. These being where the Authorising Officer has authorised an activity he is directly involved in and those where confidential material is sought or obtained.

10.3 A further inspection regime has been established by RIPA in relation to accessing communications data. This is undertaken by the Interception of Communications Commissioner. These inspections take place through NAFN, with queries raised individually with local authorities where necessary. Similar recourse to the Tribunal exists for complaints against the activities of the authority.

11 Complaints

11.1 An independent complaints procedure is provided by the legislation. Complaints can be made to:
The Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ
Tel: 0207 035 3711
http://www.ipt-uk.com/

12 Management Records

12.1 The management files, authorisations/renewals/cancellations and Source Records **must be** kept in a secure place with restricted access. These files will provide the basis of the audits and be liable for inspection by the Office of the Surveillance Commissioners. **Originals of the authorisations (including refusals), reviews, renewals and cancellations, must also be provided to the Central Record. This is managed by the Director of Governance, Finance and Public Services.** Officers forwarding confidential material to the Central Record must ensure that it is forwarded by a secure method.

12.2 **Security of the Central Record**

The Central Record is to be held in a suitable locked cabinet, or secure electronic folder.

Scrutiny Committee

Report of the Director of Development and Corporate Resources

Meeting to be held on 11 December 2015

Electoral Division affected: ALL

Lancashire Superfast Broadband Programme – Interim Update

Contact for further information:
Sean McGrath, External Funding and Investment, Programmes Office;
(01772 531053), sean.mcgrath@lancashire.gov.uk

Executive Summary

The report provides an interim position on the progress of the current Superfast Broadband project, planning for the Superfast Extension programme and further opportunities for domestic and business premises to access Superfast Broadband. This information will be made available in the form of a presentation to the meeting.

Recommendation

That the contents of the report and presentation be noted.

Background and Advice

Superfast Broadband (SFBB) refers to a range of measures to ensure businesses and consumers are best able to exploit the benefits of high speed broadband connections. Through Broadband Delivery UK (BDUK), the government has defined SFBB as a speed of not less than 24Mbs. Mbs stands for Megabits and is the expression used to measure broadband speeds.

Public investment can only be made in support of the extension of Superfast Broadband in those areas with deemed market failure, which is considered to be postcodes with no provider of Superfast Broadband services. In Lancashire, this mainly constitutes rural areas, although not exclusively.

The current Lancashire Superfast Broadband programme, which will deliver access to Superfast Broadband to 130,000+ premises, started in 2013 and is now coming to an end. The Superfast Extension programme will start in the New Year and deliver Superfast access to another 12,000+ premises. These programmes will run in parallel to commercial activity delivered by BT and other providers, such as B4RN, and should result in 99% of Lancashire premises having access to Superfast Broadband by the end of 2017.

The presentation will set out the detail and achievements of the current programme, provide further information on the planning and implementation of the Superfast Extension Programme, and highlight a number of other initiatives that will be utilised to support further access to and use of Superfast Broadband in Lancashire. Paper copies of the presentation will be made available at the meeting.

Consultations

N/A

Implications:

This item has the following implications, as indicated:

Risk management

N/A

Local Government (Access to Information) Act 1985
List of Background Papers

Paper Date Contact/Tel

Reason for inclusion in Part II, if appropriate

Scrutiny Committee
Meeting to be held on 11 December 2015

Electoral Division affected:
All

Sub-committee of the Scrutiny Transport Asset Management Plan (TAMP) Task Group

Contact for further information:
Karen Cassar, (01772) 534422, Highways Asset Manager,
Karen.cassar@lancashire.gov.uk

Executive Summary

At the meeting of the Scrutiny Committee held 11 July 2014 the Committee resolved to: note the County Council's TAMP 2015-2030 and establish a Task Group to monitor the implementation of the TAMP. The Scrutiny TAMP Task Group met recently and County Councillor John Fillis, Cabinet Member for Highways and Transport, suggested that the Task Group could expand in terms of membership from its current format. The Task Group agreed to the expansion of the membership.

Recommendation

Approval is granted to expand the Scrutiny TAMP Task Group.

Background and Advice

Recent changes to Government and Department for Transport (DfT) funding has incentivised highway authorities to adopt the principles of asset management to maximise their funding opportunities. With the introduction of the Transport Asset Management Plan (TAMP), Lancashire County Council has introduced the principles of asset management to manage its highway assets. At the meeting of the Scrutiny Committee held 11 July 2014 the Committee resolved to: note the County Council's TAMP 2015-2030 and establish a Task Group to monitor the implementation of the TAMP. The Scrutiny TAMP Task Group met recently and County Councillor John Fillis, Cabinet Member for Highways and Transport, suggested that the Task Group could expand in terms of membership from its current format. The Task Group agreed to the expansion of the membership. To expand the Task Group membership it was agreed to write to the Leaders of the 12 districts and invite them to nominate an Elected Member to represent their district and attend future meetings of the Task Group.

The benefits derived from the formation of the sub-committee will demonstrate the commitment of the authority to communicate its strategy for maintaining the highway

and its assets in line with the principles of asset management identified in the TAMP strategy. The commitment from all elected councillors is vital in maintaining the highways in order to implement the principles of asset management and secure maximum funding from Department for Transport.

Consultations

N/A

Implications:

This item has the following implications, as indicated:

Risk management

Failure to implement this proposal may result in miscommunication of the strategy of the TAMP and the principles of asset management which the authority has adopted. The lack of commitment by elected members to the TAMP strategy may result in the principles of asset management being adopted across the county.

Financial

N/A

Legal

N/A

Scrutiny Committee

Meeting to be held on 11 December 2015

Electoral Division affected:
None

Work Plan and Task Group Update
(Appendix 'A' refer)

Contact for further information:
Habib Patel, (01772) 536099, habib.patel@lancashire.gov.uk

Executive Summary

The plan set out at Appendix 'A' summarises the work to be undertaken by the Committee in the coming months, including an update on Task Group work. The information will be updated and presented to each meeting of the Committee for information.

Recommendation

The Committee is asked to note the report.

Background and Advice

Information on the current status of work being undertaken by the Committee and Task Groups is presented to each meeting for information.

Consultations

N/A

Implications:

This item has the following implications, as indicated:

Risk management

There are no significant risk management implications.

List of Background Papers

Paper	Date	Contact/Directorate/Tel
N/A		

Reason for inclusion in Part II, if appropriate

N/A

Appendix 'A'

Scrutiny Committee Work Plan 2014/15

11 December 2015		**Regulation of Investigatory Powers Act 2000 Update**	Amanda Maxim/Ian Young/Laura Sales	Annual update
		Superfast Broadband Roll Out	Sean McGrath	Full update on progress as agreed as requested by Executive Scrutiny Committee on 31 March 2015
15 January 2015		**Report of the Planning Matters Task Group**	Andrew Mullaney	

Future Topics: not yet scheduled

- Bus Services and Subsidies - to consider outcomes of discussions with districts and next steps
- Transforming Social Care - to consider the work undertaken by independent consultants
- Lancashire Enterprise Partnership Update
- United Utilities
- Libraries and Cultural Services
- Rail Travel – Update on developments since task group
- Supporting Young People

Task Groups

The following task and finish groups are ongoing or have recently been established:

- Planning Matters: Interface between upper and lower tiers authorities in making the right decisions on planning applications (especially flood management and educational provision)
- Fire Prevention Measures in Schools
- Transport Asset Management Plan (TAMP)