Appendix 'C'

Covert Social Networking Checks and Surveillance Policy

Lancashire County Council

www.lancashire.gov.uk

Purpose:

To provide guidance to Lancashire County Council (LCC) employees when using social media or internet open source information in furtherance of LCC investigations, as to when authorisation for surveillance activities should be sought.

Responsibilities:

Director of Governance, Finance and Public Services
Director of Legal and Democratic Services
Service Managers

Guidance:

For Directed Surveillance and Covert Human Intelligence Sources
https://www.gov.uk/government/collections/ripa-codes
Corporate Policy and Guidance On The Regulation Of Investigatory Powers Act 2000
Corporate Policy and Guidance On Non RIPA surveillance activities

NOTE

Before any investigation takes place using the internet or social media, the investigating officer should have regard to the potential need for a directed surveillance application or a covert human intelligence source application in accordance with corporate policy.

Guidance must always be sought from a manager in the first instance, and in cases of doubt from the Director of Legal and Democratic Services. The important considerations are that the surveillance is necessary, in that there is no other way of obtaining the information, and proportionate – taking into account the following:-

• 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

Open Source

Information which is "open source", that is to say where the individual can have no reasonable expectation of privacy, can generally be utilised in furtherance of an investigation. However, where an operation involves the longer term monitoring of an individual and is likely to result in the gathering and retaining of private information, consideration should be given to obtaining authorisation for directed surveillance.

Where it is proposed to gather information from a source or informant, consideration should be given to authorising a CHIS.

Using Facebook/similar social networking sites

Overt warnings

Consideration will always be given to the appropriateness of gathering information in a covert way. Wherever possible the target of any investigation will be made aware of the issue and given the opportunity to amend their behaviour, unless in all the circumstances given the seriousness of an allegation, this is not appropriate.

The warning should make it clear that the target's activities will be monitored and investigated should the conduct continue. The warning, the reason for it, and a screen shot of any web page should be saved on file.

Covert activity

There may be circumstances where it is decided that it is inappropriate to send an overt warning to an individual: For example:

- where the individual has previous history of the behaviour complained of,
- where it is intended to carry out more detailed investigations into social or business links that the individual has, because serious issues are involved
- where the activity is clearly carried out with a deliberate intention to defraud, or
- Where the activity is on such a scale or linked with other illegal activity such that it is thought robust action is necessary.
- Where vulnerable individuals are at serious risk of harm from the behaviour.

This may necessitate ongoing monitoring of social media, and/or also entering into a relationship with the target, and authorisation for this should be discussed and agreed with a service manager. **LCC officers should never use their own Facebook accounts to facilitate this activity.**

RIPA authorisation

Where an overt warning has been provided, a further check should be made to assess whether the behaviour is continuing. If this is the case, the investigating officer should take a screen shot and record this on file. No further monitoring or activity should take place at this point. The investigating officer should provide full details to their manager, to discuss applying for an authorisation for CHIS or Directed Surveillance.

Summary

Authorisation is not normally necessary for open source investigations unless there is some ongoing monitoring of an individual.

Where a relationship which is more than merely transitory is entered into with an individual, authorisation under CHIS should be sought.

Where ongoing monitoring of social media is involved but no relationship is established and there is no possibility of obtaining private information, authorisation may not be necessary.

In cases of doubt further advice should be sought.

All decisions about the case should be properly logged and recorded.

Authorisations should clearly describe the conduct which is authorised.

Reviews and cancellations of authorisations should be carried out and clearly documented.

All applications should be made on the corporate forms, and sent to the central record of authorisations for retention for 5 years.

In addition any retention and disclosure of information needs to be carried out in accordance with the Data Protection Act 1998 - in particular:-:

- Only collect and process appropriate personal data to the extent that it is required to fulfil operational needs or to comply with legal requirements.
- Ensure the quality of the data we use.
- Apply retention schedules to determine the length of time we hold information and dispose of information securely when it has reached its disposal date.
- Ensure that individuals, about whom we hold data, can fully exercise their rights under the DPA 1998.
- Take appropriate security measures to safeguard personal information.
- Ensure that we do not transfer personal data outside the country without suitable safeguards.

If in doubt seek advice from the Information Governance Team.

Be aware that content you share and actions you take may show up on pages other than your own and could be reshared by other users.

For more detailed guidance on directed surveillance and CHIS see the corporate policies for RIPA and non RIPA authorisations, and the Home Office Guidance.

Version Control

Named Owner:	Laura Sales: Director – Legal and Democratic Services
Version Number:	1.00
Date Of Creation:	November 2016
Last Review:	
Next Scheduled Review:	November 2017
Overview of Amendments to this Version:	