Appendix

Covert Surveillance and the Acquisition of "Communications Data" Policy Statement

1. This policy sets out how Leicestershire County Council (the Council) will comply with the Regulation of Investigatory Powers Act 2000 (RIPA), the Investigatory Powers Act 2016 (IPA), the Human Rights Act 1998 and the European Convention on Human Rights (ECHR) - Article 8, when carrying out any covert investigatory techniques. If such covert investigatory techniques are conducted by the Council, RIPA and the IPA regulates them in a manner that is compatible with ECHR, particularly the right to respect for private and family life (Article 8). The use of covert investigatory techniques is an interference with the rights protected by the ECHR (Article 8) and there may be a potential violation of those rights, unless the interference is in accordance with the law and is necessary in a democratic society in the interests of:

   - national security;
   - public safety;
   - economic well–being of the country;
   - the prevention of disorder or crime;
   - protecting of health or morals; or
   - the protection of the rights and freedoms of others.

   Any such interference must be proportionate requiring a balancing of the seriousness of the intrusion against the seriousness of the offence and consideration of whether there are other means to obtain the required information.

   The Council has several specific core functions requiring it to investigate the activities of private individuals, groups and organisations within its jurisdiction, for the benefit and protection of the greater public. Such investigations may require the Council to undertake covert investigatory techniques.

2. In accordance with RIPA and the IPA the Council will only use three covert investigatory techniques for its core functions (details set out below).

   " Directed Surveillance" will only be used for the purposes of the Council's investigations. This is covert non-intrusive surveillance, which is carried out in such a way that the persons subject to the surveillance are unaware that it is or may be taking place. It is undertaken for the purposes of a specific investigation or operation and is conducted in such a manner, that it is likely to result in the obtaining of private information about a person and in circumstances other than by way of an immediate response to events, where it would not be reasonably practicable to seek authorisation for the surveillance. The Council will not undertake surveillance in residential properties or private vehicles.

"Covert Human Intelligence Source" (CHIS) will only be used for the purposes of the Council's investigations. This is an individual, who may or may not reveal their identity, establishes or maintains a personal or other relationship with another person(s), for the covert purpose of obtaining information and disclosing the information to the Council. It is immaterial whether information provided by the source is given voluntarily or the source is tasked by a public authority to obtain the information. A CHIS activity is determined by the manner in which the information was covertly obtained and then subsequently passed on to the Council.

"Communications Data" (CD) includes the 'who', 'when', 'where', and 'how' of a communication, but not the content i.e. what was said or written. The Council may only acquire less intrusive types of CD; "Entity data" (e.g. the identity of the person to whom services are provided) or "Events Data" (e.g. the date and time sent, duration, frequency of communications). The location of the entity or events data at the time the communication is sent or received may also be obtained in appropriate cases.

The Council is prohibited from obtaining "Content Data", the meaning of the communication, (e.g. what the communication says or contains).

3. Applications for CD are subject to independent examination, scrutiny and approval by the Investigatory Powers Commissioner (IPC) through the "Office of Communications Data Authorisations" (OCDA)

4. The Council will continue to maintain a collaboration agreement with the National Anti-Fraud Network (NAFN), to comply with IPA and to ensure any investigation follows best practice. The Council will consult and work with NAFN throughout the application process to ensure the legal basis for all applications are met. NAFN will act as a single point of contact between both the communications service providers and the Council concerning the request and provision of CD

5. The Council will not acquire CD unless an application for authorisation is approved both internally, by designated senior officers and externally, by the Office for Communications Data Authorisations (OCDA).

6. An authorisation to acquire CD will remain in force for 1 month, unless a further application is made by the Council through NAFN and approved by OCDA. The authorisation may be cancelled at any time, by either OCDA or the Council.

7. In respect to applications for communications data made under the IPA, the "applicable crime purpose" must be met concerning all applications for both Entity Data and Events Data. The applicable crime purpose is defined differently in relation to each of these data types. Where the CD sought is

Entity Data, the applicable crime purpose is the prevention or detection of crime or the prevention of disorder. Where the CD is wholly or partly Events Data, the applicable crime purpose is defined as preventing or detecting serious crime (the serious crime threshold). Data relating to Events has the potential to be more intrusive than data relating to Entities.

8. The Council will not utilise a RIPA "Directed Surveillance" or "Covert Human Intelligence Source" authorisation, until an order approving the grant or renewal of an authorisation and/or notice(s) has been granted by a Magistrates' Court.

9. Digital investigation, in particular, the review of 'open source' material which has been placed in the public domain without the expectation of privacy, will not normally require a RIPA authorisation. However, the Council will seek an authorisation to undertake repeated or systematic examinations of open source sites, if such examination is undertaken to build up a picture of a person's activities or lifestyle. The Council will seek a CHIS authorisation if there is to be any interaction with the site host, for example, sending messages and/or making covert enquiries of any kind.

10. Before an authorisation is submitted to a Magistrates' Court it must be internally authorised by an "Authorising Officer" or a "Designated Person" of the Council. Such covert investigatory techniques will only be used where it is considered necessary (e.g. to investigate a suspected crime) and proportionate (e.g. balancing the seriousness of the intrusion into privacy against the seriousness of the offence and whether the information can be obtained by other means). The Council will follow the relevant Codes of Practice on the scope of powers, necessity and proportionality.

    In accordance with the Protection of Freedoms Act 2012 the Council will only submit a "Directed Surveillance" authorisation to the Magistrates' Court for authorisation, for the purpose of preventing crime, where a criminal offence(s) is punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment, is suspected, or if the offence relates to the underage sale of alcohol tobacco or nicotine inhaling products and where the necessity and proportionality tests are met. The Council will ensure that any authorisations and/or notices, which are granted and/or renewed by the Magistrates' Court or by the Council's Authorising Officers, are not utilised beyond the statutory time limits prescribed.

11. The Council will maintain a list of senior officers, who are designated to oversee the covert investigatory techniques specified in paragraph 2, in respect of the Council's internal procedures for authorisations ~~and/or notices~~ under RIPA and IPA, prior to the authorisations and/or notice(s) being approved by a Magistrates' Court or the IPC/ OCDA, and to oversee the process following such approvals until cancellation. A record of approved authorisations and notices will be kept by the Council. The Council's Monitoring Officer, being the Senior Responsible Officer under RIPA, will ensure that the senior officers with responsibility for overseeing any covert

investigatory techniques are at Director, Head of Service, Service Manager or equivalent level of seniority and are aware of the Council's obligations to comply with RIPA and with this policy. Furthermore, all officers who are required to undertake covert techniques will receive appropriate training or be appropriately supervised.

12. The Council may undertake any of the covert investigatory techniques specified in paragraph 2 above, in respect to the prevention and detection of illegal sales of the following age restricted products: Butane, Knives and Fireworks, even though these products do not meet the criteria specified in the Protection of Freedoms Act 2012 and therefore do not attract the protections of RIPA, in respect to these covert investigatory techniques. The Council believes that it is important that the Council's Trading Standards Service is authorised to use any of the aforementioned covert investigatory techniques, in order to undertake enforcement activities in respect of the aforementioned products, even though the Council will not be afforded the protection of RIPA. The Council will ensure that it continues to comply with its obligations under the ECHR (Article 8), by requiring its Trading Standards Service to adhere to the same authorisation procedures for RIPA authorisations and/or notices, except for the requirement to seek the approval of a Magistrates' Court.

13. The Council will ensure that any other covert investigatory techniques, not requiring the approval of a Magistrates' Court, will be subject to the same internal authorisation processes as referred to above.

14. This policy and the procedures for the proper approval of authorisations and/or notice(s), the recording of covert investigatory techniques, will be reviewed when it is considered appropriate to do so.

Reviewed April 2019.
Approved: Cabinet [insert new date]