IPCO
Investigatory Powers Commissioner's Office

PO Box 29105, London
SW1V 1ZU

Ms D Tilley
Chief Executive
Lichfield District Council

1 March 2021

Dear Ms Tilley,

IPCO Surveillance and CHIS inspection of Lichfield District Council

Please be aware that IPCO is not a "public authority" for the purpose of the Freedom of Information Act (FOIA) and therefore falls outside the reach of the FOIA. It is appreciated that local authorities are subject to the FOIA and that they may receive requests for disclosure of our reports. In the first instance the SRO should bring the matter to the attention of the IPCO Data Protection Officer (at: info@ipco.org.uk), before making any disclosure. This is also the case if you wish to make the content of this letter publicly available.

Your Council was recently the subject of a remote inspection by one of my Inspectors, Mrs Samantha Jones. This has been facilitated via MS Teams through your Senior Responsible Officer (SRO), Ms Christie Tims, Head of Governance and Performance. No formal recommendations have been made as a result of this inspection process.

The last inspection of Lichfield Council took place during April 2018, by Mrs Grainne Athorn, who made one formal recommendation:

- *The RIPA Procedure document allows for Lichfield District Council investigators to utilise overt surveillance powers to undertake covert observations online, utilising social media and other sites. In order to ensure this activity is subject to suitable oversight it is recommended that the procedures document should be updated to include control and management mechanisms including: a register of covert profiles used to undertake surveillance; details of who has used these profiles and when; and a record of what information was recorded, which should be made available to the relevant authorising officer for review.*

Litchfield Council does not operate, and at present has no immediate intention to use, covert profiles as part of its investigation strategy. However, whilst discharging this recommendation it is with the caveat that continuing consideration should be given to the oversight and governance of any future covert structures and subsequent evidential capture of material.

It should also be emphasised to staff that personal profiles should not be used for Council business, as it is incumbent on you to ensure the safety and security of the staff. The dangers aligned to using personal social media accounts for business purposes, especially those of a covert nature, should not be underestimated and all staff should be cognisant of their own personal online security and of the vulnerabilities attached to using any insecure or personal online platform.

My Inspector was assured by Ms Tims that the RIPA policy was fully up to date and scheduled to be approved by Elected Members in July, but while non RIPA activity had been reported on a regular basis, this was the first time that policy would be presented since 2018. This represents a failure to comply with paragraph 4.47 of the Home Office Surveillance Code of Practice, as policy should be approved by Elected Members on an annual basis. You should therefore ensure this becomes the usual practice beyond July 2021.

Although your Council has not exercised its powers for many years, it remains of great importance that officers engaged in investigatory or enforcement areas where RIPA considerations are not so immediately apparent, maintain their levels of knowledge and know whom to approach for guidance. It is therefore pleasing to note that relevant external training took place for key officers in 2019 and further training is scheduled for this year.

There have been no authorisations for the use and conduct of a CHIS. This reflects the widespread practice common amongst local authorities of never, or rarely, authorising CHIS. The possibility of status drift was discussed with the SRO in relation to the monitoring of information provided by members of the public, as well as online activity. Ms Tims is alive to the possibility and is confident that sufficient awareness exists amongst staff to be alert to any potential status drift.

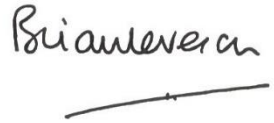
It is understood that your Council is registered with the National Anti-Fraud Network (NAFN) for the purposes of obtaining communications data and although rarely used, is cognisant of the extention of powers introduced by the Investigatory Powers Act 2016 to include details of in and out call data and cell site location. This represents a significant opportunity to enhance investigations, and in addition, registration with NAFN also provides lawful access to other forms of data from the DVLA, Equifax and a variety of other financial/fraud check organisations.

As part of the inspection process, the Council's stance on the review, retention and destruction (RRD) of documentation was also assessed. The Central Register is comprised of an Excel spreadsheet, although as would be expected, no details are currently held. Access is restricted to the Governance team. The data pathways of any material captured by way of an authorisation under the legislation are clear, with product being stored electronically and inbuilt prompts which are flagged to the data owner to ensure compliance with the RRD policy.

Mrs Jones would like to thank Ms Tims for her engagement at a time of unprecedented demands on local authorities. I hope that this video-based inspection has proved to be helpful and constructive. My Office is available to you should you have any queries following the inspection, or at any point in the future. Contact details are provided at the foot of this letter.

I shall be grateful if you would acknowledge receipt of the report within two months.

Yours sincerely,



The Rt. Hon. Sir Brian Leveson
The Investigatory Powers Commissioner