



Investigatory Powers
Commissioner's Office

PO Box 29105, London
SW1V 1ZU

Ms G Beasley
Chief Executive
Cambridgeshire County and Peterborough City Council

1 March 2021

Dear Chief Executive,

IPCO Surveillance and CHIS inspection of Cambridgeshire County and Peterborough City 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 Authorities were recently the subject of a joint remote inspection by one of my Inspectors, [REDACTED]. This was facilitated by Ms Fiona McMillan, Director of Law and Governance, as the Senior Responsible Officer (SRO), and Mr Ben Stevenson, Head of Information Governance and Data Protection Officer, via MS Teams, together with preceding supporting documentation provided. There are no formal recommendations as a result of this inspection process.

There was one previous recommendation emanating from the 2018 inspection conducted by [REDACTED], in relation to revising the draft RIPA policy in line with the agreed amendments. Principally, clarification on the role of a CHIS and the authorisation process, and structured oversight of the use of the internet and social media. This recommendation can be discharged with a slight caveat that the policy still requires reference to paragraphs 4.11 - 4.17 of the Home Office CHIS Code of Practice when using social media.

I note that the Authorities' policies and non RIPA usage are put before the respective Elected Members on an annual basis through the Audit/Audit and Accounts Committees, in accordance with paragraph 4.47 of the Surveillance Code of Practice.

Whilst your Authorities have not exercised their RIPA powers for a considerable period of time, it was clear they are alive to the possibility of online social media research being carried out. This, combined with specific training material and management oversight, should provide assurances that any research undertaken does not drift into surveillance territory without the appropriate authorisation being in place. Continuing consideration should also be given to the oversight and governance of any future covert structures and subsequent evidential capture of material.

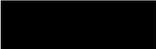
Cambridgeshire and Peterborough have also emphasised to staff within the policy that personal profiles should not be used for council business, and this should be reiterated regularly as it is incumbent on you to ensure the safety and security of the staff. The dangers aligned to using personal social 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.

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

It is understood that your Authorities are registered with the National Anti-Fraud Network (NAFN) for the purposes of obtaining communications data, and do so on an infrequent basis. The extension of powers introduced by the Investigatory Powers Act 2016, to include details of in and out call data and cell site location, 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.

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 an array of training material is available to staff.

As part of the inspection process, your Authorities' stance on the review, retention and destruction (RRD) of documentation was also assessed. The Central Register is comprised of a spreadsheet held by Mr Stevenson. There are clearly defined data pathways for the handling of material captured by way of an authorisation under the legislation. In essence, any investigative files are held within the relevant Service department i.e. Trading Standards, until they are shared with Legal Services. There is an ICT Security policy which covers the handling of all material held, with specific responsibility for each Head of Service to trigger the review and destruction process.

 would like to thank both Ms McMillan and Mr Stevenson for their engagement at a time of increased 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