Appendix B

POLICY DOCUMENT ON THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA FROM COMMUNICATION SERVICE PROVIDERS

Policy approved by CABINET
on

[ ] July 2017

CONTENTS

REGULATION OF INVESTIGATORY POWERS ACT 2000 POLICY IN RELATION TO ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA FROM COMMUNICATION SERVICE PROVIDERS

1 INTRODUCTION

1.1 The Regulation of Investigatory Powers Act 2000 (the Act) regulates the acquisition and disclosure of communications data from communication service providers by a number of bodies, including Local Authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that law enforcement and security agencies have the powers they need to do their job effectively.

1.2 Whilst the Act also regulates directed surveillance and of the use of Covert Human Intelligence Sources (CHIS), the acquisition of communications data is overseen by the Interception of Communications Commissioner (the Commissioner). The Commissioner does not oversee surveillance and CHIS issues. This policy therefore only relates to the part of the Act that is the responsibility of the Commissioner.

1.3 This policy applies to the acquisition and disclosure of communications data from communication service providers under the Act.

1.4 Hertfordshire County Council (Council, we, us) is included within the Act's framework with regard to the acquisition and disclosure of communications data but only for the purpose of the prevention and detection of crime. Hertfordshire Fire and Rescue Service may access communications data about the maker of an emergency call within one hour of its termination to enable the provision of emergency assistance. Such access is outside the provision of the Act (it is under the Communications Act 2003) and therefore outside the scope of this policy

1.5 In summary, the Act requires that when the Council undertakes the acquisition or disclosure of communication data, these activities must be authorised by a designated person when the relevant criteria are satisfied and the authorisation must be approved by a Justice of the Peace.

1.6 For the avoidance of doubt, Local Authorities such as Hertfordshire County Council cannot apply for the content of communications nor 'intercept' communications and therefore cannot apply to listen into telephone conversations or read emails. Local Authorities can only apply for communications data (see 4. below for an explanation of 'communications data').

1.7 The Home Office publish a code of practice (the code) pursuant to section 71 of RIPA, for the Acquisition and Disclosure of Communications Data (March 2015). https://www.gov.uk/government/publications/code-of-

practice-for-the-acquisition-and-disclosure-of-communications-data This code applies to public authorities and the code and its principles will be followed by us. This policy should be read in conjunction with current guidance issued by the Home Office and the Interceptions of Communications Commissioner (2016). https://osc.independent.gov.uk/wp-content/uploads/2013/07/OSC-Procedures-Guidance-July-2016.pdf

1.8 The Investigatory Powers Act received Royal assent on 29 November 2016 and when it comes in to force this Policy will be updated.

2 ROLES

2.1 The legislation creates a number of roles:

2.2 The Senior Responsible Officer ensures the integrity of the process within the Local Authority, compliance with the Act and the Code of Practice, oversight of the reporting of errors to the Commissioner, engagement with the inspectors when they conduct inspections and where necessary oversight of the implementation of post-inspection action plans. The Senior Responsible Officer is the Chief Legal Officer of Hertfordshire County Council.

2.3 The Designated Person is a person holding a prescribed office who considers the application and either grants or rejects the application in accordance with the legislation and the code. The Designated Person(s) are the Assistant Chief Legal Officer Environment and Dispute Resolution and the Head of Commercial and Property Law.

2.4 The single point of contact (SPoC) is a group of trained, externally accredited individuals who facilitate the effective co-operation between us and the communication service providers. We can use the services of an alternative SPoC facility and we use the SPoC facility of the National Anti-Fraud Network (NAFN) of which we are a member.

2.5 The applicant is the person involved in conducting the investigation.

2.6 The person within the Council with responsibility for RIPA is the Deputy Director of Community Protection.

3 PURPOSE

3.1 The Act prescribes the purpose for which we can access communications data. We will comply with those requirements.

3.2 The only purpose for which we can access such data is for the purpose of preventing or detecting crime or of preventing disorder. The exception is

the Fire and Rescue service who may also access such data in the interests of public safety.

3.3 Any postal or telecommunications operator is referred to as a communications service provider (CSP). All applications for communications data from a CSP must follow this policy.

4 COMMUNICATIONS DATA

4.1 Communications data is divided into three categories. Note that the content of communications is not communications data. The categories are defined in the legislation. Briefly:

4.2 Traffic data is information that identifies the person to or from whom the communication is transmitted or the location. Such information is not available to us.

4.3 Service use information is data relating to the use made by any person of a postal or telecommunications service, such as itemised phone bills. We may access such information in accordance with the legislation and code

4.4 Subscriber information is information about the person to whom the communications service provider has provided the service, so the name and address of someone who may own a specific mobile phone. We may access such information in accordance with the legislation and code.

5 CONSIDERATIONS

5.1 Authorisation and renewal is a 2 stage process. The first being the internal authorisation, which if successful then has to go before a court for judicial approval.

5.2 The applicant must apply for the data through NAFN and at the same time must forward a copy of the application to the Designated Person who will check the application and seek further information if required. Once approved by NAFN and Legal Services, judicial approval must be sought before the data can be obtained from NAFN.

5.3 The Designated Person will need to be made aware of particular sensitivities in the local community with respect to the data applied for and the purpose of the investigation. In addition, as required by the legislation they must have regard to whether the acquisition is necessary and proportionate and the degree, if any, of interference with the privacy of persons other than the direct subject(s) of the application.

6 FORMS AND KEEPING OF RECORDS

6.1 The Community Protection Directorate shall be responsible for ensuring the authority has the appropriate forms and records to comply with the requirements of the legislation and code. They are responsible for retaining and keeping secure the applications and product as detailed in the code.

6.2 Further guidance is available from the procedure: Procedure Document on the Regulation of Investigatory Powers Act 2000 Communications Data, which can be found on the intranet.

7 COMPLAINTS

7.1 The Authority's complaints procedure applies to complaints about activities within the scope of this policy.

7.2 The Act establishes an independent Tribunal, called the Investigatory Powers Tribunal that has full powers to investigate and decide on any case within its jurisdiction.

8 SCRUTINY

8.1 This policy must be examined by Members on a yearly basis to be approved as fit for purpose.