STRONGER together

Lewes District Council

EASTBOURNE Borough Council

Working in partnership with **Eastbourne Homes**

Document name:	Policy on the Acquisition of Communications Data under Part 3 of the Investigatory Powers Act 2016
Document type:	Policy

Authority(ies) covered:	Aligned
Responsible (Executive Lead):	Councillor James MacCleary, Leader of LDC; Cllr David Tutt, Leader of EBC
Accountable (Operational Lead):	Oliver Dixon, Senior Responsible Officer
Version (e.g. first draft, final report):	Final report following IPCO inspection recommendations from June 2022
Approved by:	LDC Audit and Standards and EBC Audit and Governance Committees
Date of publication:	November 2022
Revision due:	November 2023
Final Equality and Fairness Analysis (EaFA) report approved by:	Not applicable
Date final EaFA report approved:	Not applicable

Contents

1. Introduction

1.1 Part 3 of the Investigatory Powers Act 2016 ('the Act') permits certain public bodies to acquire specified types of communications data in limited circumstances, subject to prior authorisation granted in accordance with the Act. Part 3 applies principally to the police and central government departments and agencies, including defence, security and intelligence bodies. The power it grants to local authorities is less extensive, limiting the acquisition of data to cases involving the prevention or detection of serious crime (see further at 3.2).

1.2 The communications data which, in defined circumstances, local authorities are permitted to obtain under the Act is known as 'entity data' and 'events data'. Their scope is explained in section 2 below but, in brief, data of this nature can identify who a suspected offender has been in communication with via their telephone or e-mail, as well as where that communication was made or received. The data may therefore be of real investigative benefit.

1.3 The legal framework for this policy is the Act and statutory guidance contained in the Home Office Code of Practice on Communications Data (November 2018).

2. Communications data

2.1 In the Act and this policy, the term 'communications data' means 'entity data' and 'events data' and includes the 'who', 'when', 'where', and 'how' of a communication but not the content i.e. what was said or written.

2.2 **Entity data** means any data which—

(a) is about—
  (i) an entity (a person or thing such as a phone, tablet or computer),
  (ii) an association between a telecommunications service and an entity, or

(iii) an association between any part of a telecommunication system and an entity,

(b) consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity's location), and

(c) is not events data.

2.3 Entity data covers information about a person or thing, and about links between a telecommunications system and a person or thing that identifies or describes the person or thing. This means that individual communication devices such as phones, tablets and computers are entities. The links between a person and their phone are therefore entity data but the fact of or information about communications between devices on a network at a specific time and for a specified duration would be events data.

2.4 Examples of entity data include:

- Subscriber checks such as “who is the subscriber of phone number 01234 567 890?”, “who is the account holder of e-mail account example@example.co.uk?” or “who is entitled to post to web space www.example.co.uk?”

- subscribers’ or account holders’ account information, including names and addresses for installation, and billing including payment method(s), details of payments;

- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services;

- information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes; and information about selection of preferential numbers or discount calls.

2.5 **Events data** is more intrusive and means any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time.

2.6 Events data includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning, of the communication.

2.7 Events data can also include the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made. It covers

electronic communications including internet access, internet telephony, instant messaging and the use of applications.

2.8 Examples of events data include, but are not limited to:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);
- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed)
- itemised telephone call records (numbers called);
- itemised internet connection records;
- itemised timing and duration of service usage (calls and/or connections);
- information about amounts of data downloaded and/or uploaded;
- information about the use made of services which the user is allocated or has subscribed to (or may have subscribed to) including conference calling, call messaging, call waiting and call barring telecommunications services.

3. <u>Extent of data acquisition powers</u>

3.1 The Council's acquisition of communications data under Part 3 of the Act will be a justifiable interference with an individual's human rights under Article 8 (the right to respect for privacy and family life) and, in certain circumstances, Article 10 (right to freedom of expression) of the European Convention on Human Rights **only** if the conduct being authorised or required to take place is:

(i) **necessary** for the purposes of a specific investigation or operation – see further at 3.2; and

(ii) **proportionate** – see further at 3.4.

3.2 When applying for authorisation to acquire communications data, the Council must believe the acquisition is necessary for the purpose of the **prevention or detection of serious crime**.

3.3 'Serious crime' means:

- an offence for which an adult is capable of being sentenced to one year or more in prison;
- any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal;
- any offence committed by a body corporate;
- any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy.

3.4 The Council must also believe the acquisition to be proportionate to what is sought to be achieved by obtaining the specified communications data – that the conduct is no more than is required in the circumstances.

3.5 The Council has no power to obtain the **content** of a communication.

4. <u>Roles in applying for and granting authorisation</u>

4.1 Acquisition of communications data under the Act involves four roles:

- the applicant – see 4.2;
- the single point of contact ('SPoC') – see 4.3;
- the Senior Responsible Officer – see 4.4;
- the authorising individual – see 4.5.

4.2 The **applicant** is a Council officer involved in conducting or assisting an investigation or operation who makes an application in writing or electronically for the acquisition of communications data. For this specialised function, the role would normally be reserved to a counter-fraud officer but the Chief Finance Officer may – where he/she considered it appropriate – authorise a named and suitably qualified officer from a different specialism to make an application.

4.3 The **SPoC** is an individual trained to facilitate the lawful acquisition of communications data and effective co-operation between the body applying for authorisation (the Council) and the body with statutory power to grant the authorisation (the Office for Communications Data Authorisations – 'OCDA' – who act on behalf of the Investigatory Powers Commissioner – 'IPC'). In

respect of local authorities, the SPoC role is performed by the National Anti-Fraud Network ('NAFN') – see further at 5.2.

4.4 The **Senior Responsible Officer** ('SRO') must be a member of the corporate management team. The designated SRO for Lewes and Eastbourne Councils is the Head of Legal Services, which is consistent with that role's SRO functions for RIPA matters.

The SRO is responsible for:

- the integrity of the process in place within the Council to acquire communications data;
- compliance with Part 3 of the Act and with the Home Office code of practice on communications data;
- oversight of the reporting of errors to the ('IPC') and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- ensuring the overall quality of applications submitted to the Council's SPoC;
- engagement with the IPC's inspectors when they conduct their inspections; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the IPC.

4.5 For local authorities, the **authorising individual** is OCDA, acting on behalf of the IPC.

5. <u>Procedure for applying for authorisation to acquire communications data</u>

5.1 The procedure adopted by the Council in applying for an authorisation and in implementing any authorisation granted must comply with the Act and the Home Office Code of Practice, which include the measures set out in 5.2 to 5.6 below.

5.2 The Council must use NAFN's SPoC services for any application it wishes to submit for authorisation. Following SPoC evaluation, authorisation to proceed may only be provided by OCDA.

5.3 Council applicants are required to consult a NAFN SPoC throughout the application process. The accredited SPoCs at NAFN will scrutinise the applications independently and will provide advice to the Council, ensuring it acts in an informed and lawful manner.

5.4 In addition to involving the NAFN SPoC, the Council must ensure that someone – "the verifying officer" – of at least the rank of the Council's SRO is aware the application is being made before it is submitted to an authorising

officer in OCDA. For Lewes and Eastbourne Councils, the verifying officer is the Chief Finance Officer, and this nomination will be notified to NAFN.

5.5 NAFN is responsible for submitting the application to OCDA on behalf of the Council.

5.6 The Council may not make an application that requires the processing or disclosure of internet connection records for any purpose.

5.7 The Council must cease any and all authorised acquisition of communications data as soon as the OCDA authorisation is cancelled or at the expiry of one month following the date of authorisation (whichever is sooner).

6. Training for officers with designated roles

6.1 The Council must provide an adequate level of initial and refresher training to relevant officers to enable them to perform the role of applicant (see 4.2 above), SRO (see 4.4 above) or verifying officer (see 5.4 above), as applicable.

6.2 The Council may enter into formal or informal partnership arrangements with other local authorities for the purpose of procuring region-wide training, in the interests of efficiency and effectiveness.

7. Records to be kept

7.1 The Council must keep records of the appropriate matters set out in Chapter 24 of the Home Office Code of Practice, including the number of applications it submits to the SPoC for the acquisition of communications data.

7.2 Under Chapter 24, the Council's SPoC has record keeping responsibilities of its own, for example recording how many applications it forwards to OCDA for authorisation and, of these, the number granted and declined.

7.3 All material obtained through the Acquisition of Communications Data, including all copies, extracts and summaries must be handled and stored securely on Council systems to reduce the risk of loss or theft. Access to the material must be restricted to Council officers undertaking the operation or where necessary as part of the retention process or legal proceedings.

7.4 All material which could be relevant to a pending or future criminal or civil proceedings must be retained in accordance with established disclosure requirements detailed in the Criminal Procedure and Investigations Act 1996.

7.5 All communication data obtained, including copies, extracts and summaries should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer required in accordance with the Council's Data Retention, Storage and Disposal Policy.

8. Policy review and member oversight

8.1 The first version and any substantive review of this policy must be approved by the Audit and Governance Committee (in respect of EBC) or the Audit and Standards Committee (in respect of LDC).

8.2 Minor or purely technical amendments to the policy may be implemented by the SRO under delegated powers.

8.3 A report on any use the Council makes of its data communications acquisition powers will be submitted annually to the A & G Committee or A & S Committee as applicable.

8.4 At national level, the Investigatory Powers Commissioner (IPC) provides comprehensive oversight of the use of the powers contained within the Act and adherence to the practices and processes described by the Home Office Code of Practice.

8.5 The IPC ensures compliance with the law by inspecting public authorities and investigating any issue which they believe warrants further independent scrutiny. The Council will engage and co-operate in full with any IPC inspection or scrutiny into the Council's proper or improper exercise of powers under the Act. Further, the Council will promptly act on any IPC recommendations for policy and procedural improvement or rectification.