APPENDIX C

London Borough of Hammersmith & Fulham

Investigatory Powers Act 2016
Policy for Use of Communications Data

February 2020

Reviewed July 2023

CONTENTS

1. INTRODUCTION 3
2. WHAT IS COMMUNICATION DATA? 3
Entity Data: 3
Events Data: 4
3. AUTHORISATIONS 4
Approved Rank Officer (ARO) 5
Single Point of Contact (SPoC) 5
Senior Responsible Officer (SRO) 5
4. NECESSITY AND PROPORTIONALITY 6
Necessity 6
Proportionality 6
Collateral Intrusion 7
5. DURATION OF AUTHORISATIONS – REVIEW, RENEWAL AND CANCELLATION 7
6. RECORD OF AUTHORISATIONS 8
7. HANDLING AND DISCLOSURE OF MATERIALS AND DOCUMENTS 8
8. ERRORS 9
9. TRAINING 9
10. OFFENCES FOR NON-COMPLIANCE WITH IPA 10
11. FURTHER GUIDANCE 10

1. INTRODUCTION

1.1. The Investigatory Power Act (IPA) 2016. The IPA builds on, and supersedes parts of, the Regulation of Investigatory Powers Act (RIPA) 2000. The IPA has granted law enforcement and public authorities updated powers to access communications data for legitimate purposes. It requires a local authority to follow a specific procedure and obtain independent authorisation before obtaining communications data.

1.2. The IPA does NOT allow local authorities to intercept communications (e.g. bugging of telephones etc.). Local authorities are NOT allowed to intercept the content of any person's communications or to access internet connection records for any purpose. It is an offence to do so without lawful authority.

1.3. Failure to comply with the IPA may mean the Council's actions are unlawful and amount to a criminal offence. It may also mean that evidence obtained would be inadmissible in court proceedings and jeopardise the outcome of the case, It could also lead to a claim for damages against the Council.

1.4. Officers of the London Borough of Hammersmith & Fulham who want to access communications data must do so in accordance with this policy.

2. WHAT IS COMMUNICATION DATA?

2.1. The term communications data embraces the 'who', 'when' and 'where' of communication but not the content. It is information about a communication whether it originated from the internet, the postal services, or a telecommunications service.

2.2. Communications data captures who an individual is communicating with, when and where they are communicating, as well as the type of communication and device used.

2.3. There are 2 types of communication data "Entity data" and/or "Events data".

2.3.1. Entity Data:

This relates to the association between an entity and a telecommunications service or telecommunications system or could be description and identification of an entity. Basically, data about a person or thing (such as a device) or information linking them.

For example:

- Billing information such as name, address and bank details of the subscriber
- Phone numbers or other identifiers linked to customer accounts
- Customer address provided to a communications service provider
- IP address allocated to an individual by an internet access provider
- Account holder details for an email account

Entity Data is less intrusive than Events Data and can be obtained for the prevention and detection of any crime.

2.3.2. Events Data:

This means any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunications system where the event consists of one or more entities engaging in a specific activity at as specific time.

For example:

- The type of communication, time sent and duration
- The fact that someone has sent or received an email, phone call, text or social media message
- The location of a person when they made a mobile phone call or the Wi-Fi hotspot their phone was connected to

Events Data can be ONLY be obtained for the prevention and detection of 'Serious Crime'. Which includes:

- A crime involving violence or substantial financial gain
- An offence that can attract a sentence of 12 months or more imprisonment
- An offence which involves, as an integral part of it, a breach of a person's privacy or the sending of a communication
- Offences committed by a corporate body

3. AUTHORISATIONS

3.1. No Council Officer may obtain any form of communication data **unless and until** they have obtained the proper authorisation.

3.2. This means that:

- An Approved Rank Officer (ARO) must be consulted;

- The application must be sent to the Council's Single Point of Contact (SPoC); and
- The application must be approved by the Office for Communication Data Authorisations (OCDA).

3.3. The following types of conduct may be authorised:

- Conduct to obtain communications data - including obtaining data directly or asking any person believed to be in possession of or capable of obtaining such data to obtain and disclose it; and/or
- Giving of a notice – requiring a telecommunications operator to obtain and disclose the required data.

Approved Rank Officer (ARO)

3.4. The following Council Officers are empowered to act as Designated Persons for applications for communications data:

- Andy Hyatt: Tri Borough Head of Fraud
- Valerie Simpson: Strategic Lead for Environmental Health and Regulatory Services
- Matthew Hooper: Chief Officer for Safer Neighbourhoods & Regulatory Services

Single Point of Contact (SPoC)

3.5. The National Anti-Fraud Network (NAFN) provides a SPoC service to the Council. All applications for communication data must be submitted to NAFN.

3.6. All forms to access communications data are covered by the online application process through NAFN.

3.7. Prospective applicants and are required to register on the NAFN Website.

3.8. Once registered, applications for the acquisition of communications data can be managed through the Focus 112 Portal.

Senior Responsible Officer (SRO)

3.9. The Act also requires the Council to have an SRO who is responsible for ensuring compliance with the Act and Code of Guidance and the integrity of the process in place within the authority to acquire communications data.

3.10. Bram Kainth, Executive Director of Place, acts as the SRO for the Council.

3.11. Further details of roles and responsibilities are set out in Appendix 1.

4. NECESSITY AND PROPORTIONALITY

4.1. A local authority is required to show that an interference with an individual's right to privacy is justifiable, to the extent that it is both ***necessary and proportionate***.

Necessity

4.2. Applications to obtain Communications Data should only be made where it is **necessary** for an "applicable **crime purpose**".

4.3. Applications can be made for **'entity data'** where the purpose of obtaining the data is for the **prevention and detection of crime or prevention of disorder.** This definition permits the obtaining of entity data for any crime, irrespective of seriousness or for preventing disorder.

4.4. Applications for **'events data'**, requires a higher threshold, and applications for this data should only be made were the purpose is the 'prevention and detection of **serious crime'** as outlined in section 2.3.2.

The application must explain:

- The crime or event under investigation;
- The person whose data is sought, such as a suspect AND description of how they are linked to the crime;
- The communications data sought, such as a telephone number or IP address, and how this data is related to the person and crime; **and**
- The link between these 3 points to demonstrate it is necessary to obtain communications data.

Proportionality

4.5. All applications for communication data must also demonstrate that the means of obtaining the information is **proportionate** to what it is sought to achieve.

4.6. In effect, any intrusion into individual's privacy should be no more than is absolutely necessary.

4.7. The applicant should demonstrate how they reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the proverbial 'sledgehammer to crack a nut').

4.8. Applications should contain the following:

- An outline of how obtaining the data will benefit the investigation. The relevance of the data being sought should be explained and anything which might undermine the application;
- The relevance of time periods requested;
- How the level of intrusion is justified against any benefit the data will give to the investigation. This should include consideration of whether less intrusive investigations could be undertaken;
- A consideration of the rights (particularly to privacy and, in relevant cases, freedom of expression) of the individual and a balancing of these rights against the benefit to the investigation;
- Any details of what **collateral intrusion** may occur and how the time periods requested impact on the collateral intrusion, if applicable;
- Where no collateral intrusion will occur, such as when applying for entity data, the absence of collateral intrusion should be noted.

Collateral Intrusion

4.9. As part of this process an assessment should be made of the risk of what is termed '*collateral intrusion'* - intrusion into the privacy of persons other than those that are the subjects of investigation.

4.10. Measures should be taken, wherever possible, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation.

5. DURATION OF AUTHORISATIONS – REVIEW, RENEWAL AND CANCELLATION

5.1. An authorisation will be valid for a maximum of one month from the date of OCDA approval. This means that the conduct authorised should have been commenced or the notice served within that month. All authorisations and notices must relate to the acquisition or disclosure of information for a specific date or period.

5.2. Applications can be renewed before the date on which they would cease to have effect provided they continue to meet the relevant criteria. OCDA approval is required for all renewals. The renewal takes effect on the day on which the authorisation would have expired and continues for a one-month period.

5.3. Renewal may be appropriate where there is a continuing requirement to acquire or obtain data that will or may be generated in the future. The reasoning for seeking renewal should be set out by an applicant in an addendum to the application on which the authorisation or notice being renewed was granted or given.

5.4. A note should be made of the date and time of applications for renewal.

5.5. An Authorisation must be cancelled if at any time after they are given it comes to the Council's notice that it is no longer necessary or proportionate to what was sought to be achieved. The council is under a duty to notify NAFN immediately.

6. RECORD OF AUTHORISATIONS

6.1. Applications, authorisations, copies of notices, and records of the withdrawal and cancellation of authorisations, must be retained in written or electronic form for a minimum of 3 years and ideally 5 years. A record of the date and, when appropriate, the time each notice or authorisation is granted, renewed or cancelled.

6.2. All records are stored and retained by NAFN online for inspection by the Investigatory Powers Tribunal (IPT).

7. HANDLING AND DISCLOSURE OF MATERIALS AND DOCUMENTS

7.1. The ARO should retain IPA related documents for a period of 3 years. However, where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

7.2. Material obtained or produced during the course of investigations subject to IPA authorisations should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 2018, the Freedom of Information Act 2000, any other legal requirements, including those of confidentiality, and the Council's policies and procedures currently in force relating to document retention.

7.3. All IPA records, whether in original form or copies must be kept in secure locked storage when not in use.

7.4. All electronic copies of IPA records, as well as the Central RIPA register, must be stored and shared in accordance with point 7.3. and password protected.

7.5. If there is any doubt regarding information handling and confidentiality, advice should be sought from the RIPA Coordinator or Legal Services.

8. ERRORS

8.1. Where any error occurs in the granting of an authorisation, or because of any authorised conduct, a record should be kept.

8.2. Where the error results in communications data being obtained or disclosed incorrectly, a report must be made to the IPC by whoever is responsible for it. E.g. The telecommunications operator must report the error if it resulted from them disclosing data not requested, whereas if the error is because the public authority provided incorrect information, they must report the error. The SRO would be the appropriate person to make the report to the IPC.

8.3. Where an error has occurred before data has been obtained or disclosed incorrectly, a record will be maintained by the public authority. These records must be available for inspection by the IPC.

8.4. A non-exhaustive list of reportable and recordable errors is provided in the Code of Practice.

8.5. There may be rare occasions when communications data is wrongly obtained or disclosed and this amounts to a “serious error”. A serious error is anything that “**caused significant prejudice or harm to the person concerned**” It is insufficient that there has been a breach of a person’s human rights.

8.6. In these cases, the public authority which made the error, or established that the error had been made, must report the error to the SRO and the IPC.

8.7. When an error is reported to the IPC, the IPC may inform the affected individual subject of the data disclosure, who may make a complaint to the IPT. The IPC must be satisfied that the error is a) a serious error AND b) it is in the public interest for the individual concerned to be informed of the error.

8.8. Before deciding if the error is serious or not the IPC will accept submissions from the Public Authority regarding whether it is in the public interest to disclose. For instance, it may not be in the public interest to disclose if to do so would be prejudicial to the prevention and detection of crime.

9. TRAINING

9.1. Officers requesting communication data should have an appropriate accreditation or be otherwise suitably qualified or trained. ARO's will have received training that has been approved by the SRO.

9.2. All training will take place at reasonable intervals to be determined by the SRO, but it is envisaged that an update will usually be necessary following legislative or good practice developments or otherwise every 12 months.

9.3. A log will be kept recording all training received by officers involved in IPA. This training log will be stored alongside the Central RIPA Register.

10. OFFENCES FOR NON-COMPLIANCE WITH IPA

10.1. It is an offence for a person in a public authority knowingly or recklessly to obtain communications data from a telecommunications operator or postal operator without lawful authority (section 11 of IPA 2016).

10.2. The roles and responsibilities laid down for the SRO and SPoC are designed to prevent the knowing or reckless obtaining of communications by a public authority without lawful authorisation. Adherence to the requirements of the Act and the Code, including procedures detailed in this Policy, will mitigate the risk of any offence being committed.

10.3. An offence is not committed if the person obtaining the data can show that they acted in the reasonable belief that they had lawful authority.

10.4. It is not an offence to obtain communications data where it is made publicly or commercially available by a telecommunications/postal operator. In such circumstances the consent of the operator provides the lawful authority. However, public authorities should not require, or invite, any operator to disclose communications data by relying on this exemption.

11. FURTHER GUIDANCE

11.1. This policy must be read in conjunction with current Home Office guidance.

Full Codes of Practice can be found on the Home Office website

https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice

Note the current code is dated November 2018 and will be updated to be fully up to date with changes in legislation.

Legal advice can be obtained from Legal Services, contact:
Janette Mullins, Chief Solicitor (Litigation and Social Care), 0208 753 2744

APPENDIX 1 – ROLES AND RESPONSIBILITIES

Obtaining communications data under the Act involves five roles:

- Applicant;
- Approved rank officer (ARO);
- Single point of contact (SPoC);
- Authorising agency (OCDA); and
- Senior Responsible Officer in a Public Authority (SRO).

Applicant

- A person involved in conducting or assisting an investigation or operation within the Council who makes an application in writing or electronically to obtain communications data.

Approved Rank Officer (ARO)

- A person who is a manager at service level or above within the Council. The ARO's role is to have an awareness of the application made by the Applicant and convey this to the SPoC.

- The ARO does not authorise or approve any element of the application and is not required to be "operationally independent".

- The AROs for the Council are identified in section 3.4. of this Policy and shall be the only officers within the Council who act as an ARO in accordance with the procedures set out in this Policy.

- ARO's must ensure that staff who report to them follow this Policy and do not obtain communication data without first obtaining the relevant authorisations in compliance with this Policy.

- ARO's must have current working knowledge of human rights principles, specifically those of necessity and proportionality.

- ARO's must attend training as directed by the SRO.

Single Point of Contact (SPoC)

- An individual trained to facilitate the lawful obtaining of communications data and effective co-operation between a public authority, the Office for Communications Data Authorisations (OCDA) and telecommunications and postal operators. To

become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued the relevant SPoC unique identifier.

- The Council is a member of the National Anti-Fraud Network (NAFN) and use NAFN's shared SPoC service. NAFN is an accredited body for the purpose of providing data and intelligence under the IPA for all public bodies.

Authorising Agency (OCDA)

- The independent body responsible for the authorisation and assessment of all Data Communications applications under the Act.

- They undertake the following roles:
    - Independent assessment of all Data Communications applications;
    - Authorisation of any appropriate applications; and
    - Ensuring accountability of Authorities in the process and safeguarding standards.

Senior Responsible Officer (SRO)

- A person of a senior rank, a manager at service level or above within the Public Authority.

- The SRO is identified at section 3.10 of this Policy responsible for:

    - The integrity of the process in place within the public authority to obtain communications data;
    - Engagement with authorising officers in the Office for Communications Data Authorisations (where relevant);
    - Compliance with Part 3 of the Act and with the Code of Practice, including responsibility for novel or contentious cases;
    - 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 OCDA;
    - Engagement with the IPC"s inspectors during inspections; and
    - Where necessary, oversight of the implementation of post-inspection action plans approved by the IPC.

Head of Community Safety (HoCS)

- The Head of Community Safety will report on the use of IPA to the Hammersmith & Fulham Council Community Safety and Environment Policy

and Accountability Committee annually, and to other panels and committees (where appropriate).