INVESTIGATORY POWERS ACT 2016:

COMMUNICATIONS DATA

HARINGEY POLICY

www.haringey.gov.uk

Contents

Policy History					
Version	Summary of Change	Contact	Implementation Date	Review Date	EqIA Date
1.0	New policy following the coming into force of the IPA 2016.	Business Manager for Corporate Governance	November 2019	October 2020	October 2019

Links and dependencies
Corporate Anti-Fraud Policy and Fraud Response Plan Whistleblowing Policy Sanctions Policy Anti-Money Laundering Policy Anti-Bribery Policy Employee Code of Conduct

Related forms
IPA Communications Data Authorisation IPA Application for Communications Data

1. Overview of IPA

1.1 The Investigatory Powers Act ("IPA") 2016 regulates access to communications data. It requires local authorities to follow a specific procedure and obtain independent authorisation before obtaining communications data.

1.2 Failure to comply with IPA 2016 may mean that the Council's actions are unlawful and amount to a criminal offence. It may also mean that the evidence obtained would be inadmissible in court proceedings and jeopardise the outcome of such proceedings. Such action could also lead to a successful claim for damages against the Council.

1.3 It is in the public interest for criminal investigations to be undertaken efficiently and promptly. Therefore, where proportionate and necessary, the IPA should be used as a tool to advance criminal investigations accordingly.

1.4 This policy should be read in conjunction with the latest Home Office Code of Practice on Communications Data.

Please note that, at the time of writing, the code published in November 2018 is not fully up to date with legislative changes. A new code is expected to be published soon. Therefore, legal services should always be consulted if an officer is considering obtaining communication data.

1.5 Further information on IPA can be obtained from the Investigatory Powers Commissioner's Office, the body responsible for overseeing the use of investigatory powers.

1.6 The procedure for use of surveillance and covert human intelligence sources (CHIS) is dealt with under the Regulation of Investigatory Powers Act 2000 and in a separate policy.

2. Policy statement

2.1 Haringey Council will apply the principles of IPA 2016 when obtaining communication data. In doing so, the Council will also take into account its duties under other legislation, in particular the Human Rights Act 1998, Data Protection Act 2018 and its common law obligations.

2.2 The purpose of this policy is to ensure that:

- an individual's right to privacy is not unlawfully breached;
- the investigation is necessary and proportionate to the alleged offence;
- proper authorisations are obtained for obtaining of communications data; and
- the proper procedures are followed.

3. Communications data

3.1 Communications data includes the 'who', 'when', 'where', and 'how' of a communication but not the content i.e. what was said or written. It 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.

3.2 Communications data can include the address to which a letter is sent, the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device.

3.3 It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.

3.4 Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services including telecommunications or postal services.

3.5 Communications data is defined as 'entity data' and/or 'events data'. These terms are defined in the Code of Practice on Communications Data. However, in essence:

Entity data is data about a person of thing (such as a device) or information linking them, that can change over time. For example, information about which person is the account holder of email account example@example.co.uk.

Events data concerns specific communications. For example, information about who sent a particular email or the location of a mobile phone when a call was made. There is a higher threshold to obtain events data than for entity data.

4. Data that cannot be requested under IPA 2016

4.1 The Council does not have legal power under IPA 2016 to:

- Intercept communications data;
- Access the content of data communications e.g. the content of text messages, emails etc.;
- Access internet connection records.

5. Authorisations

5.1 It is crucial that the obtaining of communications data is properly authorised. No officer may seek to obtain any form of communication data unless he has obtained the proper authorisation to do so, i.e.

- An Approved rank officer (ARO) must be consulted.
- The application must be provided to the Single Point of Contact (SPoC).
- The application must be approved by the Office for Communications Data Authorisations (OCDA).

5.2 Where an authorisation to obtain communications data has been granted, persons within a public authority may engage in conduct relating to a postal service or telecommunication system, or to data derived from a telecommunication system, to obtain communications data.

5.3 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.

5.4 In the case of Haringey Council the obtaining of communications data will be facilitated through our membership of the National Anti-Fraud Network (NAFN), which provides a comprehensive single point of contact (SPoC) service.

5.5 It will be the responsibility of NAFN to ensure all requests to a telecommunications/ postal operator for communications data, pursuant to the granting of an authorisation, comply with the requirements of the Code of Practice.

6. Roles and responsibilities

6.1 Obtaining communications data under the Act involves five roles:

1) Applicant;
2) Approved rank officer (ARO);
3) Single point of contact (SPoC);
4) Authorising agency (OCDA);
5) Senior Responsible Officer in a Public Authority (SRO).

Applicant

6.2 The applicant is a person involved in conducting or assisting an investigation or operation within a relevant public authority who makes an application in writing or electronically to obtain communications data.

6.3 Any person in a public authority which is permitted to obtain communications data may be an applicant, subject to any internal controls or restrictions put in place within public authorities.

Approved rank officer (ARO)

6.4 The Approved Rank Officer is a person who is a manager at service level or above within the Public Authority. The ARO's role is to have an awareness of the application made by the Applicant and convey this to the SPoC.

6.5 The ARO does not authorise or approve any element of the application and is not required to be 'operationally independent'. The AROs for Haringey Council are identified in **Annex A.**

Single point of contact (SPoC)

6.6 The SPoC is 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.

6.7 Public authorities are expected to provide SPoC coverage for all reasonably expected instances of obtaining communications data. Haringey Council is a member of the National Anti-Fraud Network (NAFN). NAFN is an accredited body for the purpose of providing data and intelligence under the IPA for all public bodies. As part of their portfolio they offer a comprehensive SPoC service.

Authorising agency (OCDA)

6.8 The Office for Communications Data Authorisations (OCDA) is the independent body responsible for the authorisation and assessment of all Data Communications applications under the Act. The They undertake the following roles:

- Independent assessment of all Data Communications applications.
- Authorisation of any appropriate applications.
- Ensuring accountability of Authorities in the process and safeguarding standards.

Senior responsible officer (SRO)

6.9 The Senior Responsible Officer (SRO) is a person of a senior rank, a manager at service level or above within the Public Authority. The SRO for Haringey Council is identified in **Annex A**.

6.10 The SRO is 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.

7. Necessity test

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

7.2 This allows for applications to 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.

7.3 Applications for **'events data'**, previously referred to as service or traffic data, requires a higher standard, and applications for this data should only be made were the purpose is the 'prevention and detection of **serious crime**'. Serious crime is defined in Section 86(2A) of IPA 2016, and includes, but is not limited to:

- Any crime that provides the potential for a prison sentence of imprisonment for 12 months or more (Either way or indictable offences);
- Offences committed by a corporate body;
- Any offence involving, **as an integral part**, the sending of a communication OR a breach of a person's privacy.

7.4 Necessity must be demonstrated by including in every application a short explanation of:

- The event under investigation, such as a crime.
- The person whose data is sought, such as a suspect AND description of how they are linked to the event.
- The communications data sought, such as a telephone number or IP address, and how this data is related to the person and event.

7.5 The application must explain the link between the three aspects to demonstrate it is necessary to obtain communications data.

8. Proportionality test

8.1 Applications should only be made where they are proportionate, and alternative means of obtaining the information are either, exhausted, not available or considered not practical to obtain the same information.

8.2 For example, the following should be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

8.3 Applications should include the following key explanations:

- 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.

- Any circumstances which give rise to significant collateral intrusion.
- Any possible unintended consequences. This is more likely in more complicated requests for events data or in applications for the data of those in professions with duties of confidentiality. E.G journalists/doctors/solicitors.

9. Application procedure

9.1 Applicants must submit applications through the central NAFN (SPoC) portal. Applicants will need to be registered with NAFN to access the portal and have valid login and security details. An allocated SPoC officer will then check all applications for legal compliance and, where necessary, provide feedback before submitting for authorisation to OCDA.

9.2 OCDA will independently assess each application and will either grant or refuse the authorisation.

Authorised applications

9.3 Where the OCDA authorises the data request, this decision is communicated to the SPoC (NAFN) and actions are taken to request the data from the relevant telecommunications providers and other agencies holding such communications data to provide the necessary data.

Refused applications

9.4 Where the OCDA rejects an application, the Council has three options:

- Not proceed with the application;
- Re-submit the application with revised justification and/or revised course of conduct to obtain the communications data; or
- Re-submit the application without alteration and seek a review of the decision by the OCDA. This may only be done where the SRO (or a person of equivalent grade) has agreed to this course of action. The OCDA will provide guidance on this process.

10. Notices in pursuance of an authorisation

10.1 The giving of a notice is appropriate where a telecommunications operator or postal operator can retrieve or obtain specific data, and to disclose that data, and the relevant authorisation has been granted. A notice may require a telecommunications operator or postal operator to obtain any communications data, if that data is not already in its possession.

10.2 For local authorities the role to issue notices to telecommunications/postal operators sits with the SPoC (NAFN), and it will be the SPoC's role to ensure notices are given in accordance with the Code of Practice.

11. Duration of authorisations

11.1 An authorisation becomes valid on the date the authorisation is granted by the OCDA. It remains valid for a maximum of one month. Any conduct authorised or notice served should be commenced/served within that month.

11.2 Any notice given under an authorisation remains in force until complied with or until the authorisation under which it was given is cancelled.

11.3 All authorisations should relate to a specific date(s) or period(s), including start and end dates, and these should be clearly indicated in the authorisation.

11.4 Where the data to be obtained or disclosed is specified as 'current', the relevant date is the date on which the authorisation was granted.

11.5 Please note however that where a date or period cannot be specified other than for instance; 'the last transaction' or 'the most recent use of the service', it is still permitted to request the data for that unspecifiable period.

11.6 Where the request relates to specific data that will or may be generated in the future, the future period is restricted to no more than one month from the date of authorisation.

12. Renewal of authorisations

12.1 A valid authorisation may be renewed for a period of up to one month by the grant of a further authorisation and takes effect upon the expiry of the original authorisation. This may be appropriate where there is a continuing requirement to obtain data that may be generated in the future.

12.2 The Applicant will need to consider whether the application for renewal remains 'necessary and proportionate' and should reflect this in any renewal application made. The Authorising body (OCDA) will need to consider this carefully in authorising any renewal.

13. Cancellation of authorisations

13.1 Where it comes to the Council's attention after an authorisation has been granted that it is no longer necessary or proportionate, the Council is under a duty to notify the SPoC (NAFN) immediately.

13.2 It is the SPoC's (NAFN) responsibility to cease the authorised action and take steps to notify the telecommunications service provider. E.g. Such a scenario may occur where a legitimate application has been made for Entity data to identify and locate a suspect, but subsequently, and before the data has been obtained the Council becomes aware by some other legitimate means of the suspects name and address etc.

14. Offences for non-compliance with IPA 2016

14.1 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).

14.2 The roles and responsibilities laid down for the Senior Responsible officer 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 this Code, including procedures detailed in this Policy, will mitigate the risk of any offence being committed.

14.3 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.

14.4 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.

15. Monitoring and record keeping

15.1 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.

15.2 Records kept must be held centrally by the SPoC and be available for inspection by the Investigatory Powers Commissioner's Office upon request and retained to allow the Investigatory Powers Tribunal (IPT), to carry out its functions. The retention of documents service will be provided by NAFN.

15.3 The Business Manager for Corporate Governance will maintains an internal record on behalf of the SRO, and retains hard and electronic copies of all forms sent to the NAFN.

15.4 The documents in the internal record are retained in accordance with legal services' records management policy which complies with relevant data protection legislation. The original documents should be retained by the service area responsible for the surveillance activity.

15.5 The Investigatory Powers Commissioner's Office (IPCO) monitors compliance with RIPA. Haringey's SRO and Business Manager for Corporate Governance will act as the first point of contact for the Inspectors within the Council, but all service areas that use IPA should expect to be involved in any inquiries from IPCO.

15.6 Nothing in the Code or this policy affects similar duties under the Criminal Procedure and Investigations Act 1996 requiring material which is obtained in the course of an investigation and which may be relevant to the investigation to be recorded, retained and revealed to the prosecutor.

15.7 For full details of the level of information expected to be retained by the SPoC reference should be made to the Code of Practice.

15.8 Regular reports will be made to Members in accordance with the requirements of the IPA Codes of Practice.

16. Errors

Errors generally

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

16.2 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. ('reportable error'). 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.

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

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

Serious errors

16.5 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.

16.6 In these cases, the public authority which made the error, or established that the error had been made, must report the error to the Council's Senior Responsible Officer and the IPC.

16.7 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.

16.8 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'.

17. Investigations resulting in criminal proceedings

17.1 When communications data is been obtained during a criminal investigation that comes to trial an individual may be made aware data has been obtained.

17.2 If communications data is used to support the prosecution case it will appear in the 'served' material as evidence and a copy provided to the defendant.

17.3 Where communication data is not served but retained in unused material it is subject of the rules governing disclosure under the Criminal Procedure and Investigations Act 1996 (CPIA). The prosecution may reveal the existence of communications data to a defendant on a schedule of non-sensitive unused material, only if that data is relevant, and copies of the material may be provided to the defendant if it might reasonably be considered capable of undermining the prosecution case and/or assisting the defence.

17.4 Where communications data is obtained but not directly relied on to prove offences, the material may alternatively be listed in the 'Sensitive' unused material and not disclosed to the defendant. The CPIA sets out exemptions to the disclosure obligation. Under section 3(6) of that Act, data must not be disclosed if it is material which, on application by the prosecutor, the Court concludes it is not in the public interest to disclose. Any communications data which comes within the scope of this exemption cannot be disclosed. E.g. Material that reveals a 'method of investigation' is usually not disclosable.

17.5 If through any of the above notification processes, an individual suspects that their communications data has been wrongly obtained, the IPT provides a right of redress. An individual may make a complaint to the IPT without the individual knowing, or having to demonstrate, that any investigatory powers have been used against them.

Annex A

Haringey Council - Approved Rank Officers for IPA 2016

Job Title
Chief Executive
Director of Finance
Director of Environment and Neighbourhoods
Assistant Director for Stronger Communities

Haringey Council – Senior Responsible Officer for IPA 2016

Job Title
Assistant Director of Corporate Governance