Investigatory Powers Act 2016

Acquisition of Communications Data Policy and Procedure

Page left intentionally blank

Contents

Glossary

AO	Approval Officer
CPIA	Criminal Procedure and Investigations Act 1996
IPA	Investigatory Powers Act 2016
IPC	Investigatory Powers Commissioner
IPCO	Investigatory Powers Commissioners Office
IPT	Investigatory Powers Tribunal
NAFN	National Anti-Fraud Network
OCDA	Office for Communications Data Authorisations
RIPA	Regulation of Investigatory Powers Act 2000
SPoC	Single Point of Contact

SRO	Senior Responsible Officer.

1. Policy Statement

1.1 Walsall Council will apply the principles of IPA 2016 and its relevant codes of practice 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.

1.2 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;
- the proper procedures are followed

2. Overview of IPA

2.1 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.

2.2 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.

2.3 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.

2.4 This policy should be read in conjunction with the latest Home Office Code of Practice on Communications Data. Any queries or concerns in relation to the legalities of an investigation should be raised with Legal Services

2.5 This Policy should also be read in conjunction with Walsall Council's Regulation of Investigatory Powers Act 2000 Policy which deals with the use of surveillance and covert human intelligence sources (CHIS) and any relevant Enforcement Policy currently in force for the service undertaking the investigation.

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

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.

Entity data is data about a person or 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 mailto:example@example.co.uk?"* and *"who is the subscriber of phone number 01234 567 890?*"

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 Walsall Council does <u>not</u> 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 they have obtained the proper authorisation to do so and that the authorisation is necessary for the purposes of detecting crime or of preventing disorder.

- An Approval Officer (AO) 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).

5.3 The following types of conduct may be authorised:

- conduct to acquire communications data - which may include Walsall Council obtaining communications data themselves or asking any person believed to be in possession of or capable of obtaining the communications data to obtain and disclose it; and/or
- the giving of a notice – requiring a telecommunications operator to obtain and disclose the required data.

5.4 In the case of Walsall 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) Approvals Officer (AO);
3) Single Point of Contact (SPoC);
4) Authorising Agency (OCDA);
5) Senior Responsible Officer in a Public Authority (SRO)

6.2 Applicant and their responsibilities

The applicant is a person involved in conducting or assisting an investigation or operation and who makes an application in writing or electronically to obtain communications data. 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. The applicant will complete an application form setting out for consideration the necessity and proportionality of a specific requirement for acquiring communications data.

6.3 Any member of staff engaged in a relevant role i.e. one which requires carrying out investigations may be an applicant, subject to any internal controls or restrictions put in place within public authorities.

The applicant must

- describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the data is required, by reference to a statutory purpose under the Act;
- include a unique reference number;
- include the name and the office, rank or position held by the person making the application;
- describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
- include the operation name (if applicable) to which the application relates;
- identify and explain the time scale within which the data is required;
- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it;
- present the case for the authorisation in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;
- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;

- consider and, where appropriate, describe any possible unintended consequences of the application; and
- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data.

6.4 The applicant should record subsequently whether the application was authorised by an authorising individual and when that decision was made. Applications should be retained by the public authority and be accessible to the SPoC.

6.5 Approval Officer (AO) and their responsibilities

The Approval Officer is a person who is a manager at service level or above. The AO's role is to have an awareness of the application made by the Applicant and monitor the correct procedures are undertaken including contact with the SPoC.

6.6 The AO does not authorise or approve any element of the application and is not required to be operationally independent.

6.7 Single point of contact (SPoC) and their responsibilities

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.

6.9 Public authorities are expected to provide SPoC coverage for all reasonably expected instances of obtaining communications data. Walsall 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.

6.10 The SPoC will

- assess whether the acquisition of specific communications data from a telecommunications operator or postal operator is reasonably practicable or whether the specific data required is inextricably linked to other data;
- advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of telecommunications operators or postal operators;

- engage with applicants to develop and implement effective strategies to obtain communications data in support of operations or investigations;
- advise on and manage the use of the request filter, specifically in relation to progress of requests through the filter and compliance by the filter with the relevant authorisation;
- advise on the interpretation of the Act, particularly whether an authorisation is appropriate;
- provide assurance that authorisations are lawful under the Act and free from errors;
- consider and, where appropriate, provide advice on possible unintended consequences of the application;
- assess any cost and resource implications to both the public authority and the telecommunications operator or postal operator of communications data requirements.

6.11 Authorising Agency (OCDA) and their responsibilities

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 and undertakes 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.

6.12 Senior Responsible Officer (SRO) and their responsibilities

The Senior Responsible Officer (SRO) within Walsall Council is Simon Neilson the Executive Director Economy, Environment and Communities.

6.13 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, 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.

The application must explain the link between these three points 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.
- 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 period 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. Authorised applications

9.1 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.

10. Refused applications

10.1 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.

11. Notices in pursuance of an authorisation

11.1 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.

11.2 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.

12. Duration of authorisations

12.1 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.

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

12.3 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.

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

12.5 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.

12.6 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.

13. Renewal of authorisations

13.1 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.

13.2 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.

14. Cancellation of authorisations

14.1 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.

14.2 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.

15. Offences for non-compliance with IPA 2016

15.1 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).

15.2 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 this Code, including procedures detailed in this Policy, will mitigate the risk of any offence being committed.

15.3 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.

15.4 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.

16. Monitoring and record keeping

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

16.2 Records kept must be held centrally by the SPoC (NAFN) and be available for inspection by the Investigatory Powers Commissioners Office upon request and retained to allow the Investigatory Powers Tribunal (IPT), to carry out its functions.

16.3 A member of staff who acts in the capacity of a personal assistant to the SRO will maintain an internal record on behalf of the SRO, and retain hard and electronic copies of all forms sent to NAFN. The records will be retained and subsequently destroyed in accordance with Walsall Councils records management policy, which complies with relevant data protection legislation.

16.4 Walsall Council (see 16.3) will keep a record of the following information:

- the number of applications submitted by an applicant to a SPoC seeking the acquisition of communications data (including orally);
- the number of applications submitted by an applicant to a SPoC seeking the acquisition of communications data (including orally), which were referred back to the applicant for amendment or declined by the SPoC, including the reason for doing so;
- the number of applications submitted to an authorising individual for a decision to obtain communications data (including orally), which were approved after due consideration;
- the number of applications submitted to an authorising individual for a decision to obtain communications data (including orally), which were referred back to the applicant or rejected after due consideration, including the reason for doing so;
- the number of authorisations of conduct to acquire communications data granted (not including urgent oral applications);

- the number of authorisations to give a notice to acquire communications data granted (not including urgent oral applications);
- the number of notices given pursuant to an authorisation requiring disclosure of communications data (not including urgent oral applications);
- the number of times an urgent application is approved orally;
- the number of times an urgent notice is given orally, or an urgent authorisation granted orally, requiring disclosure of communications data;
- the priority grading of the authorisation for communications data including urgent oral authorisations;
- whether any part of the authorisation relates to a person who is a member of a profession that handles privileged or otherwise confidential information (such as a medical doctor, lawyer, journalist, member of a relevant legislature, or minister of religion) (and if so, which profession)72;
- the number of times an authorisation is granted to obtain communications data in order to confirm or identify a journalist's source; and
- the number of items of communications data sought, for authorisation granted (including orally).

16.5 For each item of communications data (including consequential data) included within a notice or authorisation, Walsall Council will also keep a record of the following:

- the unique reference number (URN) allocated to the application, authorisation and where relevant the notice;
- the statutory purpose for which the item of communications data is being sought, as set out at section 60A(7), 61(7) or 61A(7) of the Act;
- where the item of communications data is being sought for the applicable crime purpose as set out at section 60A(7), 61(7) or 61A(7) of the Act, the crime type being investigated;
- whether the item of communications data is events or entity, as described at section 261(5) of the Act, and Chapter 2 of this code;
- a description of the type of each item of communications data included in the notice or authorisation74;
- whether the item of communications data relates to a victim, a witness, a complainant, or a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;

- the age of the item of communications data. Where the data includes more than one day, the recorded age of data should be the oldest date of the data sought;

- where an item of data is event data retained by the telecommunications operator or postal operator, an indication of the total number of days of data being sought by means of notice or authorisation75; and

- the telecommunications operator or postal operator from whom the data is being acquired.

16.6 The Investigatory Powers Commissioners Office (IPCO) monitors compliance with RIPA. Walsall' s SRO 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.

16.7 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.

16.8 This policy and guidance document will be considered by Cabinet on an annual basis and this report will include a review of the use of IPA by the organisation. Where changes are required to the Policy either because of updates to legislation, codes of practice or other guidance; or due to structural changes within the organisation the Policy and details of the use to which it has been put will be considered by Cabinet before progressing for approval and adoption by full Council.

17. Errors

Errors generally

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

17.2 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, the public authority must report the error. The SRO would be the appropriate person to make the report to the IPC.

17.3 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.

17.4 The following is a non-exhaustive list of reportable errors.

- an authorisation or notice made for a purpose, or for a type of data, which the relevant public authority cannot call upon, or seek, under the Act;
- human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is acquired or disclosed;
- disclosure of the wrong data by a telecommunications operator or postal operator when complying with a request under Part 3 of the Act;
- acquisition of the wrong data by a public authority when engaging in conduct specified in an authorisation; and
- the omission of, or incorrect matches in filtered results, or the release of results that exceed specified thresholds.

17.5 The following is a non-exhaustive list of Recordable errors.

- a notice has been given which is impossible for a telecommunications operator or postal operator to comply with and the public authority attempts to impose the requirement;
- failure to review information already held, for example unnecessarily seeking the acquisition or disclosure of data already acquired or obtained for the same investigation or operation78;
- failure to cancel a requirement to acquire or obtain data as soon as possible once it is known to be no longer valid;
- failure to serve written notice (or where appropriate an authorisation) upon a telecommunications operator or postal operator within one working day of urgent oral notice being given or an urgent oral authorisation granted;
- where an error has occurred but is identified by the public authority or the telecommunications operator or postal operator without data being acquired or disclosed wrongly; and
- human error, such as incorrect transposition of information from an application to an authorisation or notice where communications data is not acquired or disclosed.

Serious errors

17.5 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.

17.6 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.

17.7 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 Investigatory Powers Tribunal. The IPC must be satisfied that the error is a serious error AND it is in the public interest for the individual concerned to be informed of the error.

17.8 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'.

18. Investigations resulting in criminal proceedings

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

18.2 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.

18.3 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.

18.4 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.

18.5 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 it.

19. Contacts

19.1 The Home Office is responsible for policy and legislation regarding communications data acquisition and disclosure.

Communications Data Policy Team
Home Office
2 Marsham Street
London
SW1P 4DF

19.2 **Complaints** - **Data security, integrity and destruction**

19.3 The Information Commissioner is responsible for the oversight of the security, integrity and destruction of data retained in accordance with the Act. Failure to comply with this code's provisions in these areas may also engage concerns about compliance with data protection and related legislation. Any concerns about compliance with data protection and related legislation should be passed to the Information Commissioner's Office (ICO) at the following address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

www.ico.org.uk

19.4 The Investigatory Powers Tribunal (IPT) has jurisdiction to consider and determine complaints regarding public authority use of investigatory powers.

Any complaints about the use of powers as described in this code should be directed to the IPT

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

The Investigatory Powers Tribunal - Home Page (ipt-uk.com)