Wiltshire Council

Corporate Policy and Procedures Document on

ACCESSING COMMUNICATIONS DATA

(The Investigatory Powers Act 2016 (IPA))

INDEX

1. DEFINITIONS

Authorising Individual

An individual who can authorise Communications Data applications. For the purposes of any applications made by the Council, an Authorising Individual will be either an Authorising Officer from the Office for Communications Data Authorisations or a Judicial Commissioner (see below).

Authorising Officer

An officer of the Office for Communications Data Authorisation with delegated authority from the Investigatory Power's Commissioner's Office to authorise Communications Data applications.

Cabinet

The body defined in Article 7 of the Wiltshire Council Constitution.

Collateral Intrusion

Collateral Intrusion is intrusion into the privacy of persons other than those who are directly the intended subjects of the investigation or operation.

Communications Data

Communications Data means any information held or obtained by a telecommunications operator or postal operator that relates to a person. It includes any information held by those service providers about that person's use of those services, including the way in which and the method by which the person communicates with another person or thing.

Communications Data does not include the content of any communications held by any telecommunications operator or postal operator and nothing in this policy authorises Council officers to access such data.

Confidential Information

Confidential Information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples might include consultations between a health professional and a patient, or information from a patient's medical records.

Designated Senior Officer

A Designated Senior Officer may also be referred to as the Designated Person. They are a senior officer of the Council who holds the position of director, head of service or service manager, who has received training for the purpose of considering applications for access to Communications Data.

Designated Senior Officers are listed at Appendix 2 of this policy.

Investigatory Powers Commissioner's Office (IPCO)

The independent body that oversees compliance with IPA 2016 and surveillance powers contained in RIPA 2000 and other legislation.

Judicial Commissioner

A member of the judiciary based at the Investigatory Powers Commissioner's Office who is responsible for providing an independent review of IPA authorisations to identify or confirm journalistic sources.

Office for Communications Data Authorisations (OCDA)

The Office for Communications Data Authorisations carries out a safeguarding function and decides applications on behalf of the Investigatory Powers Commissioner (IPC).

RIPA Co-ordinating Officer (RCO)

An experienced member of Legal Services' team (Senior Solicitor or above) responsible for the day to day oversight of applications (both IPA and RIPA) and reporting to the Senior Responsible Officer of any failings, training needs or improvements to the system.

Senior Responsible Officer (SRO)

The Head of Legal Services, Wiltshire Council.

Single Point of Contact (SPoC)

A single point of contact (SPoC) is a person who has received specific training in accessing communications data.

Local authorities are required to have collaboration agreements in place with the National Anti-Fraud Network (NAFN) to provide SPoC services. The officers at NAFN scrutinise applications independently and, following final approval from an Authorising Officer at Office for Communications Data Authorisations, acquire the communications data on behalf of the Council.

2. INTRODUCTION

The Investigatory Powers Act 2016 (IPA), which came into force on 11 June 2019, governs the use of investigatory powers by local authorities in relation to the acquisition of Communications Data.

The Act brings together the powers already in existence as created by the Regulation of Investigatory Powers Act 2000 (RIPA) as well as creating additional safeguards and oversight arrangements. Section 12 and Schedule 2 of IPA abolishes and amends other information gathering powers that provided for access to Communications Data without appropriate safeguards.

IPA provides a statutory framework for the authorisation and conduct of the acquisition of Communications Data. Its aim is to provide a balance between preserving people's right to privacy and enabling enforcement agencies to gather evidence for effective enforcement action.

It is consistent with the Human Rights Act 1998 and creates a system of safeguards, reflecting the requirements of Article 8 of the European Convention on Human Rights (right to respect for a person's private and family life, home and correspondence).

Compliance with IPA means that any conduct authorised under it is "lawful for all purposes". This important protection derives from section 81(1) of IPA, which gives the authorised person an entitlement to engage in the conduct which has been authorised.

Compliance with IPA will assist the Council in any challenges to the way in which evidence has been gathered and will enable the Council to demonstrate that it has acted lawfully. Non-compliance may result in:

(a) evidence being disallowed by the courts;
(b) a complaint of maladministration to the Ombudsman; or
(c) the Council being ordered to pay compensation.

It is essential therefore that the Council's policies and procedures, as set out in this document, are followed. A flowchart of the procedures to be followed appears at Appendix 1.

Council officers will also need to ensure compliance with the Code of Practice at Appendix 2. Where any provision of the Code of Practice appears to be relevant to any court or tribunal hearing, the Code will be admissible in evidence for both criminal and civil proceedings.

3. OVERSIGHT OF THE POLICY

The Senior Responsible Officer is responsible for the integrity of the process within Wiltshire Council to authorise use of Covert Human Intelligence Sources (CHIS) and compliance with;

- Part III of IPA 2016 (Authorisations for obtaining Communications Data)
- Part II of RIPA 2000 (Surveillance and Covert Human Intelligence Sources)
- Part III of the Police Act 1997 (Authorisation of Action in respect of Property)
- The Codes of Practice

The Senior Responsible Officer (SRO) is also responsible for;

- Engagement with Authorising Officers from the Office of Communications Data Authorisations (OCDA)
- Engagement with the Investigatory Powers Commissioner's Office (IPCO) and its Inspectors
- Oversight of any post-inspection action plans recommended by an Inspector, including ensuring that all Designated Senior Officers (DSOs) are of an appropriate standard

The RIPA Co-ordinating Officer (RCO) is responsible for the day to day oversight of applications and for the maintenance of the central record. The RCO shall report to the SRO any failings, training needs or improvements to the system.

The Cabinet Member for Resources shall be responsible for ensuring that IPA is being used consistently with this policy and that the policy remains fit for purpose. The SRO shall provide a report on Wiltshire Council's use of IPA to the Cabinet Member for Resources on a quarterly basis. A summary of this report shall be made available to all members of the Council. Annually, the report shall include a review of the effectiveness of this policy and any recommendation for changes to be made. Any significant amendments to the policy shall be referred to the Cabinet for approval.

For the avoidance of doubt the Cabinet and the Cabinet Member for Resources are not to be involved in making decisions on specific authorisations.

4. AUTHORISATION AND APPROVAL PROCEDURE

Applications for the acquisition of Communications Data should only be made where it is necessary for an Applicable Crime Purpose as defined at Section 60(A)(8) of the IPA (see section 5 below). This allows for applications to be made for Entity Data (formerly known as subscriber data) and Events Data (formerly known as service or traffic data).

Authorisation cannot be granted where an application is for any purpose other than the Applicable Crime Purpose. Under S11 of the IPA, it is an offence to knowingly or recklessly obtain communications data without lawful authority. Any person guilty of this offence will be liable to imprisonment for a term not exceeding 12 months and/or a fine.

Making an honest mistake will not amount to an offence. The conduct must have been intentional and voluntary, or the consequences of such conduct must have been foreseeable.

Communications Data does not include the content of any communications held by any telecommunications operator or postal operator and nothing in this policy authorises Council officers to access such data.

Council officers are also unable to acquire Internet Connection Records which provide details of the internet service that a specific device has been connected to.

A Council officer who wishes to access Communications Data must notify a Designated Senior Officer (DSO) before submitting an application electronically through the central NAFN Portal (www.nafn.gov.uk).

The DSO does not authorise or approve the application and as such is not required to be operationally independent. The DSO's role is to have an awareness of the application made, and to confirm this to the SPoC.

The application should contain the following information:

- a description of the Communications Data required;
- information as to time periods or any historic or future date(s);
- the purpose for which the data is required, by reference to the Applicable Crime Purpose under the IPA;
- a unique reference number;
- the name and position held by the person making the application;
- whether the Communications Data relates to a suspect, a witness, a complainant, a victim, next of kin, vulnerable person or other person relevant to the investigation or operation;
- the timescale within which the data is required;
- an explanation as to why the acquisition of that data is considered necessary and proportionate
- a description of any meaningful Collateral Intrusion and the extent to which the rights of individuals who are not under investigation may be infringed, and any
- justification for this in relation to the circumstances;
- where data is sought from a telecommunications operator or postal operator whether or not those operators may inform the subject(s) that an application has been made requesting Communications Data relating to them.

The role of the Single Point of Contact (SPoC)

Wiltshire Council is a member of the National Anti-Fraud Network (NAFN) an accredited body who provides SPoC services.

The SPoC facilitates the lawful acquisition of Communications Data, acting as a point of contact between the Council, the Office for Communications Data Authorisations (OCDA) and telecommunications operators and postal operators.

The SPoC will review the application for errors and advise as to the most appropriate methodology for the acquisition of data and assess any cost and resource implications.

The SPoC will also assist with good practice and provide advice regarding interpretation of the IPA to ensure that the Council acts in an informed and lawful manner.

If the SPoC is of the opinion that the application requires further work, it will be returned to the applicant who will have 14 days to make any amendments required and to resubmit the application.

If the SPoC is satisfied with the application, the SPoC will send the application for consideration by OCDA.

The Role of the Office for Communications Data Authorisations

OCDA provides independent authorisation and assessment of all Communications Data applications on behalf of the Investigatory Powers Commissioner.

An Authorising Officer from OCDA will only approve applications where s/he considers

that it is necessary for the Applicable Crime Purpose.

Should an Authorising Officer refuse the request submitted, the Council can decide not to proceed with the request, or to resubmit the application with a revised justification or course of conduct to acquire Communications Data.

The application may also be resubmitted without amendment seeking a review of the decision by OCDA, but the applicant must seek approval from the SRO in order to do so and the application must be resubmitted within 7 days.

The SPoC will notify the applicant of the outcome, and where an authorisation has been received the SPoC shall:

(a) serve the request notice on the telecommunications or postal operator requesting the Communications Data;
(b) liaise with the telecommunications or postal operator in order to obtain the Communications Data required; and
(c) provide the Communications Data to the applicant once it is received

Duration of authorisations and notices

An authorisation becomes valid on the date upon which the authorisation is granted. Authorisations can only be issued for a maximum time period of one month and any conduct authorised should be commenced or any notice should be served within this period.

A notice may be given to a telecommunications operator or postal operator requiring the operator to obtain any communications data, if that data is not already within the operators' possession. The giving of a notice is appropriate where the operator is able to obtain or retrieve and disclose specific data. The SPoC will issue any notices on the Council's behalf and such notices will remain in force until complied with or until the authorisation under which the notice was given is cancelled.

Where a request relates to data that may not be generated until the future, the future period can be no more than one month from the date of the authorisation.

Renewal of authorisations

Authorisations must be renewed where there is a continuing requirement to acquire or obtain data which is outside of the original authorisation period.

The original authorisation may be renewed for a period of up to one month which will take effect upon the expiry of the original authorisation.

The reasons for seeking renewal should be set out in the application which should be sent to the SPoC for review in the same way as the original application.

Cancelling an authorisation

The applicant must notify the SPoC immediately if it considers that the information being obtained under the authorisation granted is no longer necessary or the obtaining of it is no longer proportionate to the operation.

The SPoC will then cease the authorised action and will notify the telecommunications or postal operator accordingly.

5. NECESSITY AND PROPORTIONALITY

Applications for Communications Data will only be approved where it is necessary for an Applicable Crime Purpose.

The Applicable Crime Purpose varies depending upon whether the Communications Data sought is classified as Entity Data or Events Data.

Entity Data is the identity of an individual communications device or the person to whom services are provided, such as the registered user of a telephone number or email address.

Events Data is the date, time and type of communications and the duration and frequency of communications.

Where the communications data being sought is **Entity Data**, the Applicable Crime Purpose must be for the prevention and detection of crime. This permits the Council to obtain Entity Data irrespective of the seriousness of the crime.

In the case of **Events Data**, the threshold is higher to reflect the fact it contains more intrusive Communications Data, as such the purpose of obtaining the data must be for the prevention or detection of serious crime.

A serious crime is defined in Section 86(2A) of the IPA as an offence for which an adult is capable of being sentenced to 12 months or more in prison or any offence:

- involving violence;
- resulting in a substantial financial gain;
- involving conduct by a large group of persons in pursuit of a common goal;
- any offence committed by a body corporate; or
- any offence which involves, as an integral part of it, the sending of a communication or a breach of a person's privacy.

The Home Office publishes a list of 'notifiable' offences which may be useful in checking whether the maximum sentence for an offence is 12 months or more. A link to this publication can be found in Appendix 2.

Applications should only be made where the applicant is satisfied that there is no other reasonable means of carrying out the investigation, or obtaining the desired information, without undertaking the activity for which authorisation is sought.

Demonstrating Necessity

In order to demonstrate that an application is necessary a link between the following three aspects must be established and set out within the application;

- the event under investigation (the crime or disorder);
- the person whose data is sought (e.g. the suspect, and how they are linked to the event);
- the Communications Data sought, and how this relates to the person and the event.

Demonstrating Proportionality

Applicants should consider the following questions;

- Is the proposed covert surveillance proportional to the mischief under investigation?
- Is it proportionate to the degree of anticipated intrusion on the target and others?
- Is it the only option, other overt means having been considered and discounted?

Such considerations involve balancing the intrusiveness of the activity on the target and others, against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the particular circumstances or if the information sought could reasonably be obtained by less intrusive means.

Any activity must be carefully managed to meet the objective in question and must not be arbitrary or unfair. Any unnecessary intrusion, including Collateral Intrusion, must be minimised as much as practically possible.

The following should therefore be set out within the application:

- The reasons as to why that activity is sufficient and adequate for obtaining the information sought;
- Whether there are any other reasonable means of obtaining the information sought;
- Whether the surveillance is an essential part of the investigation;
- The type and quality of the information the activity will produce and its likely value to the investigation;
- The amount of intrusion, other than Collateral Intrusion, the activity will cause and whether there are ways to minimise that intrusion; and
- The length of time for which the authorisation is sought and whether the activity can be undertaken within a shorter time frame.

Confidential Information

Consideration should also be given as to the likelihood of Confidential Information being acquired. Confidential Information consists of matters subject to legal privilege, confidential private information or confidential journalistic material.

Where the purpose of a Communications Data application is to identify a journalistic source, the application will require authorisation from both OCDA and a Judicial Commissioner from the IPCO. Before making such application, the applicant should inform the SRO and obtain further advice from Legal Services.

Where Confidential Information is likely to be acquired, authorisation will only be given in exceptional and compelling circumstances with full regard to the proportionality issues this raises.

Risk of Collateral Intrusion

The applicant should describe the activity sufficiently widely to include not only named individuals, but also any others who are the not primary subject of the investigation but whose private life may be at risk of Collateral Intrusion.

Where the risk of Collateral Intrusion is sufficiently significant, the applicant should consider whether a separate authorisation is required in respect of these other persons.

And in circumstances where the investigation or operation unexpectedly interferes with the privacy of individuals not covered by the authorisation, an application for authorisation should be made.

Where an application may give rise to significant Collateral Intrusion, use of the 'request filter' should be considered. The request filter is operated on behalf of the Home Office and is overseen by the Investigatory Powers Commissioner. The filter operates as a safeguard, automatically filtering Communications Data to ensure that only the Communications Data that matches specified criteria is provided. Any irrelevant data will be deleted and will not be provided to the SPoC or the applicant.

The SPoC is responsible for monitoring the request filter progress, but the Council will be the data owner and processor of any Communications Data disclosed.

Novel or Contentious Applications

The Council is able to seek guidance from a Judicial Commissioner where an application to obtain Communications Data is either novel or contentious.

Applications involving new technical methods of acquisition or new types of Communications Data may be considered novel, and applications involving an unusual amount of Collateral Intrusion or where there is an unusual sensitivity attached to the application may be considered contentious.

The requirement to seek guidance is optional, but the SRO should be made aware and be supportive of any course of action decided by the applicant.

6. RECORDS MANAGEMENT

Applications submitted to OCDA will only be retained for a limited period of time. The SPoC will hold a central electronic copy of all:

- Applications
- Authorisations
- Copies of notices
- Records of the withdrawal of authorisations
- Records of cancellation of notices

The record of authorisations and notices will also include the time when each authorisation or notice was granted or given, renewed or cancelled.

All of these records are to be retained for five years and must be available for inspection by the Investigatory Powers Commissioner (IPC). The records may also be used by the Investigatory Powers Tribunal who are able to consider complaints made up to one year after the conduct to which the complaint relates to was carried out. The period of one year may be extended where equitable to do so, or where the conduct to which the complaint is alleged is still continuing.

Each service must also keep a record of:

(a) the number of applications which have been submitted to a SPoC seeking the acquisition of Communications Data;

(b) the number of applications submitted seeking the acquisition of Communications Data, which were referred back for amendment or declined by the SPoC, including the reason for doing so;
(c) the number of authorisations of conduct to acquire Communications Data granted;
(d) the number of authorisations to give a notice to acquire communications data granted;
(e) the number of notices given pursuant to an authorisation requiring disclosure of Communications Data;
(f) whether any part of the authorisation relates to a person who is a member of a profession that handles privileged or otherwise confidential information, and if so, which profession e.g. a journalist.
(g) the number of times an authorisation is granted to obtain Communications Data in order to confirm or identify a journalist's source; and
(h) the number of items of Communications Data sought, for which authorisation was granted.

In respect of each item of Communications Data included within a notice or authorisation, each service must also keep a record of:

(i) the unique reference number allocated to the application, authorisation and where relevant the notice;
(j) the statutory purpose for which the item of Communications Data is being sought. For the Council's purposes this will be as set out at section 60A(7)(b), the Applicable Crime Purpose;
(k) whether the item of Communications Data is Events or Entity Data;
(l) a description of the type of each item of Communications Data included in the notice or authorisation;
(m) 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;
(n) the age of the item of Communications Data by reference to the oldest date on which it was sought;
(o) 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 authorisation; and
(p) the telecommunications operator or postal operator from whom the data is being acquired.

Where the advice of a Judicial Commissioner or OCDA has been sought prior to the acquisition of communications data that could be considered novel or contentious, the Senior Responsible Officer must record and maintain a record of any views given.

Retention and Destruction of Material

Each Service must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. **Confidential material must be destroyed as soon as it is no longer necessary**. It must not be retained or copied unless it is necessary for a specified purpose. Where there is doubt, advice must be sought from the Solicitor to the Council or the SRO.

7. RECORDABLE/REPORTABLE ERRORS

A record should be kept where any error occurs in the granting of an authorisation, giving of a notice or as a consequence of any authorised conduct.

Reportable Error

Where an error results in Communications Data being wrongly acquired or disclosed, a report must be made to the Investigatory Powers Commissioner by the person responsible for the error.

Recordable Error

Where an error has occurred but is identified before any data has been acquired or disclosed, a record should be kept by the Council.

A list of reportable and recordable errors is provided in the Code of Practice.

8. NOTIFICATION OF SERIOUS ERRORS

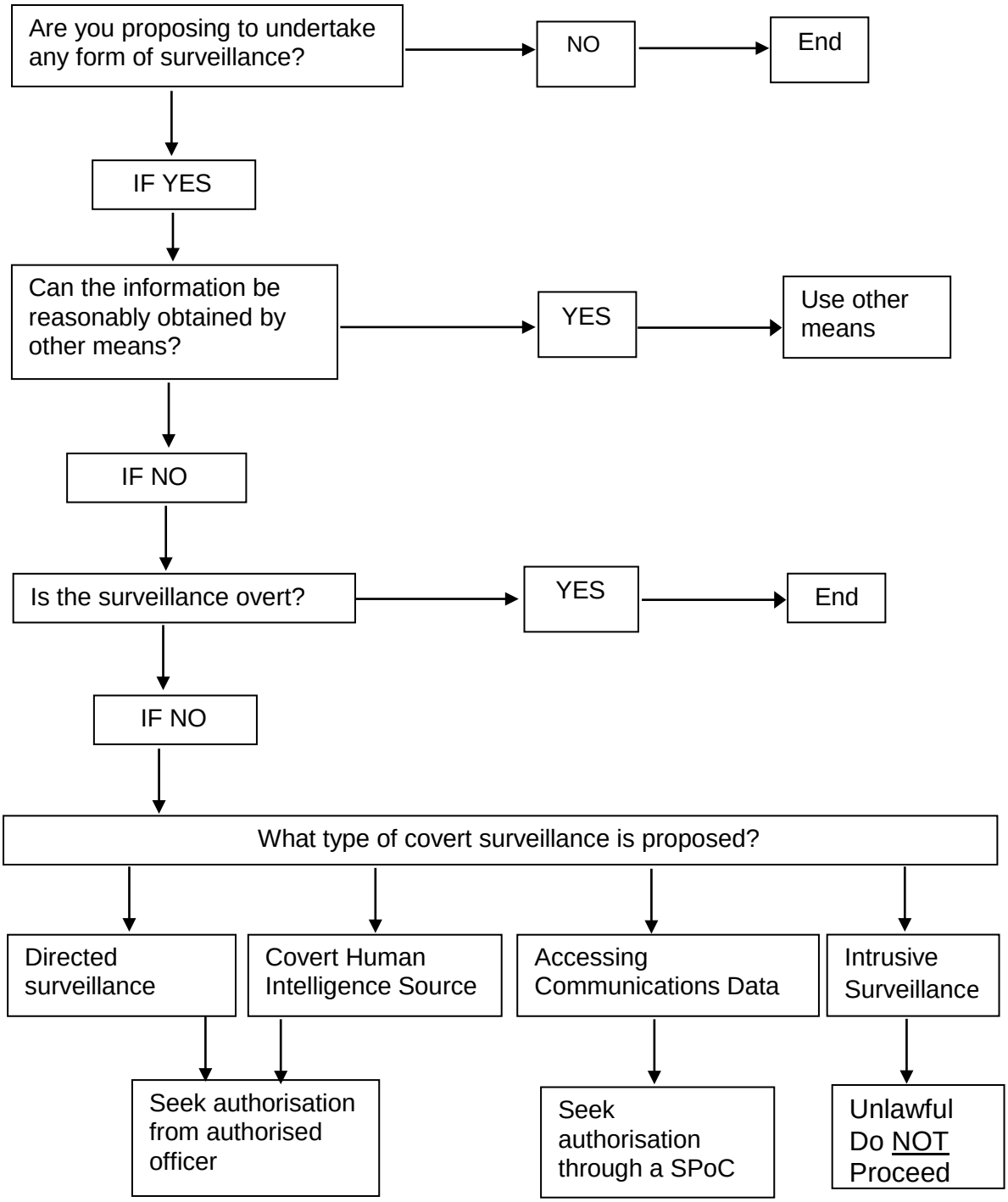
Where Communications Data is wrongly acquired or disclosed which amounts to a serious error, the person responsible for the error must report this to the SRO and the IPC.

A serious error will have occurred where such error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of the person's human rights will not by itself be sufficient for an error to be regarded as a serious error.

The IPC may inform the individual affected, who may make a complaint to the Investigatory Powers Tribunal. Prior to notifying the individual the IPC must be satisfied that the error is serious, and that it is in the public interest for the individual concerned to be informed of this error.

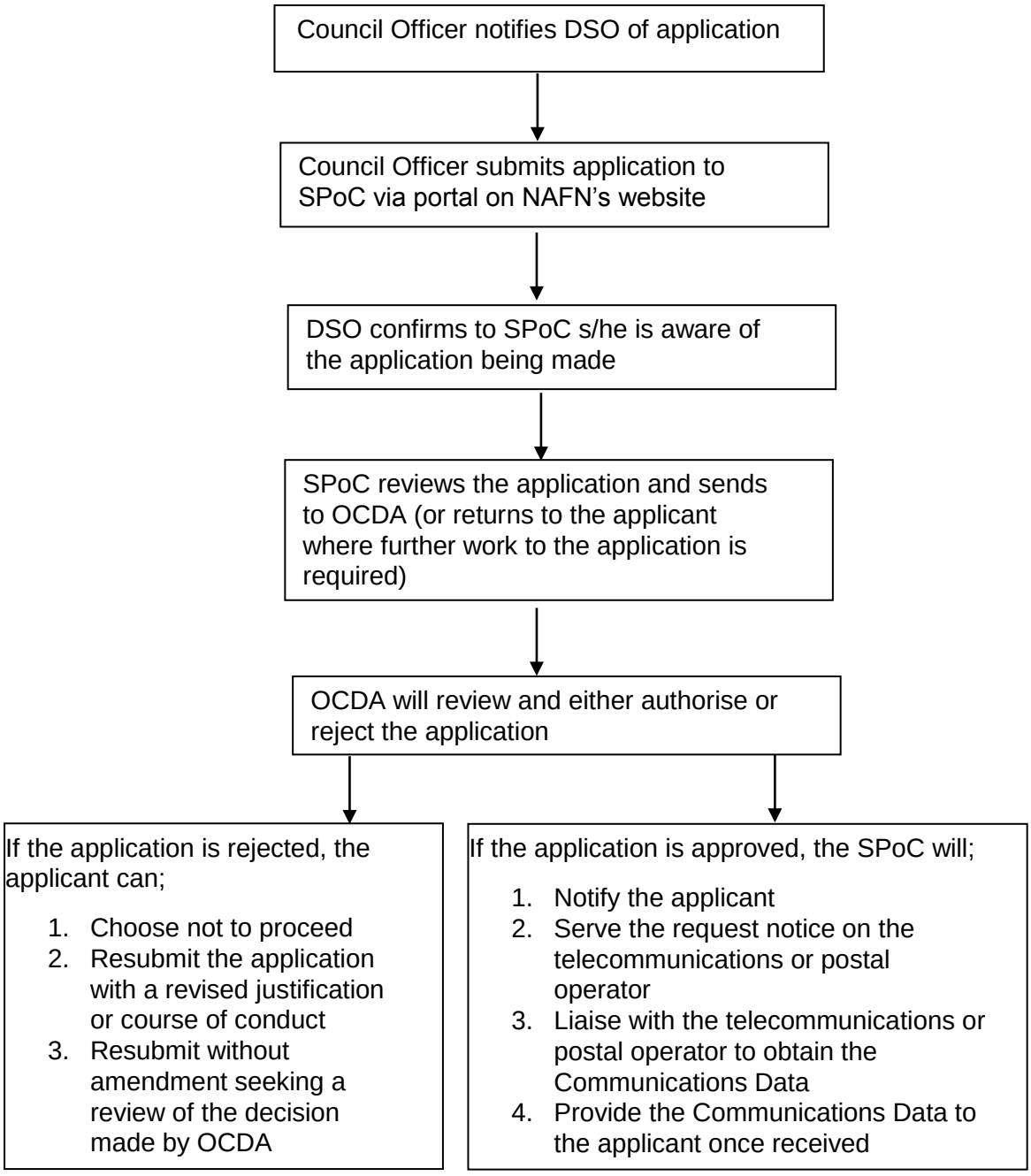
APPENDIX 1A

Do you need an IPA authorisation?



APPENDIX 1B

Application Process for Authorisation to Access Communications Data



APPENDIX 2

List of Designated Senior Officers

John Carter, Head of Public Protection, Trowbridge

Nicole Smith, Head of Housing Operations, Chippenham

Charlotte Wilson, SWAP Internal Audit Services

SPoC

The National Anti-Fraud Network

Useful Links

Communications Data Code of Practice

Investigatory Powers Act 2016

Website for the Office of Communications Data Authorisations

Website for the Investigatory Powers Commissioners Office

Counting Rules for Notifiable Offences