Stoke-on-Trent City Council
ACQUISITION OF COMMUNICATIONS DATA

City of Stoke-on-Trent

ANNEX 5

ACQUISITION OF COMMUNICATIONS DATA

Contents

1. Background

1.1 The Human Rights Act 1998 requires Stoke-on-Trent City Council ("the Council"), to have respect for the private and family life of citizens. However, in rare cases, it may be necessary for the Council to act covertly in ways that could interfere with an individual's rights.

1.2 The Investigatory Powers Act 2016 ('IPA') provides a mechanism for a Local Authority to acquire communications data from telecommunications and postal operators by setting up an authorisation procedure. The definition of communications data is very wide and can include subscriber information, telephone numbers called or received, the IP address of the sender of an email or the status or contact details of the customer of a social networking site. However it does not include the content of the communications.

1.3 The legislation seeks to ensure that public authorities only acquire communications data where it is necessary and proportionate, for a legally prescribed purpose, and that the acquisition is carried out in such a way that the risk of infringing the human rights of individuals is kept to a minimum. For a local authority the only legal purpose for acquiring communications data is for the preventing or detecting crime or of preventing disorder.

1.4 In accordance with section 1(1) of Schedule 7 of the IPA, the Secretary of State has issued a Communications Data Code of Practice which can be found at the following link:-

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

This policy must be read in conjunction with the Code of Practice and all staff involved in the acquisition of communications data must have regard to the provisions of the Code of Practice.

2. Introduction

2.1 The Council will on occasion need to acquire communications data to carry out its enforcement functions effectively. By following the authorisation procedures set out by IPA 2016, officers can demonstrate that the data acquisition is for a permitted purpose in connection with a specific investigation or operation and that it is a necessary and proportionate measure to take, given all the circumstances.

2.2 The Council is fully committed to complying with the Human Rights Act 1998 and the IPA 2016. The purpose of this policy is to reinforce the requirements of the IPA 2016 and the Communications Data Code of Practice, to ensure compliance with the law, to protect the rights of individuals and to minimise the risk of legal challenge as a result of officer actions.

2.3 All communications data acquisition must be done in accordance with the legislative framework and this policy including where these activities are carried out by a contractor. Any restrictions on the type of communications data that the Council is authorised to access and the tests to be applied must be observed, and any acquisition must be properly authorised and recorded.

2.4 Within the Council, a Senior Responsible Officer is appointed to oversee the process for the acquisition of communications data. They are responsible for the implementation and effective operation of this policy.

2.5 All applications for the acquisition of communications data made by the Council will be considered by an independent body, The Office for Communications Data Authorisations (OCDA) who perform this function on behalf of the Investigatory Powers Commissioner.

3. Communications Data

3.1 Communications data is the "who", "when", "where" and "how" of a communication but does not include the content and under no circumstances can the content of a communication be obtained. Local authorities have no right to listen in to telephone conversations without permission or read post or electronic communications before they have been received.

3.2 However, the definition of Communications Data in the legislation is very broad and the Communications Data Code of Practice gives specific examples of what is included and excluded from the definition. 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, of the communication.

3.3 Communications Data can include the address to which a letter or parcel 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 from which the communication was made. It covers electronic communications, including internet access, internet telephony, instant messaging and the use of apps.

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

3.5 **Telecommunications Data**: All communications data held by a telecommunications operator, or obtainable from a telecommunications system fall into one of two categories

- data about the entity:- This data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as

mobile phones or other communications devices).This might include subscriber details or billing information including payment methods.

- data about the event:-this data identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time, such as itemised telephone calls or their duration, or the location of a device when it was used to send a communication.

3.6 The only lawful purpose for which local authorities can obtain events data is in relation to **"serious crime".** This means an offence for which an adult is capable of being sentenced to one year or more in prison; any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy.

3.8 A local authority may not make an application that requires the processing or disclosure of internet connection records for any purpose.

3.9 **Postal Data**. A postal service is a service which includes one or more of collection, sorting, conveyance, distribution and delivery of postal items. Postal data may be:

- Anything comprised in or attached to a communication for the purpose of the service by which it is transmitted. This can include addresses or markings of the sender or recipient written on the outside of the postal item or online tracking.

- Data relating to the use made by a person of a postal service. This can include redirection services, price and postage class used, registered post or special/recorded delivery and parcel consignment records.

- Information held or obtained about persons who have used a communications service such as PO Box numbers even if no mail has ever been received

3.10 Postal data must however be related to a postal service and does not include data which may be held about a customer more generally.

4 Accessing Communications Data

4.1 Part 3 IPA 2016 allows a designated senior officer of a local authority, to authorise local authority officers to obtain data from any person which relates to a telecommunications system or data derived from a telecommunication system if he considers it necessary for the purpose of preventing or detecting

crime or of preventing disorder. This is subject to the requirement for the local authority to enter into a collaborative agreement.

4.2 The Council is party to a collaborative agreement with the National Anti-Fraud Network (NAFN) and uses the NAFN shared SPoC (Single Point of Contact) services for the acquisition of Communications Data. Applicants consult a NAFN SPoC throughout the application process and the SPoC will scrutinise the applications independently. All applications are made electronically using the NAFN secure portal.

4.3 There are 5 roles set out within the Code of Practice in respect of who will be involved in the acquisition of communications data.

- **The Applicant**
  This is the person involved in conducting or assisting an investigation or operation within the Council who makes an application in writing (electronically) for the acquisition of communications data. The Council limits the persons who are permitted to make an application to acquire communications data to those who have had sufficient training and knowledge of this area of law and only authorised officers in the Public Protection Team may submit an application.

- **The Single Point of Contact (SPoC**)
  The SPoC promotes efficiency and good practices in ensuring that only practical and lawful applications for communications data are made.

  Applicants follow the advice of the SPoC to ensure that the local authority acts in a lawful and informed manner.

  No application is submitted for authorisation until the SPoC is satisfied that it practical and lawful and that the appropriate verification procedure has been followed by the local authority.

  Within the Council, the SPoC is a member of the NAFN Service Team.

- **The Authorising Individual**
  Communications data applications can be authorised by three separate categories of individual depending on the circumstances of the specific case.

  1. An authorising officer in the Office for Communications Data Authorisations.
  2. The designated senior officer who holds a prescribed office or rank in the relevant public authority (where the independent authorisation does not apply). In the Council, the designated senior officer in the Consumer Protection Manager.
  3. A judicial commissioner who is responsible for approving requests to identify or confirm journalistic sources.

- **The Senior Responsible Officer**
  The Senior Responsible Officer is responsible for:
  - the integrity of the process in place within the public authority to acquire communications data,
  - engagement with authorising officers in the Office for Communications Data Authorisations (where relevant),
  - compliance with Part 3 of the IPA and with the Communications Data Code of Practice, including responsibility for novel and 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 by the public authority,
  - engagement with the IPC's inspectors when they conduct their inspections, and
  - where necessary, oversight of the implementation of post inspection action plans approved by the IPC.

  Within the Council, the Senior Responsible Officer is James Doble, Assistant Director (Governance).

5. The Application Process

5.1. The applicant will complete an application form setting out for consideration the necessity and proportionality of a specific requirement for acquiring communications data. This is done via the NAFN secure portal by completing the electronic application form. The applicant will have regard to the Communications Data Code of Practice in completing this form and in particular:-

- 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.

5.2 **Necessity**

The applicant must ensure that any application is necessary for the purpose of preventing or detecting crime or preventing disorder. In addition events data must only be sought for serious crime. See 3.6 above. The application should demonstrate how the investigation, the person and the communications data link together for the statutory purpose specified. Further detail on necessity is provided in the Communications Data Code of Practice.

5.3 **Proportionality**

The applicant must also ensure that the application is proportionate to what is sought to be achieved by obtaining the specified communications data and that the conduct is no more than is required in the circumstances. This involves balancing the interference with an individual's rights and freedoms against a specific benefit to an investigation or operation and that it is in the public interest. In particular the local authority must consider

- whether what is sought to be achieved could be reasonably achieved by other less intrusive means
- whether the level of protection to be applied should be higher because of the sensitivity of the information
- the public interest in the integrity of the postal or telecommunications systems
- any other aspects of the public interest in the protection of privacy.
- Collateral Intrusion. When accessing communications data there is the potential to obtain information relating to individuals who are not the subject of the investigation. Therefore the degree of collateral intrusion must be considered particularly when applying for events data. Taking all things together it may be that an interference with the rights of an individual may still not be justified because the adverse impact on another individual or group is too severe.
- The relevance of the data being sought and how it will benefit the investigation should be demonstrated. Any time periods must be explained outlining how these are proportionate to the event under investigation.

- Overall a consideration should be given to the rights of the individual and balancing these rights against the benefit of to the investigation. Further detail on proportionality is given in the Communications Data Code of Practice.

5.4 The application form will be reviewed by the National Anti-Fraud Network (NAFN) SPoC. If changes need to be made it will be referred back to the Applicant with suggestions, otherwise the NAFN SPoC will complete the relevant part and forward it to the Local Authority Verifier.

5.5 Local Authority verifier will confirm to the SPoC that they have been notified of the application via the NAFN electronic portal.

5.6 When satisfied that the local authority has completed the verification process the NAFN SPoC will forward the application to the Office for Communications Data for consideration by an Authoriser. The application will only be authorised if the officer is satisfied that the acquisition of communications data meets the requirements and is necessary and proportionate in the circumstances.

5.7 An authorisation becomes valid on the date upon which the authorisation is granted. It is then valid for a maximum of one month.

5.8 In the event that the application is rejected the local authority may decide to discontinue with the application, amend the application, or ask for a review of the decision. A review of the decision can only be requested with permission of the Senior Responsible Officer and will be instigated following the OCDA procedure.

5.9 An authorisation may authorise the NAFN SPoC to obtain the specific communications data, or to give notice to require a telecommunications operator to obtain and disclose the specific data if it is not already in their possession. The NAFN SPoC will proceed with the acquisition of communications data from the service provider on behalf of the local authority in accordance with the authorisation.

5.10 Any valid authorisation may be renewed for up to a period of 1 month by the grant of a further authorisation. The applicant should prepare an addendum to the original application explaining why there is a continuing requirement to acquire data and again demonstrating that it is necessary and proportionate in the circumstances. A renewed authorisation takes effect upon the expiry of the original authorisation.

5.11 Where the applicant identifies that a granted authorisation is no longer necessary for the statutory purpose or it is no longer proportionate it must be cancelled by notifying the NAFN SPoC. They will cease the authorised conduct and ensure that any notices are cancelled by advising the telecommunications operator and the authorising individual who will produce a record of the notice being cancelled.

6. Data Protection

6.1 Communications data obtained by the Council can only be held for the statutory purpose of preventing or detecting crime or of preventing disorder and should be adequate, relevant and not excessive for this purpose. In addition the specific requirements of data protection legislation should be adhered to.

6.2 Communications data held by the local authority is classified as OFFICIAL SENSITIVE and only authorised personnel can have access to the material. Those persons are limited to the officers directly involved in the investigation of the specific case and those involved in the approval process.

6.3 The Public Protection Division has a secure, restricted access, electronic storage facility which is used for this purpose.

6.4 All material must be handled in accordance with Data Protection principles and all records should be securely destroyed as soon as they are no longer needed for any of the authorised purposes.

6.5 Any additional disclosure of data must be in accordance with the provisions of data protection legislation.

6.6 The Council must keep a detailed record of all applications, authorisations, notices, renewals and cancellations so that they are available for inspection by the Investigatory Powers Commissioner or to allow the Investigatory Powers tribunal to carry out its functions. NAFN complies with these requirements on the Council's behalf.

6.7 Where authorised conduct results in the acquisition of excess data, or its disclosure by a telecommunications operator or postal operator in order to comply with the requirement of a notice, the excess data acquired or disclosed should only be retained by the Council where appropriate to do so – for example in relation to a criminal investigation

6.8 The Council is responsible for the retention of records to comply with the statutory obligations of the Criminal Procedure and Investigations Act 1996. There is a requirement to record and retain data which is relevant to a criminal investigation, even if that data was disclosed or acquired beyond the scope of a valid authorisation. If a criminal investigation results in proceedings being instituted all material that may be relevant must be retained at least until the accused is acquitted or convicted or the prosecutor decides not to proceed.

6.9 If, having reviewed the excess data, it is intended to make use of the excess data in the course of the investigation or operation, an applicant must set out the reason(s) for needing to use that material in an addendum to the application upon which the authorisation or notice was originally granted or given. The senior responsible officer (or a person of equivalent grade in the

public authority) will then consider the reason(s) and review all the data and consider whether it is necessary and proportionate for the excess data to be used in the investigation or operation

7. Errors

7.1 Proper application of the Act and Code of Practice in line with this policy including the careful preparation and checking of applications, and authorisations, should reduce the scope for making errors. However NAFN keep a records of any errors that have occurred and a report and explanation is sent by NAFN's Senior Responsible officer to the Commissioner as soon as is practicable.

8. Complaints

8.1 The Council has a complaints procedure which can be accessed here. In addition the Investigatory Powers Tribunal has power to investigate complaints from anyone who believes they have been a victim of unlawful action by a public authority using covert investigative techniques.

9. Oversight

9.1 The Senior Responsible officer shall establish and maintain regular meetings, as appropriate, to check and test processes and address any training requirements.

9.2 The SRO shall record any issues arising from these meetings or the process as it operates in practice and determine any actions necessary to ensure the proper application of this policy.

9.3 In addition the SRO shall arrange an oversight meeting as soon as possible following an inspection to discuss issues and outcomes as appropriate.

10. Review

10.1 This policy will be reviewed annually or sooner if legislation changes.