SANDWELL METROPOLITAN BOROUGH COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 AND INVESTIGATORY POWERS ACT 2016

ACQUISITION OF COMMUNICATIONS DATA

CORPORATE POLICY

Author:	Legal and Assurance
Owner:	Director of Law and Governance
Version:	1.0
Modified by:	Legal and Assurance
Date:	October 2023
Review Date:	October 2024

1. INTRODUCTION

1.1 Originally the Regulation of Investigatory Powers Act 2000 (RIPA 2000) provided qualified powers to enable local authorities including Sandwell MBC to access the communications data of its citizens for specified purposes in qualified circumstances. These powers still exist but are now regulated by the Investigatory Powers Act 2016 (IPA 2016).

1.2 This policy explains the context in which these powers exist their extent as far as local government is concerned and how Sandwell MBC will use them.

2. BACKGROUND

2.1 The European Convention on Human Rights is a binding international agreement that enshrines fundamental civil and political rights. The Human Rights Act 1998 has made Convention Rights enforceable in our domestic courts. The HRA gives people a clear legal statement of their basic rights and fundamental freedoms.

2.2 The Human Rights Act 1998 covers 17 convention rights and 3 additional rights in the First Protocol and 2 additional rights in the Sixth Protocol. Key rights engaged in the context of the acquisition of communications data are Article 8 (A right to respect for private and family life) and Article 1 of the First Protocol (The Protection of Property).

2.3 The Investigatory Powers Act 2016 (IPA 2016) in conjunction with RIPA 2000 provides for and regulates the use of a range of investigative powers by a variety of public authorities .IPA 2016 to quote the Acts own overview, sets out the extent to which to which certain investigative powers may be used to interfere with privacy.

2.4 There are powers in Part 2,(Interceptions of Communications),Part 5(Equipment Interference),Part 6 (Bulk Warrants) and Part 7 (Bulk Personal Database Warrants) that the Council have no legal powers to apply for and as a matter of policy would clearly not seek to do so

as unauthorised activity will ,in addition be a criminal offence. The 2016 Act abolishes previous general powers to access communications data and generally seeks to protect privacy other that in quite specified circumstances.

2.5 Whilst IPA 2016 is the main legislation regulating access to Communications Data further protections can be found in the Human Rights Act 1998,Section 170 of the Data Protection Act 2018,(unlawful obtaining of personal data) ,Section 48 of the Wireless Telegraphy Act 2006 (offence of intercepting/disclosing messages) ,Section 1-3A of the Computer Misuse Act and the offence of Misconduct in Public Office.

2.6 A public authority such as Sandwell MBC can interfere with a person`s Article 8 or Article 1 First Protocol rights (protection of private life and protection of property) but must do so on a clear legal basis. If the Council are seeking to access “Events Data” (see later) they must broadly be investigating a criminal offence carrying a maximum penalty of at least 12 months imprisonment upon conviction. If they are seeking to access “Entity Data” (see later) they must be investigating Crime or Disorder. Quite independently of this the use of these powers must be necessary and proportionate-not just reasonable.

3. ACQUISITION OF COMMUNICATIONS DATA

3.1 The Councils powers to access Communications Data are contained in Section 60A of the Investigatory Act 2016. They are dependent upon the thresholds of seriousness reaching the level described in 2.6 above.

3.2 “Entity Data”- Is information about a person or an item such as a phone, computer or tablet. It includes Account Information; Subscribers to e mail and telephone accounts; Installation and Billing Addresses and sign up data.

3.3 “Events Data” is more private information and therefore requires a higher threshold (basically serious crime carrying at least a maximum

sentence of 12 months imprisonment) and includes Itemized telephone call, text and connect records; Itemised timing and duration of calls; Connect/Disconnect /Reconnection of Data; Mobile Phone Data Records ,Device Data Records, the Use of forwarding/postal redirection services and records of postal items.

3.4 Communications Data concerns the "who,when where and how" of communications **but not the content.** The Council do not have the power to access the **content** of a communications via a communications system.

4. ADDITIONAL SAFEGUARDS

4.1 An application to access Communications Data must firstly be authorised by the authorising officer from within the Council.

4.2 The decision to authorise must, under Section 76 of the IPA 2016 be reached after consultation with a "Single Point of Contact" (SPoC) at the National Anti-Fraud Network (NAFN) currently based at Tameside Metropolitan Borough Council. They will assess and quality control the application. If the application meets the legal threshold for obtaining communications data then the SPoC will act as a go -between to facilitate co-operation between the local authority and the Communications Service Provider (CSP), thereby acting as a "gatekeeper".

4.3 At this stage the Council must then seek authorisation from the Magistrates Court. This is the responsibility of the Council and not the National Anti-Fraud Network (NAFN). The JP or District Judge will then complete a Judicial Order to the SPoC at NAFN. The Notice is then served on the Communications Service Provider (CSP) by the SPoC. Once the data is obtained the SPOC will provide the data to the applicant.

4.4 All records are kept centrally by NAFN who will record and report any reportable errors to the SRO as well as notifying the Investigatory Powers Commissioners Office who has oversight of the exercise and performance of duties under the IPA 2016.

4.5 In addition the Council will have regard to the 2018 Communications Data Code of Practice.

5. PROHIBITIONS

5.1 The Council will only seek to access communications data in accordance with its legal authority to do so under Sections 60A and 73 of the Investigatory Powers Act 2016 as outlined above.

ANNEX A

The holders of the following post is designated to grant authorisations and give notices for the acquisition of communications data:

Director of Law and Governance/Monitoring Officer

CONTACTS

NAFN (National Anti-Fraud Network_
PO Box 304
Ashton Under Lyne
Tameside OL6 O6A
Tel 0161 342 3662

IPCO (Investigatory Powers Commissioners Office)
PO Box 29105
London
SWIV 1ZU
Tel 0207 389 8900

OCDA (Office for Communications Data Authorisations)
info@OCDA.org.uk

See also Communications Data Code of Practice November 2018