APPENDIX B

Halton Borough Council

Investigatory Powers Act 2016

Policy relating to communications data

1. The Investigatory Powers Act 2016 ("the Act") was brought into force in early June 2019.
2. The Act sets out the extent to which certain investigatory powers (relating to the acquisition of communications data from a telecommunications operator or a postal operator) may be used to interfere with privacy.
3. In applying the Act Halton Council ("the Council") will apply this policy where the Council is deciding to grant, approve or cancel an authorisation under Part 3 of the Act.
4. Specifically, the Council will have regard to:
    - whether what is sought to be achieved by the authorisation could reasonably be achieved by other less intrusive means,
    - whether the level of protection to be applied in relation to any obtaining of information by virtue of the authorisation is higher because of the particular sensitivity of that information,
    - the public interest in the integrity and security of telecommunication systems and postal services, and
    - any other aspects of the public interest in the protection of privacy.
    - the interests of national security or of the economic well-being of the United Kingdom,
    - the public interest in preventing or detecting serious crime,
    - other considerations which are relevant to –
        - whether the conduct authorised or required by the authorisation is proportionate, or
        - whether it is necessary to act for a purpose provided for by the Act,
    - the requirements of the Human Rights Act 1998, and
    - other requirements of public law.

5. The Council will apply all relevant Parts of the Act and also have regard to any statutory code of practice (the current code being Communications Data Code of Practice November 2018).
6. The detailed description of how the Act is used is set out in the Council's Employees' Guide to the Act.
7. This policy replaces any previous policy relating to the acquisition of communications data from a telecommunications operator or a postal operator.

Halton Borough Council

Communications Data

Employees' Guide to the Investigatory Powers Act 2016 (Part 3)

Mark Reaney

Senior Responsible Officer

Operational Director – Legal and Democratic Services

Contents

Section 1 - What the Act refers to

- The 2016 Act relates to the obtaining of communications data from a telecommunications operator and/or a postal operator.

- Communications data include the “who”, “when”, “where”, and “how” of a communication but not the content: i.e. what was said or written.

- Communications data comes in two kinds – “entity data” and “events data”.

- Employees should be familiar with the Council’s policy on the acquisition of communications data from a telecommunications operator and/or a postal operator.

- Employees should also be familiar with and have regard to the Communications Data Code of Practice (November 2018) issued by the Home Office (“the Code”).

- Principal definitions may be found at sections 261 to 265 of the Act.

- It should be kept in mind that the Regulation of Investigatory Powers Act 2000 still applies where communications data is viewed on “open access” social media sites where this amounts to covert surveillance.

Section 2 - The Parties referred to

Applicant	means the person involved in conducting or assisting an investigation or operation who makes an application in writing or electronically for the acquisition of communications data.
Authorising Individual	means the authorising officer in the Office for Communications Data Authorisations (“OCDA”).
IPC	means the Investigatory Powers Commissioner
Made Aware Officer	see verifying officer.

NAFN	means the National Anti-Fraud Network
Senior Responsible Officer	means the person who is responsible for the matters set out at paragraph 4.10 of the Code. In addition, under paragraph 8.5 of the Code the senior responsible officer must be satisfied that the officer(s) verifying the application is (are) of an appropriate rank and must inform NAFN of such nominations.
SPoC	means the single point of contact – which means NAFN.
Verifying Officer	means the person within the Council (of at least the rank of the senior responsible officer) who is aware the application is being made before it is submitted to an authorising officer in OCDA.

Section 3 – Applications and authorisations – Procedure

1. Applications are made leading to authorisations to acquire communications data

2. The Council is a relevant authority for the purpose of Part 3 of the Act (section 73)

3. However, the Council is only a relevant public authority for the purposes relating to authorisation under section 60A (section 73 (1)).

4. There are further restrictions under section 73 (3) under which authorisations may only be given under section 60A if:

    - Section 60A(1)(a) is met in relation to a purpose within section 60A(7)(b) [i.e. the applicable crime purpose],

    - The Council is party to a collaboration agreement with NAFN to act as SPoC

- The collaboration agreement is certified by SoS.

5. The route for authorisations under section 60A is via the Investigatory Powers Commissioner [which operates through the Office for Communications Data Authorisations (OCDA)] (Section 60A(1) to (3)).

6. The process will start by the applicant (i.e. the relevant enforcement officer) generating on-line applications via NAFN which are then processed by NAFN

7. Such applications must not be sent until unless a "made- aware" officer (analogous to a Designated Person in RIPA applications) has been made aware of the application being proposed.

8. The **Senior responsible Officer** must inform NAFN of who these "made-aware" officers are.

9. The powers of designated senior officers to grant authorisations elsewhere in Part 3 of the Act do not apply to local authority applications. In fact, there is no role for "designated senior officers" in local authority applications for communications data. This role is carried out by an "authorising officer in the Office for Communications Data Authorisations".

Section 4 – Keeping of Records

- The detailed requirements regarding the keeping of records are set out at section 24 of the Code at paragraphs 24.1 to 24.9.

- The essential point is that relevant officers know who is responsible for keeping these records. The applicant will have primary responsibility for producing these records and the relevant verifying officer will have responsibility for keeping these records. The verifying officer will report annually to the senior responsible officer that proper records have been kept over the previous year.

Section 5 – Errors

- The Code sets out the rules for detecting, monitoring and reporting of errors is set out at paragraphs 24.17 to 24.37 of the Code.

- The relevant verifying officer shall monitor the processes in acquiring communications data with a view to decreasing the likelihood of errors occurring and wherever possible, technical systems should incorporate functionality to minimise errors.

- The relevant verifying officer shall report all errors which come to the attention of the verifying officer to the senior responsible officer.

- It shall be the responsibility of the senior responsible officer to report any reportable errors received by the senior responsible officer to the IPC in accordance with the Code.

Section 6 – Retention of Data

- Communications data should only be kept for the period during which it is necessary to hold the data.

- The Council's retention of documents policy should be used as a guide as to the appropriate retention period.

Section 7 – Useful Links

https://www.gov.uk/government/consultations/investigatory-powers-act-2016-codes-of-practice