

**MERSEYSIDE FIRE & RESCUE SERVICE**  
**POLICY**

---

**The use of covert surveillance techniques  
and covert human intelligence sources &  
acquisition of communications data**

## **GENERAL STATEMENT OF POLICY**

This policy document relates to use by officers of directed surveillance and covert human intelligence sources, and to the interception of telecommunications made to, from or within Merseyside Fire & Rescue Authority's ("the Authority") Business Telecommunications Systems.

- **The Authority is committed to upholding human rights.**
- **As a public body and responsible employer, the Authority wants to conform to the letter and spirit of the requirements of the Human Rights Act 1998, the Regulations of Investigatory Powers Act 2000 and associated regulations and codes of practice relating to the use of directed surveillance, the use of covert human intelligence sources, and interception.**
- **Authority officers will only undertake surveillance work when it is both necessary and proportionate to the ends it seeks to achieve.**

## **1. BACKGROUND**

1. 1. One of the functions of the Authority is to carry out regulatory functions in respect of fire safety legislation. Such regulatory functions give to the officers involved powers and rights to enable them to carry out their duties - for example the power of Fire Safety Inspectors to require production of documents, the right to enter premises and inspect goods etc.
1. 2. To balance these powers and rights, there are also controls to prevent abuse by officers and authorities. There are both statutory measures - for example the Police & Criminal Evidence Act 1984 which controls the questioning of suspects; and voluntary systems - for example the Enforcement Concordat, which provides principles of good enforcement and which has been adopted by the Authority.
1. 3. On some occasions it may also be appropriate for the Authority to conduct investigations in respect of its own employees and others to prevent or detect crime (e.g. attacks on firefighters).
1. 4. Surveillance can be a necessary and valuable tool. The Regulation of Investigatory Powers Act 2000 controls the use of surveillance, and of covert human intelligence sources such as informants and undercover officers. Compliance with the letter and spirit of the Act and associated Codes of Practice will ensure that the Authority performs its regulatory roles in a manner appropriate to a public authority and responsible employer.

## **2. THE REGULATION OF INVESTIGATORY POWERS ACT 2000**

2. 1. The main purpose of the Act is to ensure that investigatory powers are used in accordance with human rights. These powers are:
  - interception of communications
  - acquisition of communications data (e.g. billing data)
  - intrusive covert surveillance (on residential premises/in private vehicles).
  - directed covert surveillance in the course of specific operations
  - use of covert human intelligence sources (informants etc)
  - access to encrypted data
2. 2. By working in conjunction with other, pre-existing legislation, the Act ensures the following points are clearly covered:
  - purposes to which relevant powers may be used
  - which authorities can use the powers
  - authorisation of the use of the powers

- the use that can be made of material gained
- independent judicial oversight
- a means of redress for the individual where powers are breached.

### 3. DEFINITIONS

The following definitions apply throughout this policy document

- *directed surveillance* is surveillance which is covert but not intrusive, and which is undertaken for the purposes of a specific investigation or a specific operation, in such a manner as is likely to result in obtaining information about a person - whether or not the target of the investigation/operation - and is not carried out in immediate response to the events or circumstances which make prior authorisation not reasonably practical
- *Intrusive surveillance* is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle and which involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device
- *A covert human intelligence source* is an inside informant or undercover officer who develops or maintains a relationship with the surveillance target, having the covert purpose of obtaining or accessing information for the investigator
- *Confidential material* consists of:
  - matters subject to legal privilege
  - confidential personal information
  - confidential journalistic material
- *Collateral intrusion* is interference with the privacy of (an) individual(s) who is /are not the subject of the surveillance operation.

### 4. POLICY

#### 4. 1. Directed Surveillance and Covert Human Intelligence Sources

4. 1. 1. No officer of the Authority will undertake intrusive surveillance.
4. 1. 2. No officer of the Authority will undertake directed surveillance or use a covert human intelligence source without prior authorisation.

4. 1. 3. Authorisation will only be give by one of the following officers:-

- (a) Chief Fire Officer
- (b) Deputy Chief Fire Officer
- (c) Assistant Chief Fire Officer
- (d) The Clerk or Deputy Clerk
- (e) The Treasurer or Deputy Treasurer
- (f) The officer responsible for the management of an investigation.

4. 1. 4. Authorisations have a maximum duration as follows:

Directed surveillance - 3 months

Covert human intelligence source - 12 months

4. 1. 5. Authorisation will only be given for surveillance or the use of a covert human intelligence source, when the activity is necessary to prevent or detect crime, or in the interests of public safety, or for the purpose of protecting public health.

4. 1. 6. Authorisation will only be give when the surveillance is proportionate to what it seeks to achieve, having particular regard to the risk of collateral intrusion.

4. 1. 7. Copies of all authorisations, extensions to and cancellations of authorisations will be held centrally by the Clerk who will carry out an annual review of authorisations to ensure compliance with the Act.

4. 1. 8. Covert surveillance operations will only be carried out by officers in accordance with a current authorisation granted under paragraph 4.

#### 4. 2. **Interception of Telecommunications**

4. 2. 1. Interception of telecommunications is authorised in certain circumstances by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

4. 2. 2. Authorisations must be by or with the express or implied consent of the system controller, (i.e. the person with the right to control the operation and use of the Authority's Telecommunications System, in this case the Chief Fire Officer) for the purpose of monitoring or recording communications:

- to establish the existence of facts, in respect of suspected disciplinary offences or to ascertain or demonstrate standards.

- to prevent or detect crime (e.g. monitoring of fire calls),

**AND**

the system controller has made all reasonable efforts to inform potential users that interceptions may be made.

**4.3. Acquisition of Communications Data**

4.3.1. The Chief Fire Officer shall nominate an appropriate employee or employees as “Designated Persons” as the role of Group Manager or equivalent or higher to perform the role of considering, and where appropriate, granting authorisations for accessing communications data by the Authority :-

- (a) Referring the data itself, or
- (b) Giving notice to the communications service provider requiring the operator to collect or retrieve the data and provide it to the Authority.

4.3.2. The Chief Fire Officer shall nominate an appropriate employee or employees as the Single Point of Contact (SPOC) at the role of Group Manager or equivalent or higher, who will fulfil the role of Single Point of Contact with communications service providers (e.g. BT) which involves liaison with each communications service provider to apply for and obtain relevant communications data.

4.3.3. The Authority will apply to communications service providers for communications data (i.e. itemised call records, routing information and subscriber details) where the Authority considers it appropriate to do so :-

- In the interests of public safety, or
- To prevent or detect crime, or
- In an emergency to prevent death or injury.

4.3.4. The acquisition of data will be proportionate to what is sought to be achieved. In operational terms, this will cover matters such as :-

- Locating the position of a caller making an emergency call who has cleared the line before giving adequate details about the location at which the fire appliance is required.
- During a fire investigation, obtaining contact details in order to speak to whoever reported the fire to help piece together the sequence of events.
- To investigate hoax and malicious calls.

**4. 4. Confidential Material**

4. 4. 1. Confidential material must not be copied or retained unless for a specific purpose - e.g. use as evidence in proceedings.

4. 4. 2. Confidential material may only be disseminated following advice from the Clerk, or in the case of personal data the Data Protection Officer.

4. 4. 3. Any confidential material retained, copied or disseminated must be accompanied by a clear warning as to its confidential nature, and appropriate steps taken to ensure that the information contained therein cannot become available to any person whose possession of it might prejudice an related proceedings.
4. 4. 4. Confidential material must be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

## **5. RESPONSIBILITIES**

### **5. 1. Chief Fire Officer to:**

- ensure all appropriate staff are aware of and trained in the Act, and that training is kept current
- provide procedures to be adopted in the application for, granting etc. of, and recording of authorisation
- Ensure that details of the complaints procedure involving the Investigatory Powers Tribunal are readily available for public reference purposes at the Authority Headquarters or by post or e-mail on public request or on the Authority website.

### **5. 2. Clerk to:**

- maintain a record of all authorisations granted by Officers of the Authority
- carry out an annual review of authorisations to ensure compliance with the Act

### **5. 3. All Officers authorising surveillance operations to:**

- ensure applications are complete and are made out on the appropriate *pro forma*
- consider applications, and issue, renew, cancel or refuse authorisations in accordance with the criteria set out in the Act, and Codes of Practice
- maintain a record of applications and authorisations, and provide copies to the Clerk within 5 working days of the application, irrespective of whether the authorisation is granted, and copies of all cancelled authorisations within 5 working days of the cancellation
- ensure all staff involved in surveillance operations have access to the relevant Codes of Practice.
- review authorisations at least monthly - more frequently if considered appropriate - and record the review on the authorisation, ensuring that authorisations are cancelled as soon as they have either served their original purpose or no longer meet the criteria for issue, whichever is the earlier.

5. 4. **All staff involved in surveillance operations to:**

- be familiar with Act, and the relevant Codes of Practice
- ensure that the authorising officer is provided with all relevant information available to the investigation to enable an informed decision to be made
- Cease the surveillance operation immediately it has either served its original purpose, no longer meets the criteria for issue whichever is the earlier
- advise the authorising officer as soon as practicable when an operation unexpectedly interferes with the privacy of an individual who is not the subject of the surveillance

5.5. **SPOC**

To undertake and successfully complete appropriate training (e.g. Home Office accredited training)

**6. RETENTION AND DESTRUCTION OF PRODUCT OF SURVEILLANCE**

6. 1. where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.
6. 2. With regards to enforcement of fire safety legislation, material which is obtained in the course of a criminal investigation, and which may be relevant to the investigation must be recorded and retained
6. 3. There is nothing in the 2000 Act which prevents material obtained from properly authorised surveillance from being used in other investigations. The Authority must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising officers must ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.