



<u>Title</u>	Lawful Business Practice (Interception of Communications) Regulations
<u>CCMT Sponsor</u>	Deputy Chief Constable
<u>Department/Area</u>	Professional Standards
<u>Section/Sector</u>	Headquarters

1.0 Rationale

This policy relates to the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 which allows businesses, including public authorities, to intercept communications transmitted on their systems for certain purposes.

2.0 Intention

The use of this policy will be restricted to criminal or serious misconduct offences. This policy should, however, be read in conjunction with the Voice Recording Policy and CR & ED Standing Operating Procedure Number 10, which allow for all calls into a control room or PEC to be monitored for the prevention and detection of crime, and training purposes.

3.0 General Principles

Monitoring and recording of communications conveyed on the Thames Valley Police private telecommunications system.

3.1 Introduction

3.1.1 This policy provides guidance to all persons who use Thames Valley Police telecommunications systems following the introduction of the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of

NOT PROTECTIVELY MARKED

Communications) Regulations 2000. It should be read in conjunction with the Force E-Mail Policy which governs use of the E-Mail system.

3.1.2 Telecommunications systems include the private telephone system, E-mail, fax and modem transmissions. (This does not include the Force owned mobile telephones) Lawful Business Monitoring Regs apply only to transmissions over a private network - e.g: TVP)

3.2 The Lawful Business Practice Regulations

3.2.1 RIPA establishes a basic principle that communications may not be intercepted without consent and ensures compliance with the Human Rights Act 1998, Article 8 'Right to respect of private and family life'.

3.2.2 The Lawful Business Practice Regulations make an exception to this rule and allow businesses, which include public authorities, to intercept communications transmitted over their systems without consent for certain purposes, including

- i. Ascertain standards which are achieved, or ought to be achieved, by users.
- ii. Preventing and detecting crime.
- iii. Investigating or detecting unauthorised use of the business's telecommunications system.

3.2.3 Thames Valley Police will restrict the use of these regulations. This policy will be targeted at criminal or serious misconduct offences. Calls monitored for other purposes will be covered under the Voice Recording Policy.

4.0 Challenges & Representations

- 4.1** Challenges/representations in respect of decisions made in applying this policy should be addressed to:-

The Deputy Chief Constable

- 4.2** Challenges/representations in respect of the policy should be addressed to:-

Head of Professional Standards and Performance
Headquarters
Oxford Road
Kidlington
Oxon OX5 2NX

5.0 Guidance, Procedures & Tactics

5.1 Users of Thames Valley Police Telecommunications Systems

5.1.1 In all of these cases the regulations require businesses to make all reasonable efforts to inform every person who may use the systems that interception may take place. Accordingly, all potential users of the Thames Valley Police telecommunications systems are warned as follows;

5.1.2 You work in an organisation that deals with confidential and sensitive matters. You are required to maintain the highest professional and ethical standards. To ensure that these sensitivities and high standards are maintained, communications by all persons using the Thames Valley Police telecommunications systems (which includes telephone conversations, E-mail, fax and modem transmissions) may be monitored and recorded.

5.1.3 All staff, contract employees and everyone who may use Thames Valley Police telecommunications systems are reminded that their conversations and all other communications using these systems may not be considered private.

NOT PROTECTIVELY MARKED

5.1.4 The Thames Valley Police is emphatic in its determination that integrity is non-negotiable. If deemed appropriate, recorded communications will be used in criminal and disciplinary proceedings.

5.2 Authority for the Monitoring of Communications

5.2.1 Monitoring and recording of communications will be considered for the purposes outlined in paragraph 2.0 on an individual basis as to whether it is a proportionate method of investigation. An authority to monitor and/or record communications within Thames Valley Police communications systems will only be given by the Deputy Chief Constable. To ensure consistency an application on form RIPA 8 will be submitted via an officer of at least the rank of Superintendent within the Professional Standards Department. In the absence of the Deputy Chief Constable, the authorising officer will be the Assistant Chief Constable Local Policing in the first instance, thereafter the on-call ACC. Urgent verbal authority can be requested on form RIPA 8A. Monitoring and recording of communications will be targeted in response to specific concerns regarding potentially criminal or serious misconduct offences.

5.2.2 Historic E-mail usage enquiries may also be requested for the same reasons as outlined at paragraph 2.0. Such requests will be made on form RIPA 3Q and can only be authorised by an officer of at least the rank of Superintendent within the Professional Standards Department.

5.2.3 Thames Valley Police will endeavour to bring the contents of this policy to the attention of all potential users of its telecommunications systems. Area Commanders and Departmental Heads have a responsibility to ensure that their staff are made aware via internal communications systems.

NOT PROTECTIVELY MARKED**5.3 Documentation of Decisions and Decision Making Process**

Application for interception will be on form RIPA 8 via the Head of Professional Standards Department or his deputy to the Deputy Chief Constable for authorisation.

6.0 Communication**6.1 Links to Police National Legal Database Other**

There will be a link from the Policy and Procedures Intranet site to the Professional Standards and Performance Intranet site. Links will be made to existing ACPO/HMIC/Home Office policies and guidance documents relating to the interception of communications and the appropriate legislation governing this.

6.2 Communications Strategy

Force Intranet Site
Force Weekly Orders
Induction Packs (Police & Support Staff)

Target audience: All Thames Valley Police employees

7.0 Compliance and Certification**7.1 Human Rights Certification****(i) Legal Basis**

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

(ii) Human Rights Articles Engaged

It is acknowledged that this policy has the potential to engage the following Articles:-

- * Article 8 - "Right to respect of private or family life"
- * Article 10 - "Freedom of expression"

In the event that an Article of the Convention is engaged, then the legitimacy for the engagement is provided within the text of the Article:-

- * Article 8 - There shall be no interference by a public authority with the exercise of this right except as such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety for the prevention of disorder or crime, for the protection of

NOT PROTECTIVELY MARKED

health or morals, or for the protection of the rights and freedoms of others.

- * Article 10 - will apply to this policy in it's entirety.

(iii) Prohibition of Discrimination

By engaging any of the aforementioned Articles, there is a potential to engage Article 14 of the Convention. The enjoyment of the rights and freedoms set forth in the European Convention of Human Rights shall be secured without discrimination on any grounds, such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property or birth or other status. Actions taken as a consequence of this policy will be applied fairly and impartially, having due regard for natural justice and human rights.

7.2 Race Equality Impact Assessment

This policy has been graded as medium impact.

7.3 Data Protection

Personal data will be processed in accordance with the Data Protection Act 1998.

7.4 Freedom of Information Act

This policy is available to the general public.

7.5 Protective Markings

This policy has been assessed as being NOT PROTECTIVELY MARKED

7.6 Health & Safety at Work

8.0 Monitoring and Review

8.1 Links to Best Value/PPAF/Priorities/Performance Indicators

This policy does not have any direct links with the Best Value 5 year Review Programme.

8.2 Review Process

This policy document will be reviewed annually, in January, by the Administration Inspector, Professional Standards Department. The review will take account of the following criteria:-

- Changes in legislation

NOT PROTECTIVELY MARKED

- Court rulings – Domestic, European and Human Rights
- Examples of good practice from other Forces or other organisations
- Changes in Home Office Circulars
- Developments with ACPO Policy Unit
- Representations made by individuals and relevant organisations