

# Interception of Communications: The RIP Act and Lawful Business Practice Regulations

## Introduction

Two items of UK legislation were brought into force in 2000, pertaining to the interception of electronic communications. These are:

- *Regulation of Investigatory Powers Act 2000 (RIP Act)*
- *The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*

RIP establishes a new legal framework to govern the interception of electronic communications. It sets the rules regarding activities such as recording, monitoring or diverting communications in the course of their transmission over a public or private telecoms system. Interception of communications is permissible only where it can be justified on one of the following grounds:

- by virtue of an interception warrant duly signed,
- by demonstrating informed consent to the interception by *every* party to an intercepted communication; or
- in the absence of consent from all quarters, if the reason for the interception can nevertheless be justified by invoking the *Lawful Business Practice Regulations*

The *Lawful Business Practice Regulations* are defined in the second of the two items of legislation mentioned above. These allow businesses to intercept without consent for purposes such as recording evidence of transactions, ensuring regulatory compliance, detecting crime or unauthorised uses and ensuring the effective operation of their telecommunications systems. Businesses do not need to gain consent before intercepting for these purposes but they must have informed the users of the systems that interceptions may take place.

Electronic communications include telephone calls and facsimiles as well as all computer usage over the network.

## How does this apply to the University of Aberdeen?

The University of Aberdeen's electronic communications systems fall within the scope of this legislation. Any interception that takes place without explicit consent, must do so within the provision of the Lawful Business Practice Regulations.

Computer users are informed that such interception may take place through the *Conditions for Using IT Facilities* (Clause 11) and the accompanying *Notes for Guidance* – available online at [www.abdn.ac.uk/dit/policy.php](http://www.abdn.ac.uk/dit/policy.php). All users are issued with a copy of these on registration and receive an annual reminder of them at re-registration.

## Lawful Business Practice Regulations

The following summary of the regulations is extracted from the Explanatory Note appended to the Statutory Instrument.

Interceptions are authorised for -

- monitoring or recording communications -
  - to establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved (quality control and training),
  - in the interests of national security (in which case only certain specified public officials may make the interception),
  - to prevent or detect crime,
  - to investigate or detect unauthorised use of telecommunications systems or,
  - to secure, or as an inherent part of, effective system operation;

- monitoring received communications to determine whether they are business or personal communications;
- monitoring communications made to anonymous telephone helplines.

### **Examples of interception under the regulations**

The following are examples of interception that may take place on computer systems at the University of Aberdeen. This list is for illustrative purposes only; it is not exhaustive.

- Transaction logs are maintained for the purposes of performance monitoring and quality control
- Access and activity logs are maintained to enable investigation or detection of computer misuse or unauthorised use of the systems
- Monitoring to ensure the effective operation of the systems, for example
  - monitoring for and deleting viruses,
  - checking for and stopping other threats to the system, such as hacking or denial or service attacks,
  - monitoring automated processes such as net flow logs, e-mail logs, caching activity and load distribution.
- Inspection of file content to detect misuse

### **Inadvertent interception**

Systems personnel who operate and support electronic communications facilities need, from time to time, to monitor transmissions or observe transactional information to ensure proper functioning of University facilities and services. On these and other occasions, such personnel might inadvertently become aware of the contents of electronic communications. Except as provided for under the Lawful Business Practice Regulations, personnel are not permitted to intentionally examine the contents of transactional information or disclose or otherwise use what they have seen, heard or read. If, however, violations of University regulations or law are discovered, personnel are required to report these to the appropriate University authority.

### **Privacy protection limitations**

Regardless of the level of protection provided for electronic communications, confidentiality cannot be assured. Confidentiality might be compromised, for example, by law or policy, by unintended redistribution, or by the inadequacy of current technologies to protect against unauthorised access. Users should, therefore, exercise caution in using electronic communications to transmit confidential or sensitive matters.

### **Further information**

The legislation is available on the HMSO Web site:

- Regulation of Investigatory Powers Act 2000 (RIP Act)  
[[www.hmso.gov.uk/acts/acts2000/20000023.htm](http://www.hmso.gov.uk/acts/acts2000/20000023.htm)]
- Regulation of Investigatory Powers (Scotland) Act 2000  
[[www.scotland-legislation.hmso.gov.uk/legislation/scotland/acts2000/20000011.htm](http://www.scotland-legislation.hmso.gov.uk/legislation/scotland/acts2000/20000011.htm)]
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000  
[[www.hmso.gov.uk/si/si2000/20002699.htm](http://www.hmso.gov.uk/si/si2000/20002699.htm)]