

# E-Security Essentials

## Interception and Monitoring of Communications in FE and HE

**Betty Willder**

04 April 2006

**Please note:** this guidance has been prepared by **JISC Legal** for information purposes only and is not, nor is intended to be, legal advice. This information is not intended to constitute, and receipt of it does not constitute, a contract for legal advice or the establishment of a solicitor-client relationship.

### Table of Contents

1.Introduction.....	1
2.Interception.....	2
3 Lawful Authority .....	2
4 Acquisition and Disclosure of Communications Data.....	3
5. Essentials for colleges and universities .....	4

This essentials guide on aspects of E-Security is intended to provide readers with a direct, point by point guide on interception and monitoring law and its application to Further and Higher Education (FE and HE).

### 1.Introduction

Interception and monitoring legislation is a potentially contentious area for colleges and universities. It is important to strike a balance between the need on occasions to intercept or monitor communications (e.g. by the police for the prevention or detection of crime, or by the college or university itself for operational purposes) and the privacy and freedom of expression rights of the individual whose communications may be intercepted. New laws were therefore introduced to take account of advances in technology and to attempt to address the interests of both camps. The two main pieces of legislation in the UK with regard to interception of communications are:

- The Regulation of Investigatory Powers Act 2000 ('the RIPA')  
<http://www.opsi.gov.uk/acts/acts2000/20000023.htm> and
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ('the Lawful Business Regulations')  
<http://www.opsi.gov.uk/si/si2000/20002699.htm>.

It is important to emphasise at the outset that any interception should be regarded as exceptional by nature and must always be done on a clear legal base. Any action taken should always be directed to a statutory provision and must be proportionate to that purpose.

## **2. Interception**

### **2.1 Interception by a College or University**

In essence the RIPA provides that

- to intentionally and without lawful authority
- ... intercept a communication on a private system (e.g. the JANET connection) in the course of its transmission
- unless it is done or authorised by someone with the right of control e.g. the principal or his IT manager acting on his authority
- **... is a criminal offence**

It should also be noted that whilst it may not be a criminal offence for someone with the right of control or authorised, to intercept on a private system, there may be grounds for a civil action for damages if there is no **lawful authority** to intercept.

### **2.2 Interception by a third party**

- Interception on a private system by an external agency (e.g. the police) with the authority of a warrant is permitted for specific purposes, e.g. prevention or detection of serious crime.
- There is a legal obligation under the RIPA to assist the warrant holder and to maintain confidentiality.
- Failure to comply is a criminal offence.

### **2.3 Interception in the course of transmission**

Interception is defined widely in the RIPA and includes making some or all of the contents of the communication available, to someone other than the sender or intended recipient. It is thought that transmission may also cover access to both read and unread messages e.g. on a university central server.

## **3 Lawful Authority**

### **3.1 Lawful Authority to Intercept**

- Lawful authority is required to intercept.
- If there is no lawful authority then consent of the sender and receiver of the communication is needed.
- The RIPA allows some limited interception by the controller of the system without the consent of the sender or the recipient.
- The RIPA sets out the conditions under which third parties such as the police may intercept.

- The Lawful Business Regulations are the main source of lawful authority for the controller of the system to intercept and monitor. They permit the monitoring or keeping a record of communications to for purposes such as standards, national security, prevention and detection of crime, investigating unauthorized use, and ensuring effective system operation.
- The interception must also be relevant to the business of the system controller
- Every effort must have been made to tell users that interception may take place.
- A communication which has been intercepted and contains personal data is subject to the Data Protection Act 1998.

### **3.2. Possible examples of permitted interceptions**

- To check the content of e-mail to ensure that the institutions standards and quality control is not being breached or that third party standards are being followed e.g. the JANET Acceptable Use Policy
- To check that the system is being used for legitimate purposes only
- Under a valid warrant obtained by a specified authority e.g. the police or customs and excise etc
- Some measure of interception is likely to be essential to for example, check or prevent a virus spreading through the system, or to eliminate spam.
- Routine interception for operational purposes such as backing up or forwarding to the correct address.
- Monitoring (but not recording) may also be permissible to ascertain whether a communication is business or personal. An institution may need to check e-mails or voice mail for example in the prolonged absence of staff in accordance with an agreed institutional procedure
- Where a college operates a confidential helpline service, (for example a collaboration between the institution and the students union), monitoring (but not recording) of calls to support or protect the staff.

None of these examples should be taken as providing unlimited interception powers to colleges and universities and heed should always be paid to the purpose of the interception and the legal basis on which it is done. Staff and students should be clear as to the level of monitoring which may take place.

## **4 Acquisition and Disclosure of Communications Data**

The RIPA also sets out rules regarding communications data:

- Communications data refers mainly to traffic data and not to the content of messages.
- Specified authorities (for example the police or the Inland Revenue) may request that communications data is obtained by a service provider and disclosed to them for certain purposes e.g. prevention of crime.
- If required to obtain and disclose this data, a college or university should only do so on receipt of a formal notice from the requesting authority.

- There is currently no compulsory retention period for this data to be held by a private communications provider.

## **5. Essentials for colleges and universities**

Colleges and Universities as a minimum should have the following in place:

An email and internet policy which:

- Lets the user know what level of interception is likely to take place
- states the do's and don'ts for the user including whether personal use is permitted
- states the level of privacy the user can expect including whether 'cookies' or other information gathering devices are in use
- lets the user know the penalties for breach of the policy
- is linked with employment contracts, grievance and disciplinary procedures, and acceptable use policies
- has been cross checked with student and staff handbooks, departmental guidelines etc to ensure consistency
- forms part of induction training
- is visible to all e.g. consider notices at log in, on walls in computer suites, and regular on screen reminder notices to ensure ongoing visibility of the policy
- is reviewed on a regular basis

### **FE and HE establishments should also have in place:**

- a procedure for dealing with third party interception requests
- a procedure/guidelines for investigating misuse of the system

Having these policies and procedures in place will aid in compliance with the law but cannot guarantee complete protection in what is recognised as a difficult area of the law which in many respects has still to be interpreted by the courts.

**Betty Willder**

04 April 2006

© JISC Legal - [www.jisclegal.ac.uk](http://www.jisclegal.ac.uk)