



Date	Version	Author	Comments
07/2002	F01	ITS	Ratified by the Information Technology Policy Committee 11/2002
10/2008	D01	Duncan Woodhouse	Updated to refer to Information Security Policy 2008 and in line with ISO 27001
11/2008	D02	Duncan Woodhouse	Review and comments by Senior Assistant Registrar
01/2009	D03	Duncan Woodhouse	Review and comments by Deputy Registrar

University of Warwick Statement on the Regulation of Investigatory Powers Act 2000: E-mail and Telephone Monitoring

1. Introduction

The University respects the privacy of its users and there is no routine monitoring of e-mail content or individual Web access. However, users should be aware that the University may make interceptions in certain circumstances under the terms of the Regulation of Investigatory Powers (RIP) Act as outlined below.

The RIP Act statement is part of the strategic Information Security Policy.

The RIP Act statement is designed to the ISO 27001 standard. Subsequently this policy shall be reviewed regularly and updated as necessary to ensure that it remains appropriate in the light of any changes to legal, contractual or acceptable use obligations.

2. Objectives

The objective of the Warwick statement on the RIP Act is to ensure members of the University are fully aware of reasons in which email and telephone communications may be intercepted and investigated. The Act is referred to in the University's Information Security Policy and is clarified within this document.

3. Scope

The University of Warwick statement on the Regulation of Investigatory Powers Act 2000 applies to all staff and student members of the University.

Author: Duncan Woodhouse, Assistant Registrar for Information Security, Risk Management and Business Continuity

Date: 02/10/08

4. The RIP Act

The Regulation of Investigatory Powers Act 2000 replaces the Interception of Communications Act 1985 to take account of technological advances in communications and to accommodate the expanding use of e-mail and the internet.

The Act can be seen in full at the [HMSO web site](#). The Act regulates the power of government security services and law enforcement authorities by allowing the interception, surveillance and investigation of electronic data in specified situations such as when preventing and detecting crime. Powers include being able to demand the disclosure of data encryption keys.

In addition, the Act empowered the Secretary of State to make regulations which allow businesses to intercept communications in the course of lawful business practice and in specific circumstances without the express consent of either the sender or the recipient. Under the regulations, businesses are required to make all reasonable efforts to inform users of their own systems that such interceptions might take place. These regulations are titled The Telecommunications (Lawful Business Practice) (Interception of Communication) Regulations 2000 and can be seen in full at www.hmso.gov.uk under Legislation, Statutory Instruments, 2000, No. 2699. The University is a business under the Regulation of Investigatory Powers Act 2000.

The Regulations allow businesses to intercept communications without consent in the following circumstances:

- To establish the existence of facts (for example to obtain evidence of a business transaction)
- To ascertain compliance with regulatory or self regulatory practices or procedures relevant to the business (to ascertain whether the business is abiding by its own policies)
- To ascertain or demonstrate standards which are achieved or ought to be achieved by persons using the system (for example staff training or quality control, but not for market research)
- To prevent or detect crime (including crimes such as fraud as well as infringement of IT related legislation such as the [Computer Misuse Act 1990](#) or the [Data Protection Act 1998](#))
- To investigate or detect unauthorised use of the systems (e.g. to check whether the user is breaking regulations)
- To ensure the effective operation of the system (e.g. to protect against viruses or other threats such as hacking or denial of service attacks, to monitor traffic levels, to forward e-mails to correct destinations)
- To check whether or not communications are relevant to the business (e.g. checking email accounts when staff are absent on holiday or sick leave to access business communications)
- To monitor (but not record) calls to confidential, counselling helplines run free of charge by the business, provided that users are able to remain anonymous if they so choose.

Author: Duncan Woodhouse, Assistant Registrar for Information Security, Risk Management and Business Continuity

Date: 02/10/08

5. The University application of the RIP Act

The University may make interceptions for the purposes authorised under the Regulations, and will make all reasonable efforts to inform users of its systems that communications may be intercepted.

The University's Acceptable Use Policies provide essential information to users of University computing facilities about what does and does not constitute acceptable use. All inappropriate use of computing facilities, including e-mail and the Internet, no matter how encountered, will be investigated.

The University reserves the right to investigate and inspect electronic communications, under the terms of the Act. In particular, files, access logs, email etc relating to individuals may be monitored in the following circumstances:

- In the investigation of an incident e.g. alleged contravention of University rules, regulations, contracts etc or alleged criminal activity
- Investigation of abnormal systems behaviour in an operational context e.g. abnormally high network traffic from a particular device, degradation of systems for other users resulting from the activity on a specific device etc
- Problem-solving e.g. ensuring a file transfer takes place; the user would normally instigate this but, on occasions, the intended recipient raises the query and the sender is unavailable

Users should note that email is not an entirely secure medium and could be seen other than by the intended recipient, including authorised system administrators carrying out their normal support duties.

The University believes its policy on the privacy and the interception of electronic communications, as summarised above, achieves a balance between the rights of individuals and the need to protect users and the University from the consequences of misuse or illegal activity.

6. Responsibilities

The Information Policy and Strategy Committee¹ are responsible for the University of Warwick Statement on the Regulation of Investigatory Powers Act 2000: E-mail and Telephone Monitoring.

The University has established a strategic information security, risk management and business continuity function within the Deputy Registrar's Office. The Senior Assistant Registrar and Assistant Registrar for information security will be responsible for development of the policy, will co-ordinate implementation and dissemination, and will monitor operation.

¹ On behalf of SENATE

Author: Duncan Woodhouse, Assistant Registrar for Information Security, Risk Management and Business Continuity

Date: 02/10/08

Heads of Departments, with support from the Deputy Registrar's Office, are responsible for ensuring that members are aware of the University of Warwick Statement on the Regulation of Investigatory Powers Act.

Everyone granted access to University information systems has a personal responsibility to ensure that they, and others who may be responsible to them, are aware of the statement on the RIP Act.

7. Policy Awareness and Disciplinary Procedures

The University of Warwick Statement on the Regulation of Investigatory Powers Act will be made available to all staff and students via the web as part of the Governance site, maintained by the Deputy Registrar's Office, dedicated to the explanation and promotion of the policy. Staff, students, authorised third parties and contractors given access to the University information systems will be advised of the existence of the relevant policies, codes of conduct and guidelines. Users will be asked to confirm that they understand the policy before being given access to some systems.

8. Information Security Education and Training

The University recognises the need for all staff, students and other users of University systems to be aware of information security threats and concerns, and to be equipped to support University security policy in the course of their normal work. Appropriate training or information on security matters will be provided for users and departments will supplement this to meet their particular requirements.

9. Maintenance

The University of Warwick Statement on the Regulation of Investigatory Powers Act will be monitored by Information Policy and Strategy Committee and reviewed as necessary. Revisions will be subject to appropriate consultation.

The Deputy Registrar's Office will report on a summary and exception basis, will notify issues and bring forward recommendations.

10. Related Policies

- Strategic information security is covered by the Information Security Policy 2008/2009
- Use of University computing facilities is covered by Regulation 31 - Regulations governing the use of University Computing Facilities
- Incidents related to bullying and harassment are covered in the Dignity at Work and Study Policy