LONDON'S GLOBAL UNIVERSITY

UCL Policy on monitoring Computer and Network Use

Information Security Policy

University College London

Document Summary

Document ID	TBD
Status	Approved
Information Classification	Public
Document Version	Endorsed by the Information Strategy Committee, 1 March 2007

University College London, Gower Street, London WC1E 6BT
Tel: +44 (0)20 7679 2000
www.ucl.ac.uk

1. Introduction

There are circumstances where UCL may monitor or record communications made using its computer and telecommunication systems, or examine material stored on those systems. This document sets out UCL's policy in respect of such activity.

It is important to be aware of the distinction made between:

- intercepting information **in transit** - email messages being sent, for example, or watching the web pages visited - here the relevant law is found in the Regulation of Investigatory Powers Act 2000 (RIPA) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBPR);
- examination of material **stored** on a computer - the law applicable here may vary according to variables such as who owns the computer, what material is being examined, and how the material is examined. However, the Human Rights Act 1998 and the Data Protection Act 1998 provide an over-arching framework to protect the individual's right to privacy[(1)].

Under the Regulation of Investigatory Powers Act 2000, unlawful interception of communications on the UCL computer network may lead to criminal proceedings against an individual operating without the institution's authority; unlawful interception may also lead to civil action against the institution where the institution authorized the interception. The RIPA and LBPR do, however, allow for legitimate interceptions of communications by organisations on their private computer and telecommunications networks - in other words, they provide 'lawful authority'.

2. Scope

The part of this policy covering the interception of information applies to any communication on or through University College London's computer systems - the latter term being taken to include all components of the network as well as the computers (whether or not they are owned by UCL) attached to it.

Policy concerned with the examination of stored material applies to **any** computer facility provided by UCL.

3. In what circumstances can monitoring occur?

Provisions in the LBPR permit UCL to intercept and record information which can be associated with an individual's communications via UCL services (whether made for purposes associated with UCL's business or activities or otherwise). This may only be done where UCL has made reasonable efforts to inform potential users that such interceptions may be made, and in order to achieve the following aims:

- to prevent or detect crime;
- to investigate or detect unauthorized use, including the use of systems outside UCL;

- to ensure the effective and authorized operation of systems;
- to establish the existence of facts necessary to ascertain compliance with regulatory or self-regulatory procedures, or to ascertain or demonstrate standards
- for other lawful purposes as set out in the relevant legislation;

Stored material (including electronic mail) may also be examined for these purposes. In addition, UCL may access stored material in the event of an urgent need (see section 7).

UCL may also monitor but not record:

- received communications to determine whether they are business or personal communications;

'Authorized use' of UCL facilities is defined in section 2 of the UCL Computing Regulations (see references below). It should be noted that although reasonable personal use of facilities is permitted, excessive use that disrupts or distracts an individual from the efficient conduct of UCL business, or involves accessing or sending unlawful or offensive material (for example, obscene, discriminatory or abusive material), is prohibited; and, consequently, monitoring may take place to detect or investigate such behaviour.

Note that the law distinguishes between monitoring for operational and policy reasons. Both classes of activity must be authorized. Note that the authorization mechanisms are different for the two cases.

3.1. Monitoring for operational reasons

Most providers of IT services within UCL routinely monitor their systems to ensure that they are performing properly. This reflects standard good practice, and normally involves only aggregate anonymous data that does not identify individuals or the contents of their communications. Information Systems, for example, records the number of email messages passing through its servers each day, and the time it takes to deliver messages, to help with capacity planning. This type of monitoring does not fall within the RIPA, as it does not involve interception, and by virtue of not identifying individuals, it does not trigger laws relating to personal privacy.

However, a general exemption in the RIPA permits UCL to intercept certain communications where the interception is by an authorized person for purposes connected with the provision or operation of a service, for example:

- email postmasters may examine mis-addressed messages in order to redirect them as necessary, or check email subject lines for malicious code;

- system operators may monitor system traffic to determine its source, where this is necessary to ensure the effective performance of their mail servers, for example to eliminate unsolicited commercial email (UCE or 'spam').
- System and network managers may investigate which system and/or individual is the source of a denial of service attack.

The RIPA LBPR requires that persons carrying out routine monitoring under this exemption must be properly authorized either through their job description or by written authorization from their Head of Department or Division Head (see section 4 below).

Persons carrying out monitoring for operational reasons must be alert to the focus of their investigation changing. If, at any stage, monitoring or access to stored material is required to investigate matters of policy (or legal) compliance the appropriate authorization must be obtained as described in sections 3.2 & 4.2.

3.2. Monitoring for policy (and legal) compliance

All other activities falling under the exemptions within the LBPR will constitute monitoring for policy or (legal) compliance. Each individual act of monitoring for this purpose must be specifically authorized and documented as described in sections 4 and 5.2, respectively.

4. Who can authorize monitoring of computer or network use?

The law distinguishes between monitoring for operational and policy reasons. However, both classes of activity must be authorized. Note that authorization mechanisms are different in the two cases.

4.1. Routine monitoring for operational reasons may be authorized through staff job descriptions or by written authorization from one of the following (or their deputies) as appropriate:

- the Head of the Computer Security Team (in pursuance of security issues)
- the Head of Department/Division or Dean of Faculty (in relation to systems under his/her authority).

4.2. Monitoring or access to stored material to investigate policy (or legal) compliance may only be carried out with written authorization from one of the following (or their deputies) as appropriate:

- the Director of Human Resources (in pursuance of staff disciplinary matters)
- the Registrar (in pursuance of student disciplinary matters)
- the Head of the UCL Computer Security Team (in pursuance of security issues)

- the Head of Department/Division or Dean of Faculty (in relation to systems under his/her authority).

In **addition**, written authorization must be obtained from the Head of the UCL Computer Security Team **and** the UCL Data Protection Officer. Note that authorization covers an individual act of monitoring and only for the purposes and scope indicated on the authorization form.

4.3. The Information Strategy Committee will oversee monitoring. All results of monitoring user communications or stored data must be reported to the Head of the UCL Computer Security Team as soon as the monitoring is completed. The Head of CST will submit a report to ISC and also provide an anonymized summary to the Security Working Group.

4.4. Attempts by any member of staff to implement monitoring without proper authorization will be in breach of this policy and may be the subject of disciplinary proceedings. Unauthorized monitoring may also attract civil or criminal liability.

UCL recognises that, due to the nature of computer systems, data held on its computer systems, passing across its networks, or printed out on UCL equipment, may at times be visible in readable form. In such circumstances, that data may well be viewed by UCL staff. Such incidental/inadvertent viewing will not constitute a breach of this policy, even where such viewing leads to the implementation of authorized monitoring and/or disciplinary procedures against the user concerned.

5. Procedures for monitoring computer or network use

5.1. In most circumstances where communications are to be intercepted, the RIPA and LBPR require that for the interception to be lawful, users of the service must have been informed **in advance** that interception may occur. Failure to adequately inform the users of the possibility of interception may result in their having a legitimate expectation of privacy in their communications on the service, and make the interception unlawful. This might render the material intercepted useless for the purpose of disciplinary or legal proceedings, and could render UCL liable to a civil lawsuit.

The following message should be displayed wherever UCL systems are used (e.g. labels on screens):

Communications, including personal communications, made on or through University College London's computing and telecommunications systems may be monitored or recorded to secure effective system operation and for other lawful purposes.

*See **www.ucl.ac.uk/privacy** for more information.*

The following should be used as part of the login banner of **all** UCL systems (capable of supporting a customizable banner) so that it is displayed to and acknowledged by users:

Use of this systems is limited to authorized individuals only. You are committing a criminal offence under the Computer Misuse Act 1990 sect. 1 if you attempt to gain unauthorized access either to this system or any others at this site.

Communications, including personal communications, made on or through University College London's computing and telecommunications systems may be monitored or recorded to secure effective system operation and for other lawful purposes.

By using this system, you accept that monitoring may take place.

Similarly, it is important to remind users of the limits on their privacy in connection with stored material. The above URL includes a reference to this policy, but in addition explicit mention of the policy should be made in documentation given to staff or students when they are granted access to any IT facilities, or during their induction.

5.2. The application form for authorizing specific monitoring for policy (and legal) compliance (section 4.2) should document:

- the reason for monitoring, including any internal disciplinary offence or suspected or alleged civil or criminal act which may have been committed and an indication of why this is felt to be a proportionate approach
- the scope of the monitoring
- the intended duration
- the names or job titles of those who will be carrying out the monitoring. A witness **must** always be present.
- steps taken to protect the privacy of the person or persons being monitored.

5.3. If there is any likelihood that an internal disciplinary offence or suspected or alleged civil or criminal act may have been committed which may result in disciplinary or legal action resulting from an investigation, specialist advice on the preservation of evidence should be sought before proceeding. UCL's Computer Security Team (email: ***cert(at)ucl.ac.uk***, tel.: 020 7679 7338) should be contacted in the first instance, and will act as liaison with law enforcement agencies as necessary.

6. Examples of monitoring

The following scenarios are intended to illustrate some of the foregoing discussions. The first two examples are based closely on material taken from the JISC senior management briefing paper (see below).

6.1. Ms. C, a staff member of UCL, illicitly uses the UCL computer network to record the web sites visited by Mr. D, a student at UCL. Ms. C does not have the express or implied consent of the College to do this. This interception is intentional and without lawful authority. **It is a criminal offence.**

6.2. Mr C, a staff member of UCL, acting on a memo from an officer of the College, uses the UCL computer network to intercept emails sent by Mr D, a member of the College. Mr C has the express or implied consent of the person with a right to control the relevant private telecommunications network (the relevant officer of the College). This is not a criminal offence. However, the officer of the College must have a lawful purpose for requiring the intercept, such as suspicion of unauthorized use. **If the intercept is made without a lawful purpose, both the officer of the College and UCL may face civil liability.**

6.3. A complaint is received that a UCL email address is being misused to send unsolicited commercial email. This is a violation of the UCL Computing Regulations. It is decided to investigate by monitoring messages sent from this email address. Having previously informed users of the relevant email system that monitoring/recording may take place (section 5), the relevant person (as set out in section 4 above) should issue written instructions authorizing the monitoring.

6.4. A member of staff is suspected of spending large amounts of time downloading inappropriate material on their computer, to the point where there is an adverse impact on their ability to perform their duties. As an investigation is likely to lead to disciplinary action, the Director of Human Resources should provide instruction on how the matter is to be pursued, and specialist advice may be required on how to preserve evidence. The success of any action may depend on whether it can be shown that the individual concerned had been properly made aware of what constitutes ‘acceptable use'.

6.5. Mr. E, who administers a computer system used by a number of departments, discovers that the system disk is almost full. To ensure effective system operation, Mr. E checks users' quotas, and finds that one member of staff has filled up the disk with what appear to be MP3 music files. The presence of these files is likely to represent a violation of the UCL Computing Regulations. However, before investigating further, Mr. E should seek authorization from the appropriate person (c.f. sections 5.1 and 5.2 above).

7. Access to stored documents (including email) for business purposes

There are occasions when UCL needs to access information held by a member of UCL within electronic mail, elsewhere on his/her computer, or in other filestore or backup media. This will usually occur when an employee is absent, either ill or on leave, and a situation arises which requires a rapid response. Members of UCL must be made aware that the College reserves the right to obtain access to files held on/in equipment owned by UCL, and that the privacy of personal material stored on/in such equipment in the event of authorized access cannot be guaranteed.

Persons facilitating such access (e.g. IT support staff) must **on each occasion** obtain written authorization from a person listed in section 4.2. The authorization must identify the material to be accessed, its location and why a delay in access would be detrimental to UCL's interests. If the location of the material is not precisely known the application must describe the proposed search methodology. The request must be authorized by the UCL Data Protection Officer. A log of operations carried out and material accessed must be maintained and signed by the person facilitating access and a witness. A copy of this log and the completed authorization form must be given to the owner of the material accessed. Advice on appropriate methods for carrying out this work is available from UCL Computer Security Team.

It is intended that these arrangements are for exceptional circumstances only: applications will only be considered if they demonstrate that delay will cause disproportionate damage to UCL's interests. Normal business processes should avoid their necessity through use of role email addresses or lists, appropriate file access control, etc.

Persons facilitating access must take all reasonable measures to respect privacy. However, difficulties may arise when searching for material, as there is no guaranteed method of distinguishing between business and personal items. Users are advised to minimize the risk of inadvertent viewing of private material by placing appropriate messages or files in folders (or directories) whose name includes “Personal”. (Mail filters can be set up to move messages automatically into folders according to sender or destination address, etc.)

8. Exceptional Modification of User Files

In exceptional circumstances, system custodians may need to make changes to user filestore. Examples include disabling programs which may adversely affect system or network performance, disabling software which is being used contrary to licensing arrangements or removing from public view confidential files or offensive material.

The permission of the file owner should be obtained unless the situation is of such urgency as to make this impracticable. Each filestore change and the associated justification must be logged. The file owner must be informed of the change and the justification as soon as possible.

The custodian may not, without specific authorization from the appropriate authority, modify the contents of any file in such a way as to damage or destroy information. If necessary, files should be moved to a secure off-line archive.

9. Status of this document

This document is a part of UCL's information security policy and has been endorsed by UCL's Information Strategy Committee.

10. References

The UCL Computing Regulations may be found at:
http://www.ucl.ac.uk/cert/swg/policy/Regulations.html

A very clear document containing examples of how the legislation applies in practice has been produced by the Joint Information Systems Committee, which promotes the use of information systems and information technology in Higher and Further education across the UK. It can be downloaded from:

http://www.jisclegal.ac.uk/LegalAreas/InterceptionandMonitoring/InterceptionandMonitoringLawEssentials.aspx

Relevant legislation includes:

The Regulation of Investigatory Powers Act 2000
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
http://www.hmso.gov.uk/si/si2000/20002699.htm

The Human Rights Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980042.htm

The Data Protection Act 1998
http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Employment Practices Data Protection Code Part 3 Monitoring at work
https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

(1) A list of the relevant legislation is provided at the end of this document.