

# Policy and Procedure for Granting Non-consensual Access to Email

---

## 1. Preamble

This policy for granting non-consensual access to University email accounts is proposed so that existing email users are aware of the procedures and policies that may be applied in their absence. This policy currently reflects the working procedures and practices being operated by ISS.

There is a steady flow of requests for non-consensual access to University email accounts and this policy aims to formalise the protocol for dealing with such requests. Non-consensual requests are the exception rather than the rule and a central record of these requests and whether the request is granted will be held by the Director of ISS and available for audit. Granting non-consensual access to email is the 'option of last resort' when consensual access is unavailable.

The policy aims to protect university employees by making clear the circumstances under which they may access an account holder's email and lays down a formal procedure to follow to do so.

Once adopted, this policy will govern all email accounts administered by Lancaster University.

Three points should be emphasised:

1. It should be noted that there are already approved procedures in place to address the case where criminal misuse of the University's ICT systems is suspected. These procedures authorise *inter-alia* the non-consensual access to email for the purposes of determining whether there may be substance in such criminal misuse allegations. Those investigative procedures take precedence over the procedures defined in this policy.
2. It should be further noted that any alleged substantive breach of the University Rules for the Use of Electronic Information Systems may require non-consensual access to email content on University systems. A request for such access will be considered on a case by case basis by the Director of ISS, after consultation with the appropriate Dean or Senior Officer as appropriate.
3. Users should be aware that basic Email security is weak. Email is transmitted in clear text and can be intercepted and read clandestinely at many points in its journey. To use a crude analogy, users should regard the security of non-encrypted email as being similar to that of a postcard, or a letter in an unsealed envelope, passing through a collection, sorting and delivery system.

## 2. The Policy for non-consensual access to email

### 2.1. Who may request non-consensual access

Heads of Department may request either access to an email account or the forwarding of incoming email destined for a member or former member of staff or department sponsored visitor. Heads may request that an out-of-office message be set on the email account. Where the email account holder is a direct report to the Head of Department, then the request must come from that Head's own line manager. The request will stipulate when such access is to be revoked.

Personal tutors and Heads of Department may request access to a student account.

The University Secretary may request access to any account that is held on institutional systems after consultation with the appropriate Faculty Dean or senior body.

### 2.2. Acceptable Use Policy for those Granted Non-consensual Access to Email

Individuals who have been granted non-consensual access to an email account:

- a. Must not use this grant of access to obtain records other than those required to continue University business in the holder's absence.
- b. Must limit their inspection of records to the least perusal of contents and the least action necessary to obtain the needed information.
- c. Must not seek out, use, or disclose personal information contained in the email except for University business purposes.
- d. Must not breach the Lancaster University Rules for Use of Electronic Information Systems<sup>1</sup> or assume false identity.
- e. Must take all necessary steps to protect the access and account from unauthorized use.

### 2.3. Processing requests for Non-consensual Access to Email

- a. All requests for non-consensual access to email should be made in writing to the Director of ISS (or nominee in case of absence) The Director of ISS (or nominee), will make a timely response consistent with the situation motivating the request.
- b. When it is necessary to sustain the routine operation of the University or in cases of disability or death, upon direction by Director of ISS (or nominee), managers of email systems will, where technically feasible, forward email to another without the consent of the original recipient.
- c. Individuals whose email is forwarded to another will be informed of this action (if possible).

---

<sup>1</sup> <http://www.lancs.ac.uk/iss/governance/rules.htm>

- d. Reasonable attempts will be made to identify alternative actions to the redirection of email messages. Such alternatives include the insertion of an automatic reply message advising senders that the recipient is not available and suggesting an alternate recipient.
- e. The Director of ISS will submit an annual summary of requests for *non-consensual access to email accounts* to the Director of Human Resources and to the Academic Registrar respectively on 31<sup>st</sup> July.

#### **2.4. Revoking Non-consensual Access to an Email Account**

- a. The initial period of non-consensual access to email will be limited to 3 months. Two weeks notice will be given after which access is revoked. .
- b. Non-consensual access to email will be revoked upon the return of a member of staff to work or a student to their studies.

### **3. Access by University Email Administrators and System Administrators**

Mail communication is divided into “traffic data”, which is control information used to route the messages, and “content data” which is the information in the messages and attachments. Access to traffic data is an essential part of system management. The nature of the management tools used and operational requirements make it unavoidable for administrators to see the source and destination of messages, and often their subject lines.

Administrators of all University mail systems are required to seek explicit, informed consent from the recipient/ sender of an incoming/outgoing message before they examine its content. Very occasionally, there may be an operational requirement (e.g. system performance or security issues) where prior approval by the message recipient/sender to study content data is infeasible. Where prior consent is not available, written authorisation can be granted by their Head of Department; the message recipient/sender will be retrospectively informed. Whether or not user consent is obtained, full details of what has been done will be recorded for future audit.

The Administrator is bound by the Section 2.2 (above) and is additionally obliged, within 24 hours, to provide their Dean or Director with a report of their actions for the purposes of future audit.

### **4. The Regulation of Investigatory Powers Act 2000 (RIPA)**

This section is included for completeness and is informed by a JISC Legal publication<sup>2</sup>. To quote from section 4.2 of this document:

*The RIPA allows colleges and universities to carry out the following interceptions without the consent of the sender or the receiver of the communication:*

---

<sup>2</sup> [www.jisclegal.ac.uk/eseconomy/eseconomy.html](http://www.jisclegal.ac.uk/eseconomy/eseconomy.html).

- *the interception by or on behalf of the person running a service , for the purposes connected with the provision of the service - a possible example might be readdressing wrongly addressed email, or checking subject lines in email for viruses.*
- *The monitoring of system traffic to ensure effective performance - a possible example might be finding out the source to cut down spam.*

There are also additional conditions set out in Section 4.3 of the same JISC Legal Publication:

- *the interception must be made solely for the purpose of monitoring or (where appropriate) keeping a record of communications relevant to the system controller's business i.e. relevant to the business of an FE or HE establishment*
- *every effort must have been made to inform users that this monitoring and recording may take place.*

This last bullet point is covered by the statement in the Message of the Day, and through publishing the policy outlined in the earlier sections.

The closing advice in Section 4 is:

*As a final thought, it must not be forgotten that the Human Rights Act should lead to a narrow interpretation of both the exceptions under RIPA and the permitted acts under the Lawful Business Regulations. Therefore colleges and universities should always take care not to take disproportionate action. Some communications may also involve confidential relationships and the exceptions and permitted acts are unlikely to justify excessive or unlimited interference.*

## **5. Advice from the Information Commissioner's Office**

Again, to give a framework to the 'Non-consensual Access to Email Policy', the following quotation is from the Employment Practices Code<sup>3</sup>, Part 3 Monitoring at Work (page 60):

*Interception without consent is allowed if it is to monitor, but not record, communications to check whether they:-*

- *involve the business entering into transactions*
- *relate in another way to the business*

*For example, an employer may open e-mails in an absent worker's in-box if this is necessary to see whether there are business communications that need to be dealt with in the worker's absence. However, the employer should not open e-mails that in their unopened state appear not to relate to the business, e.g. e-mails that are marked 'personal' in the header, unless there are convincing grounds on which to believe they are in fact business related.*

---

<sup>3</sup> [http://www.ico.gov.uk/what\\_we\\_cover/data\\_protection/guidance/codes\\_of\\_practice.aspx](http://www.ico.gov.uk/what_we_cover/data_protection/guidance/codes_of_practice.aspx).