E-mail rules

These e-mail rules concern all users of the university's e-mail systems. The parts aimed at university staff members concern all of the University's units, their employees and other users in corresponding positions (such as scholarship-funded researchers and emeritus/emerita professors). The rules also concern all users responsible for e-mail systems.

The e-mail rules comply with the currently valid laws and regulations.

The sender is responsible for making sure that the message delivery has been successful. Particularly crucial messages should be sent well before the deadline, and the recipient should be asked to confirm receipt.

Privacy of correspondence also applies to e-mail

If a user receives an e-mail message intended for another person, the unintended recipient is obligated to maintain the secrecy of the message and refrain from utilising its contents or the knowledge of its existence.

- According to the Administrative Procedure Act (434/2003), section 21, a document delivered by mistake and dealing with administrative matters beyond the recipient's competence shall be transferred to the authority deemed to be competent, and the sender of the document shall be informed about the transfer; if such a transfer is not possible, the message shall be returned to the sender and deleted from the university's e-mail system.
- All other received messages intended for another user must be returned to the sender.

The forwarding and returning obligation does not concern messages containing malware or spam.

E-mail addresses

The organisation address is an official e-mail address

The organisation address is used for official matters and service provision.

The organisation address is formed according to a certain formula, for example:

- university-level: office@lut.fi
- unit-level: unit@lut.fi
- role-level: rector@lut.fi

The work e-mail is a personal e-mail account provided for work-related use

Work e-mail messages are related to both the work e-mail account and the user's job.

As default, the University considers e-mail messages received to the work e-mail account to be private messages.

In outgoing e-mail messages, the organisation address or the work e-mail address formed from the user's name must be given as the sender's address.

The study e-mail is a personal e-mail account provided by the University for its students

The study e-mail account is primarily intended for study-related use.

The University considers students' e-mail messages to be private messages.

The sender's address in outgoing e-mail messages is the study e-mail address formed from the student's name.

The student can forbid the publishing of his/her e-mail address outside the University.

Every e-mail service user is personally responsible for keeping his/her mailboxes clean and ensuring that the reserved space does not run out.

The University determines the e-mail addresses and their format

Various domain-based addresses related to certain roles can be used, for example:

- organisation addresses could be of the format service@university.fi
- staff members' addresses could be of the format john.smith@staff.university.fi
- students' addresses could be of the format brian.kottarainen@students.university.fi

Staff and student e-mail addresses are formed from the user's name

If another user with exactly the same name joins the University, the original user's e-mail address remains the same. Characters or initials will be added to the newcomer's address.

Use of e-mail and e-mail addresses

- The name-based address must be used as the personal e-mail address.
- The organisation address or work e-mail address must be used in work-related matters.

The handling and archiving of e-mail messages are governed by the university's archive creation plan. Further information is available from the university's Records Services, asiakirjapalvelut@lut.fi.

- It is forbidden to transfer or automatically route e-mail messages from the organisation or work account outside the University; this is due to reasons related to information security, data protection and information management; in addition, it may constitute a breach of the Personal Data Act.
- If a received message contains a confirmation request or is part of an e-service[1], the message handler must send the confirmation immediately.
- Only e-service systems are allowed to use automatic receipt confirmations.

Organisation addresses have owners

The owner must make sure that messages received in the organisation address are handled on a regular basis and according to the archive creation plan, even when the owner is absent.

- E-mail messages received in the organisation account belong to the employer.
- The address owner must respond to any received messages immediately.
- The response must indicate that it is a reply to a message sent to an organisation address.
- Organisation addresses must not be used for personal communications.

Messages related to work e-mail accounts are treated as private messages

- The University can retrieve and open an employee's e-mail messages in certain cases and certain ways as defined in separate guidelines.
- Work-related e-mail messages sent by employees must, when applicable, clearly indicate whether they are official statements related to work or the employee's personal opinions.

The e-mail account provided by the University can be used for private purposes within the limitations set forth in the University's Rules of IT Service Use.

- Employees must clearly separate their personal and work-related e-mail messages, both those received and sent.
- If a user is both a student and a staff member, the e-mail messages related to each role must be clearly separated from each other.

External e-mail accounts must not be used for university-related tasks

Access to external e-mail services from the university network can be technically restricted, if such services are deemed to form a major data security risk.

---

[1] Here, the term 'e-service' refers to the electronic registration, completion and processing (incl. resolution) of administrative matters, informing about decisions, or sending a trial document in electronic format to a public court or to a person authorised by such an instance.

Use of personal auto replies

Despite the risk of increased spam flow, the University recommends the use of auto replies. They should advise the recipient to contact the relevant organisation address or substitute.

E-mail must be monitored even during absence

One option is to close the mailbox (for example, during long leaves of absence). The recommended practice is to instruct clients to use the respective organisation address for all contacts.

The e-mail account is fixed-term

Personal messages should not be left in the university mailbox when the usage right expires.

Employees must agree with their supervisor on the transfer of work-related messages to another user within the university organisation. If an employee resigns from his/her duties before the expiry of the employment contract, the employee, or his/her supervisor, can request the discontinuation of incoming e-mail immediately.

E-mail messages can be encrypted

- If a received organisation- or work-related e-mail message is encrypted so that only the recipient can decrypt it, the message must be decrypted immediately after receipt. This rule does not apply to messages containing malware or spam.
- After decrypting, the message can be encrypted again so that all handlers can open it.

In terms of information security, non-encrypted e-mail can be compared to a postcard.

Mailing lists have owners

The owner must keep the list moderated, regularly check that it is up-to-date and remove any redundant addresses from the list.

- The list owner is responsible for maintaining and removing joint mailing lists.
- Personal mailing lists are each user's own responsibility.

A mailing list forms a person register and, hence, it may be subject to confidentiality obligations and separate limitations of disclosure. If such rules apply, use the blind carbon copy (bcc) function in order to keep the list's addresses hidden from recipients.

Mass mailing and sending/forwarding chain letters is forbidden

Exceptions to this rule can be made upon separate decisions.

Service provision and administration

System administration can intervene in e-mail traffic

in order to secure the service level or safety of the e-mail system. Such interventions, as well as e-mail usage monitoring and log-keeping, are governed by separate instructions.

E-mail is checked and filtered

All e-mail traffic goes through an automatic content analysis, based on which

- messages and attachments containing malware are automatically deleted;
- the delivery of harmful, oversized or numerous attachments can be restricted.

In addition, filtering and deletion without notification can be applied to messages

- sent from known spam servers;
- classified as spam based on the automatic content analysis.

The e-mail address no longer works

when the usage authorisation has expired. Messages sent to a user whose e-mail account is no longer valid will not be delivered; instead, an automatic message is sent to inform the sender about the expiry of the address. When an e-mail account expires, all its re-routing arrangements also become invalid.

Other clauses

Entry into force

These e-mail rules become effective on 18 December 2013 and replace the earlier version of corresponding rules.

Change management

These rules will be reviewed when needed to ensure that they comply with all valid services and laws. Any significant personnel-related changes are addressed according to the co-operation procedure. The CIO makes decisions concerning change needs.

Information about changes is provided through the regular communication channels, never personally.

Deviations from the e-mail rules

Permission for exceptions to the e-mail rules can be granted for compelling reasons upon a written application. Permits are granted by the CIO. The permits may include additional terms and conditions, restrictions and responsibilities.

Monitoring

Compliance with the e-mail rules is overseen by the IT department, owners of services and supervisors within their job descriptions. Breaches of the rules lead to sanctions according to the Consequences of IT service Abuse.