E-Mail Rules

University of Tampere
University services / IT Administration

Rector's decision 28 August 2014.

Table of contents

1 Scope

The e-mail rules apply to the use of all e-mail services provided by the university. In these rules, staff refers to the entire university personnel and persons in corresponding positions (such as grant researchers and emeritus and emerita professors), and to the university's schools and other units.

2 E-mail addresses

E-mail addresses can be either organisation addresses, personal addresses or mailing list addresses. Personal addresses can be either work addresses or student addresses.

- **Work addresses** are used for e-mails related to the holder's own work.
- **Organisation addresses** are used for services and communication where the role of the organisation is prominent. Each organisation address must have an owner. Customers are always advised to use the appropriate organisation address for contacting the university. Organisation addresses may not be used for personal communications.
- **Student addresses** are used for communication between the university and students. Students working at the university must use their work address or organisation address for work-related e-mails.
- **Mailing lists** are used for group communications. Each mailing list must have an administrator who is responsible for the moderation (if applicable), regular maintenance and eventual removal of unnecessary lists.

Only personal addresses may be used for personal communications.

Students may forward their mail from the student address to the e-mail address of their choice.

The university determines e-mail addresses and their format. Descriptions of the e-mail addresses can be found on the e-mail service specification.

The university may publish e-mail addresses outside the university.

- Students can forbid the publication of their e-mail address outside their own university.
- Staff members can request their work e-mail address not to be published outside their own university only for compelling reasons.

3 Privacy of correspondence applies to e-mail

The university treats incoming and outgoing messages sent through personal addresses as private, respecting the privacy of correspondence. The privacy of incoming and outgoing messages sent through work addresses can be deviated from, as specified in Section 5.10.

If an e-mail user receives a message intended for another recipient, she/he is bound by an obligation of secrecy and a prohibition of utilisation, concerning both the contents and the existence of the message.

- The rules for handling work e-mails sent to the wrong address can be found in Section 5.4.
- All other received messages intended for another user must be returned to the sender and deleted from inbox.

The forwarding and returning obligations do not apply to malware or spam e-mails.

4 Using e-mail

4.1 Information security obligation

E-mail users must think carefully about what kind of information should be sent via e-mail. From the point of view of security, an e-mail can be compared to a postcard. Users must also consider the nature and amount of data they store in their inboxes.

4.2 Responsibility for adhering to the e-mail quota

E-mail users must adhere to the quota set for their e-mail accounts. Exceeding the quota might prevent the reception of e-mail.

4.3 Responsibility for mail delivery

If the e-mail is crucial, it should be sent well before the deadline and the recipient should be asked to confirm receipt of the message.

4.4 Sending mass e-mails is subject to a permission

Mass e-mails may be sent on topics that are relevant to the university's operations (such as research and the advertising of the university's services), after agreeing on the sending beforehand with the IT Administration.

4.5 Handling of e-mail after the expiry of usage authorisation

The usage authorisation of an e-mail account is fixed-term. A user must save the messages she/he will need later, along with their attachments, before the usage authorisation expires. When the usage authorisation expires, the e-mail address is removed from all mailing lists.

When the usage authorisation expires at the end of employment, the employee must manage her/his e-mail account as specified in Section 5.7.

5 Using work and organisation e-mail accounts

5.1 Mail handling regulations

The handling of work-related e-mails at the university is governed by the laws of Finland, the university's archive filing plan and other data management regulations.

5.2 Prohibition of transfer

It is forbidden to transfer or automatically forward e-mail messages from organisation or work e-mail to outside the university due to information security, privacy protection and information management reasons. In addition to this, it may constitute a breach of the Personal Data Act. Permission to transfer or redirect e-mails to a specific service may be granted for compelling reasons (see Section 7.1).

External e-mail services that have not been approved by the university may not be used for university-related tasks.

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

5.3 Obligation to confirm receipt

If a received e-mail contains a confirmation request, or if the message concerns e-services[1], the message handler must send the confirmation immediately.

5.4 Forwarding obligation under the Administrative Procedure Act

According to Section 21 of the Administrative Procedure Act (434/2003), an e-mail delivered by mistake and dealing with administrative matters beyond the competence of the university or the university employee shall be transferred to the authority or party deemed to be competent, and the sender shall be informed of 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.

5.5 Obligation to use organisation addresses

If an e-mail message received at a work address is an application or if it concerns another public administrative matter, the message and the handling of the matter shall be forwarded to an organisation address.

5.6 E-mail management during absence

Personal e-mail accounts must be managed even during absence, in accordance with separate instructions.

[1]The term 'e-services' refers to the electronic filing, completion and processing (incl. resolution) of matters, and to decisions.

If an automatic reply is used, the sender must primarily be advised to contact the appropriate organisation address.

5.7 E-mail management at the end of employment

Employees must save the personal messages they will need later before the end of their employment and 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 immediate discontinuation of incoming e-mail.

5.8 Management of organisation addresses

The owner of an organisation address must make sure that messages received at the organisation address are properly handled on a regular basis, according to the archive filing plan, even when the owner is absent.

- E-mail messages received at the organisation address belong to the employer.
- All incoming messages must be immediately responded to.
- The response must indicate that it is a reply to a message sent to an organisation address.

5.9 Using work addresses for personal communications

An e-mail address provided by the university may be used for personal purposes, respecting the provisions laid down in the Rules of IT Service Use.

- Employees can protect their privacy by clearly separating their personal e-mails from work-related messages. This applies both to incoming and outgoing messages.
- If the user is both a student and a staff member, communications related to the different roles must take place through the appropriate e-mail address.
- Work-related messages sent by employees must indicate, where relevant, whether the message is a work-related comment or an expression of the sender's personal opinion.

5.10 The university's right to search and open messages sent to and from work addresses

The university may search and open an employee's e-mails, as specified in separate instructions.

5.11 Encryption

All applications used for encrypting organisation- and work-related e-mail messages must be approved and implemented by the university.

Encrypted e-mail messages must be decrypted and saved in a secure place, or encrypted again so that all handlers can access them.

When sending encrypted attachments, the passwords or keys needed for accessing them must be delivered to the recipient by other means, for example, as a text message to a verified phone number.

Confidential information should not be sent via e-mail. If this is unavoidable, the information must be sent encrypted. More information on the classification and handling of information is available in separate instructions.

6 Service provision and administration

6.1 System administration can intervene in e-mail traffic

The purpose of such interventions is to secure the service level or safety of the e-mail system. Interventions, e-mail usage monitoring and log-keeping are governed by separate instructions.

6.2 Messages received within the university's e-mail service are filtered

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

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

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

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

External e-mail service providers used by the university have their own filtering procedures to secure e-mail communications.

6.3 When usage authorisation expires, e-mails will no longer be received

The university will not receive messages sent to a user whose e-mail account is no longer valid. Instead, an automatic message is sent to inform the sender about the expiry of the address. When an e-mail account expires, all its redirection arrangements also become invalid.

7 Other provisions

7.1 Exceptions to the e-mail rules

Permission for exceptions to the e-mail rules can be granted for compelling reasons upon written application. Exceptional permits are granted by the Chief Information Officer. The permit may include additional terms and conditions, restrictions and responsibilities.

7.2 Monitoring

Compliance with the e-mail rules is overseen by the IT Administration and by supervisors, as set out in their job descriptions. Breaches of the rules will lead to procedures regulated in the Rules of IT Service Use.

7.3 Validity

These e-mail rules become effective on 1 September 2014 and replace the earlier version of the corresponding rules.