Email policy - summary

Each email user can have one or several roles

– For example, some of the rules are different for staff members and students.

All rules must be complied with

– You must not use the same password at the university as you use for other services.
– Use your university email address for private purposes within reason (see the terms of use of IT services).
– If you accidentally receive an email message intended for another person, forward it to the right recipient and notify the sender.
– Remember that the privacy of correspondence also applies to email.
– Ensure your mailbox doesn't get too full.
– Do not use your account to send spam.
– Do not leave any personal messages on your university email account after your authorisation to the account expires.

Staff members (and comparable external members)

– The university's email addresses must be used for all work-related correspondence.
– Send acknowledgment for e-Service communications without delay.
– Do not redirect messages from your university work email address to external email addresses.
– Keep private and work-related email messages separate, including ones sent by you.
– If using an 'out of office' reply, advise the recipient to contact another person if necessary.
– Only use email encryption methods approved by the university.
– Before your user licence expires, forward any work-related email messages needed by the organisation to the appropriate personnel.

Students (or alumni)

– Use the university email address issued to you in correspondence related to your studies.
– You can request that the university not publish your email address.
– Messages you send and receive as a student are private.
– If you have an employment contract with the university, the staff rules also apply to you. You must also keep work-related and study-related messages clearly separate.

Mailing list coordinators

– Each mailing list must have a designated coordinator.
– Manage your list (correct and up-to-date email addresses, timely moderation).
– Request deletion of your mailing list when it is no longer required.

Coordinators of the organisation's email addresses

– Determine how messages are processed; follow up on messages and the notification of other users.

– Change the password of protected email addresses regularly and immediately when a user is no longer part of the group handling the account's messages.

Email policy

The email policy applies to all users of the university's email systems. Sections indicated as rules concerning staff apply to the university's units, all staff members and individuals comparable to staff members (e.g. researchers receiving grants, and emeritus/emerita professors) who use the university's email service. The rules also apply to all operators responsible for the operation of the email systems.

The email policy complies with current legislation.

The receipt of email messages is the sender's responsibility. Important messages should be sent well in advance of any deadlines and the email message should include a request for the recipient to confirm receipt.

Privacy of correspondence also applies to email

If a person receives an email message intended for another person, he or she is bound by confidentiality and prohibited from using the content or existence of the message to his or her advantage.

– In accordance with section 21 of the Administrative Procedure Act (434/2003), if an email message is delivered by mistake to the university or its employee for consideration of a matter beyond its competence, the university or employee shall without delay resend the message to the authority it deems competent, and the sender of the message shall be informed of the fact that the message has been resent. If the message cannot be resent, it must be returned to the sender and removed from the university's email system.
– All other messages received by mistake must be returned to the sender.

These obligations do not apply to messages containing viruses or spam.

E-mail addresses

Organisational addresses are official email addresses

Organisational addresses are used for handling official matters and offering services.

Organisational email addresses must be in a specific format as instructed, for example:

– university-level: *records@uniarts.fi*
– unit/department-level *unit@uniarts.fi*
– role-specific *rector@uniarts.fi*

Work email addresses are personal email addresses issued for the performance of work duties

Example: *vili.virta@uniarts.fi*

Work email messages are related to the email address in question and to the employee's work duties.

Email messages sent to work email addresses are usually considered private.

Email messages must be sent from organisational email addresses or work email addresses with the user's name in the address.

Student email addresses are personal email addresses issued to students by the university

Example: *vili.virta@uniarts.fi*

Student email addresses are primarily intended for study-related correspondence.

The university treats students' email messages as private.

Students can prohibit the university from publishing his or her email address to third parties.

Each email service user is personally responsible for ensuring that his or her inbox has enough free space and for deleting messages which are no longer needed.

Email addresses and their formats are decided by the university

Email addresses usually contain the user's name in the following format: *firstname.lastname@uniarts.fi*. There are also role-specific email addresses, e.g. *rector@uniarts.fi*

Use of email accounts and addresses

- Personal email addresses must be in a format that includes the user's name.
- Organisational addresses or work email addresses must be used for work-related correspondence.

The processing and archiving of organisational and work email messages is governed by the Act on the Openness of Government Activities.

- The resending or automatic redirection of messages received to organisational or work email addresses is prohibited in order to ensure data security, privacy and proper management of information, and it could violate laws such as the Personal Data Act.

Organisational email addresses have a designated coordinator

The coordinator must ensure that messages received to the organisational email address are processed frequently in his or her absence.

- Email messages received to organisational email addresses are the property of the employer.
- The coordinator must reply to messages without delay.
- The reply must indicate that it is a response to a message sent to the organisational email address.
- Organisation email addresses must not be used for private correspondence.

Messages received to or sent from personal work email addresses are treated as private messages

- The university can retrieve and open employees' email in circumstances and by methods provided by Finnish law.
- If necessary, work email messages sent by employees must clearly indicate whether the message is submitted in relation to a job duty or as a personal matter of the sender.

Work email addresses issued by the university can be used for private correspondence, provided that the restrictions specified in the IT service terms of use are observed.

- Incoming and outgoing private messages must be clearly separate from work-related messages.
- If the user is both a student and a member of staff, email messages related to these two roles must be accordingly separated and categorised.

External email addresses must not be used for work duties at the university

The use of external email services in the university's network can be restricted by technical measures, if it presents an unacceptable data security risk to the university.

Personal automatic replies should be used with discretion

If an automatic reply is necessary (despite the risk of increased spam), the message should advise the recipient to contact an organisational email address as appropriate.

Email addresses must be attended to during absence

or the account in question should be closed (for example, during long periods of leave). The best option is to advise customers in advance to contact the university through the appropriate organisational email address.

Authorisation for the use of an email address is not indefinite

Private messages must be removed from the inbox when the authorisation to use the university's email address expires.

Employees must contact their supervisor to arrange for the resending of work-related messages to the university. If an employee stops working before the end of the contract, the supervisor may request that the email address be blocked from receiving messages immediately.

Email messages can be encrypted

With regard to organisational and personal work email messages, encryption software must be approved and deployed by the university.

Each mailing list has a coordinator

The coordinator manages the mailing list, frequently checks to ensure that the list is up to date, and removes addresses that are no longer needed.

- The list's owner is responsible for managing and deleting joint mailing lists.
- Personal mailing lists are managed by individual users.
- If the list is moderated, the list administrator is responsible for moderation.

Mailing lists are personal registers and as such the information could be confidential and subject to provisions on distribution. In this case, email messages should be sent as blind carbon copies (bcc) to prevent recipients from seeing other recipients' email addresses.

Mass mailings and the sending and forwarding of chain letter emails are prohibited

Exceptions can be made by separate decision.

Service production and administration

The administrator can take measures with regard to email traffic

in order to ensure the service level or security of the email system. Interference, monitoring and the collection and storing of log data are subject to separate guidelines.

Email messages are verified and filtered

All email traffic can be verified using automatic content analysis and

- messages and attachments containing viruses or other harmful components can be removed automatically.
- the sending of harmful, very large or multiple attachments may be restricted.

In addition, the university may filter and destroy without notification messages which

- arrive from servers known to disseminate spam.
- are classified as junk mail based on automatic content analysis.

The email account is closed

when the user's authorisation to the account expires. The university does not receive messages sent to old users. The sender receives an automatic notification that the account is closed. Any redirections will also stop working at the same time.

Miscellaneous

Validity

This email policy is effective from 1 January 2014 and supersedes previous policies.

Change management

This email policy can be revised as necessary to meet the requirements of current services and legislation. The need for changes is determined by the director of data administration.

Changes will be published through regular communication channels, not individually to each person.

Exceptions to the email policy

Exceptions to this email policy may be granted by written application and on specific grounds only. Exceptions can be granted by the director of data administration. Special permissions can be subject to conditions, restrictions or additional liabilities.

Monitoring and control

Compliance with this email policy is monitored by the data administration department and individual supervisors as part of their managerial duties. Violations will be handled in accordance with the disciplinary procedure for IT violations.

Further information

Rules and guidelines related to IT services are available on the university's Intranet. The relevant guidelines related to or referred to in this policy are:

- Terms of use of IT services
- Disciplinary procedure for IT violations
- Administrative Procedure Act
- Act on the Openness of Government Activities
- Guidelines on the opening of employees' email messages