Email Rules in Brief

Every email user has one or more roles

– the rules are partly different for e.g. the staff and the students

All rules shall be obeyed

– use different passwords at the university of applied sciences (UAS) and in external services
– apply thorough consideration before using the UAS email address for private purposes (see Rules of IT Service Use)
– if you mistakenly receive an email intended for someone else, forward the message to the correct recipient and inform the sender about the mistake
– remember that the privacy of correspondence also applies to emails
– make sure you have enough free space in in your mailbox
– do not distribute spam
– do not leave any private messages in your UAS email account after your user rights expire

Staff members

– always use the UAS email address for work-related correspondence
– send a confirmation of receipt of the received emails without delay
– do not reroute work-related emails to external email accounts
– keep your private and work-related messages separated, including the ones you have sent
– archive your emails according to the instructions provided
– make sure your email is monitored during your absence
– if you use an automatic out-of-office message, instruct the recipient to use a common UAS address
– use only email encryption methods approved by the UAS
– before the expiration of your UAS user rights, forward all email messages relevant for the organisation to an appropriate employee

Students

– use the UAS email address for study-related purposes
– you have the right to forbid the UAS from publishing your email address
– all messages sent and received in the role of a student are private
– if you are also employed by the UAS, you are bound by the rules for staff members as well. You must keep your work- and study-related emails separated.

Mailing list owner

– keep the list up-to-date, i.e. correct, valid addresses and active moderation
– request your list to be deleted when it is no longer needed

Supervisor

– make sure all relevant organisation addresses are available
– make sure the employees use organisation addresses in their work-related communication
– appoint users (with deputies) responsible for monitoring organisation addresses.

Organisation address owner

– provide a procedure for handling the messages, email back-ups and informing other handlers

– change the password for the organisation email account regularly and always after an email handler who knows the password leaves the organisation

Further specifications to these rules are provided below:

Email rules

These email rules apply to all users of UAS email systems. The parts aimed at the staff of the UAS concern all UAS units, their employees and other users in corresponding positions using email services (e.g. trainees). These rule also apply to all users responsible for email systems.

These email rules comply with the valid legislation.

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

Privacy of correspondence applies to emails

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

– as stated by the Administrative Procedure Act (434/2003), § 21, an email message delivered by mistake dealing with administrative matters beyond the recipient's competence shall be transferred to the authority deemed to be competent and the sender of the message 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 UAS email system
– all other email messages intended for another user shall be returned to the sender

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

Email addresses

Organisation address is an official email address

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

The organisation address is formed according to a certain formula, such as:

– UAS-level info@karelia.fi
– unit-level *yksikko@karelia.fi*
– role-level *rehtori@karelia.fi*

Staff email is a personal email account provided for work-related purposes

Example: *vili.virta@karelia.fi*

Staff email messages are related both to the staff email account and the employee's duties.

The UAS normally considers email messages received by the staff email account as private messages.

In outgoing email messages, the organisation address or the staff email address formed from the user's name must be given as the sender's address.

Student email is a personal email account for students provided by the UAS for study-related purposes

Example: *vili.virta@edu.karelia.fi*

The student email is primarily intended for study-related purposes.

The UAS considers email messages received by the student email account as private messages.

The sender's address in outgoing email messages is the student email address formed from the student's name.

The student has the right to forbid the UAS from publishing his/her email address outside the UAS.

All email users are personally responsible for organising and emptying their mailboxes and making sure the reserved space for the account does not run out.

UAS determines email addresses and the format of email addresses

The following domains may be used for different roles:

- organisation addresses take the format *palvelu@karelia.fi*
- staff member addresses take the form *vili.virta@karelia.fi*
- student addresses take the form *brian.kottarainen@edu.karelia.fi*
- projects may take different types of forms, e.g. proj@proj.fi

Staff and student email addresses are formed from the user's name

If another user with an exact same name enters the UAS, the original user's email address may change. The parties concerned will be informed about the possible change.

Use of email and email addresses

- the address consisting of a user's name shall be used as one's personal email address
- the organisation addresses shall be used in UAS communications
- the organisation address or staff email address shall be used for work-related purposes

The handling and archiving of email messages received by the organisation or staff email account are governed by the Act on the Openness of Government Activities and by instruction on archiving procedures provided by the UAS.

- It is forbidden to transfer or automatically route email messages from the organisation or staff email account to an external service. This is to ensure information security, data protection and information management and it may also constitute a breach of the personal Data Act.

- If a received message contains a confirmation request or is a 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 needs to make sure that messages received by the organisation address are handled regularly and archived according to instructions, even during the owner's absence.

- email messages received by the organisation address 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 addressees are not to be used for private communication

Messages related to staff email accounts are treated as private messages

- the UAS has the right to retrieve and open en employee's email message in certain cases and in certain ways, as defined by separate instructions (Retrieving and Opening an Employee's Email)
- work-related email messages sent by an employee must, when applicable, clearly indicate whether they are official statements related to work or the employee's personal opinions
- when responding to applications or other matters related to public administration, the reply address of the response message must be an organisation address
    + instead of changing the reply address, the sender can be advised to use the organisation address in the future
    + the original message and the response are transferred to the organisation address for archiving

The email account provided by the UAS can be used for private purposes within the limitations set by the UAS Rules of IT-services.

- employees must clearly separate their personal and work-related email messages, including both received and sent messages
- if a user is both a student and a staff member, the email messages related to each role must be clearly separated from each other

External email account must not be used for work-related duties

Access to external email services from the UAS network can be technically restricted, if such services are deemed to create a major data security risk.

Use personal auto replies with caution

Auto replies entail a risk of spam flow, but if one is nevertheless deemed necessary, it should advise the recipient to contact an appropriate organisation address.

Emails must be monitored during absences

or the mailbox must be closed (e.g. longer leaves of absences). The recommended procedure is to instruct clients beforehand to use the respective organisation address for all contacts.

---

[1] E-service means electronic means of initiation, completion and handling of administrative matters (including the decision) as well as electronic notification of the decision or sending of trial documents to the court or to a person addressed by the court.

The right to use email the account is fixed-term

Private messages should not be left in the UAS email mailbox when the right to use expires.

Employees must agree with their supervisor on the transfer of work-related messages to the organisation. If an employee resigns form his/her duties before the expiry of the employment, the employee or his/her supervisor can request a discontinuation of incoming email immediately.

Email messages can be encrypted

All applications used for encrypting organisation- or work-related email messages must be approved and introduced by the UAS.

– If an incoming organisation- or work-related email message is encrypted so that only the recipient can decrypt it, the message must be decrypted immediately after the receipt. This rule does not apply to messages containing malware or spam.
– after decrypting, the message can be encrypted again so that all handlers are able to open it

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

Mailing lists have owners

The owner of a mailing list must keep the list moderated and up-to-date and remove any redundant addressees regularly.

– 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 it may thus be subject to confidentiality obligations and separate limitations of disclosure. If such rules apply, use the blind carbon copy (bcc) function to hide the addresses of list members from the recipients.

Mass mailing and sending/forwarding of chain letters is forbidden

Exceptions to this rule can be made upon separate decisions.

Service production and administration

System administration can intervene in email traffic

in order to secure the level of services or safety of the email system. Such an intervention as well as the monitoring of email usage and log-keeping are governed by separate instructions.

Email is checked and filtered

All email traffic goes through an automatic content analysis, based on which

– messages and attachments containing malware are automatically removed
– 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 recognised spam servers
– classified as spam based on the automatic content analysis.

Email address is no longer valid

The email address no longer works when the usage authorisation has expired. Messages sent to a user whose email account is no longer valid will not be delivered. Instead, an automatic message will

be sent to inform the sender about the expiry of the address. When an email account expires, all its re-routing arrangements also become invalid.

Other regulations

Validity
These email rules become effective as of 1 January 2014 and replace earlier corresponding rules.

Change management
These email rules will be reviewed when needed to ensure that they comply with all valid services and laws. Any significant staff-related changes are addressed according to the co-operation procedure. The Head of IT-Services makes decisions on any needs for change.

Information about changes is distributed using regular communication channels, never personally.

Deviations from email rules
Permission for exceptions from the email rules can be granted for compelling reasons upon a written application. Exceptional permits are granted by the Head of IT-Services and they may include additional terms and conditions, restrictions and responsibilities.

Monitoring
Compliance with the email rules is overseen by IT administration, email system administrators and owners as well as supervisors within their job descriptions. Breaches of these rules lead to sanctions according to the consequences of IT service abuse.

Further information
The instructions referred to or related to by these instructions are:

- IT Service User Rules
- Email Rules (this document)
- Retrieving and Opening an Employee's Email
- Consequences of IT Service Abuse
- Tables of Penalties of IT Service Abuse
- Administrative Rules for Information Systems