# Regulations for Handling Email - 21.11.2022

## 1 General

In handling electronic documents, the University shall apply the principles of privacy of correspondence, protection of privacy and good administrative procedures. The rights of communicating parties shall be protected. The bounds of secrecy and prohibition against exploitation that concern the users are described later in the Act Information Society Code (7.11.2014/917) and in the Act on the Protection of Privacy in Working Life (13.8.2004/759). The rules concerning the bounds of secrecy and prohibition against exploitation are described later in this document and in the General Policy on the Use of Information Systems and the Policy of Information Systems Maintenance (the document is only in finnish).

It is the responsibility of the sender of an email message to make sure that it has been delivered. In electronic service, the sender can be assured of delivery of the message by an acknowledgement of receipt sent by the receiving authority. Electronic service refers to the electronic initiating or completing of administrative matters, handling (including decision making) and serving of a notice of a decision or sending a trial document as an electronic message to a court of general jurisdiction or to a person ordered by the court to receive such documents.

The University shall have the right to determine for what purpose the email and the network are to be used, and user rights can be restricted.

The email system is not meant for mass distribution of files or for transmitting large files.

## 2 Definition and Handling of Email Messages and Addresses

### 2.1 Definitions and Scopes of Use

In these regulations, email messages have been divided into four different categories based on the type of address they are connected to. In the regulations, both sent and received messages are defined as follows:

- Organizational email is an email connected to an organizational address of the University or a university unit (e.g. kirjaamo@metropolia.fi, valinta@ metropolia.fi).
- Official email is connected both to the personal official email address issued to an employee by the University for working purposes (e.g. vili.virta@ metropolia.fi) and to the work duties of the said employee. If a student sends email in an active role in e.g. University executive bodies or research teams, the said email shall be considered to be an official email.
- Personal email is a personal message connected to an email address issued by the University (usually the same address as the official email address or a student's email address).
- Other email is a message connected to the user's email address outside of the University e.g. vili.virta@personal-use.fi or vili.virta@other-organization.fi.

Official and personal email addresses are composed of the user's name or the user's user ID.

The person's e-mail address is classified as personal information https://tietosuoja.fi/en/what-is-personal-data and the processing of personal data complies with the Data Protection Act (5.12.2018/1050). Personal data are registered in the personal data files of the University, of which

file descriptions have been drawn up and handled in the University in a way and for the purposes defined in the descriptions.

The University and its units shall have organizational email addresses for running official business and offering services (e.g. kirjaamo@ metropolia.fi or helpdesk@ metropolia.fi). The services of the University shall be approached primarily using the organizational email addresses instead of the official addresses of individual employees.

### 2.2 Publishing of Email Addresses

Publishing means revealing an email address in such places as the University phone book or other publication, the public web pages of the University, calling cards and index services.

The University publishes the organizational email addresses and the official email addresses of its employees, as necessary for the use of services and attending duties. As a general rule, publishing a student's email address requires the student's consent. The University does not publish email addresses that are not issued by the University.

Email addresses should always be in the form based on the user's name, both in the settings of the email client and otherwise published.

### 2.3 Handling of Organizational Email Messages

Each organizational email address shall have at least one responsible person appointed to it. The organization shall take care of handling of the received messages regularly.

In order to maintain privacy protection and information management, it is forbidden to forward or automatically redirect organizational email to an email address outside of the University.

When an employee replies on the behalf of the University, the reply must clearly state that it is in response to a message sent to an organizational email address. The reply must emphasize, or the return address must be set in such a manner that future contacts will also be directed to the organizational address.

When necessary, an email message can have an appendix referring to the confidentiality of the message.

Organizational email messages shall be handled in a manner required by the Act on the Openness of Government Activities (621/1999). The Act defines among other things what an official document is, which information in an official document is confidential, and when access to a document can be granted.

### 2.4 Handling of Official Email Messages

In order to maintain privacy protection and information management, it is forbidden to forward or automatically redirect official email to an email address outside of the University.

As a general rule the University treats messages sent to the official email address as personal messages, since the receivers cannot prevent personal messages from arriving.

There are more precise regulations in chapter 6 considering the employer's rights to retrieve or open email messages sent to or by an employee (Act on the Protection of Privacy in Working Life, 759/2004).

An official email sent by an employee shall clearly state that the sender is an authority, not a single employee. This can be accomplished e.g. by adding to the signature the employee's position and the name of the university unit. If the email message in question is an application or something that requires official authority measures, the reply address shall be set to an organizational email address, or the client shall be reminded to address further contacts to the appropriate organizational email address.

When necessary, an email message can have an appendix referring to the confidentiality of the message.

Official email messages shall be handled in a manner required by the Act on the Openness of Government Activities (621/1999). The Act defines among other things what an official document is, which information in an official document is confidential, and when access to a document can be granted.

### 2.5 Handling of Personal Email Messages

Personal email messages of an employee shall be separated clearly from messages belonging to the University. An employee shall immediately move any personal messages having arrived to the official email address to separate folders, the names of which clearly state the privacy of the messages (e.g. private, personal). This applies both to received and sent messages.

It is permitted to use the University email address to an employee's or a student's personal matters on a small scale as long as it does not impede the functions of the University. However, use for commercial purposes, such as private entrepreneurship is absolutely forbidden.

It is not allowed to use University mail servers to send chain letters or mass email. The necessity of the University to communicate on a large scale to members of the University community is considered case by case.

### 2.6 Handling of Other Email Messages

An external email address (i.e. address other than @metropolia.fi) is a personal matter, and these regulations do not consider that more closely. An employee or student is not allowed to use an external address for tasks connected to University. Tasks included emails between teacher and student.

An external email address should not be used for a student's studies and other activities as part of the University community. The University can require that an email address issued by the University is used using services by email.

When using user accounts connected to email accounts outside of the University, use of the same passwords as for University-issued user accounts is not allowed.

## 3 Messages Requiring Special Measures

### 3.1 Restricting Email Messages and Their Attachments

The University has the right to use automated checking on email messages and their attachments for possible viruses and other malware, and to restrict the sending and receiving of possibly harmful or too large/numerous attachments.

The University has also the right to delete messages and attachments containing viruses and other malware. The University is not required to inform the sender of the filtering or deletion of a single message. The filtering is performed automatically in the email system. The users will be informed of these restrictions in the document Instructions for Filtering Email.

### 3.2 Handling of Spam

The University protects its email services and diminishes the problem with spam by filtering messages arriving from servers known to relay spam or messages that are classified as spam on the grounds of the content of their subject line or automated content analysis. The restrictions are implemented in the email service by technical means. The University may also delete the filtered messages on behalf of the user.

The University is not required to inform the communicating parties of the deletion of a single spam message, or to return the deleted message to the sender.

Spam messages are not to be replied to, as this only increases the amount of received spam. Sending a reply proves the email address to be a functioning one, causing it to be added to the spammers' address lists.

Many Metropolian's have received a message in their email asking them to send ransoms as bitcoins to the blackmailer based on false allegations. If the message contains your Metropolia password, change your password at https://salasana.metropolia.fi/. Also change your password for other services where you used that password. Please do not use the same password in Metropolia's services

as you use in any other service. In other respects, there is no need to worry, and ransom should not be paid under any circumstances.

The user can report disturbing spam to maintenance personnel or the IT support (helpdesk@metropolia.fi). In practice, the maintenance can only try to intervene in messages sent from Finland.

### 3.3 Handling of Undeliverable Email

The sender of an email message is responsible for the readability of the message, the message reaching its destination, the possibility of a deadline being missed and other comparable issues, until having received the information that the message has been successfully delivered.

If the address of an arriving message is not known by the email system, an error message is automatically sent to the original sender. A notification is also sent to the original sender, if the recipient's email quota is full. Managing the quota is a user's own responsibility.

The responsibilities for sending and returning do not apply to malware messages or spam.

### 3.4 Handling of Email Arriving at an Incorrect Address

If a user receives an email message intended for another person, the receiver must inform the original sender of the unsuccessful delivery and delete the arrived message. The user has obligation of secrecy and non-exploitation considering both the contents of the message and its existence.

The duties of sending and returning do not apply to malware messages or spam.

## 4 Handling of Email in Special Situations

### 4.1 Automatic Responses to Messages

It is not recommended to use automatic replies. If, however, an automatic reply is deemed necessary (e.g. long vacations of employees, leave of absence or termination of employment), the automated reply shall advise the original sender to contact primarily the appropriate organizational address.

### 4.2 Termination of Employment or Study Right

A person's right to use the University-issued email address is terminated when the employment or study right ends. The validity of the user rights of a person outside of the University community falls under the jurisdiction of the director of the unit having recommended the issuing of the user rights. After the user rights have been terminated, the University does not accept messages sent to the person but informs automatically the sender that the address is no longer valid.

Before the termination of the employment, an employee shall inform his or her communication partners of the upcoming termination of his or her email account and delete personal messages. Other messages remain the property of the University and opening them is governed by the Act on

the Protection of Privacy in Working Life (759/2004). If an employee's ceases his or her duties before the termination of the employment, the receiving of email shall be terminated already at that time.

Before the termination of the user rights, a student is responsible for informing his or her communication partners of the upcoming termination of his or her email account.

### 4.3 Procedural Rules While an Employee is Temporarily Absent

When the absence is known in advance, the employee and his or her superior shall take care of the proper handling of the employee's email. The recommended way is to give the person in charge of the duties during the absence the access to the email by access control lists. (For information on automatic replies, see chapter 4.1.)

Within the scope set by the Act on the Protection of Privacy in Working Life (759/2004, sections 18 through 20), the University has the right to gain access to the email messages that belong to the University and are necessary for the continuation of University functions while an employee is absent. Accessing and opening the messages sent to or from an official email address is primarily based on the consent of the employee and on the possibility to clearly tell apart the confidential private messages belonging to an employee from the messages belonging to the University. (On separating the messages: see chapter 2.5.)

If the employee has not given another person, accepted by the employer, the consent to access and open the messages belonging to the employer while the employee is absent, or the consent cannot be obtained due to a serious illness, the University President may order the employee's superior, with the help of the administrator of the mail server, to access and open the above-defined official email messages, while the employee is absent. The reason for accessing and opening the email, persons taking part in it, the time of the procedure and the person or persons having received information of the opened email message have to be documented, and the employee has to be notified without unnecessary delay.

### 4.4 Messages and Mail Boxes Harming or Endangering the Email System

The right of the maintenance of the email system to intervene in the email traffic to ensure the service or security of the email system is prescribed in more detail in the document Administrative Rules of Information Systems.

## 5 Encryption and Verification of an Email Message

A user has the right to encrypt his or her email messages with Metropolias secure-email function, which is a tool accepted by Metropolia IT-services.

Confidential and sensitive personal data should not be transmitted by e-mail or any other form of data transmission over a network without encryption. Metropolia's internal e-mail traffic (when you send a message from an e-mail address ending in @ metropolia.fi to another e-mail address ending in @ metropolia.fi) is already basically encrypted.

If necessary, the accuracy and authenticity of a document received by e-mail must be verified.

## 6 Monitoring Email Usage and Collecting and Storing Log Information

Instructions on monitoring email usage and collecting and storing log information can be found in the document Administrative Rules of Information Systems.

## 7 Supervision of These Rules

These rules are supervised by the University IT Services, the administrators of the mail servers, and unit directors. Offences against these rules shall be dealt with according to the Policy of consequences for IT Offences. The rules shall be updated when necessary, or when the common recommendations of the Universities are changed. The need for updates shall be monitored by the Chief of Information Officer or a person appointed by him or her.