PROCEDURE

7 June 2021 UFV 2018/1239

Approved by:
University Director

Responsible division:
Legal Affairs Division

Bodies consulted:
Security and Safety Division
University IT Services

First issued: 25 June 2018

Procedures for managing email

Introduction

Uppsala University's *Procedures for managing email* describe how staff and other persons active at the University who have access to the University's email system are to handle their email and the University's email system to make it a secure and time-saving tool that is managed in accordance with the regulations that govern the use of email.

This is achieved by informing staff and avoiding management issues such as overly full inboxes that can lead to stress, extra work when dealing with requests for access to official documents or the disappearance of important email messages.

In addition, all staff must comply with Uppsala University's guidelines on security and all handling of the University's IT resources.

Purpose

The purpose of these *Procedures for managing email* is to provide practical instructions and support to staff on the use of email at the University, to ensure that email meets current legal requirements and is a time-saving tool that all staff know how to use.

General

Everyone at Uppsala University must use the email system and the personal email address (or organisational address) provided by the University when sending business emails. This applies to both internal and external communications.

The automatic forwarding of emails to other email systems is not permitted.

Only limited amounts of email of a private nature may be received in and sent from Uppsala University's email system.

Incoming email must be checked regularly and always dealt with in accordance with current legislation on public access and secrecy, for example, regarding registration.

Further, everyone should bear in mind that email messages are generally official documents that are open to the public and may therefore be disclosed.

To fulfil the requirements of the General Data Protection Regulation and to facilitate management, email is only to be used as a *carrier* of information, not for *storing* or *processing* vital information. To enable email to be an efficient tool, users should take care to limit the quantity of unwanted email and minimise the size of emails, for example, by being restrictive about attachments.

Every user has a responsibility to inform their line manager when they feel they lack knowledge in certain areas of email management. It is the manager's responsibility to inform their staff about the training resources available for learning to manage email efficiently.

Limit the personal data contained in emails

Reduce the spreading of personal data by always considering whether your email needs to include personal data.

Emails that contain sensitive personal data or data that is classified as secret must be encrypted. For further information, see *Procedures for information security: secure information management* (UFV 2018/668) and *Procedures for information security: risk management* (UFV 2018/211).

Sort your email

You should go through email messages that are not registered or kept in order in some other way regularly and clear them out. They must not be left in your inbox. Advertising, spam and other messages that are obviously of little importance can be deleted immediately.

Managing email when away

When you are away for more than one working day, place an automatic message in the auto-reply function and say when you expect to be back so that anyone sending email to you knows that you are not available. Give alternative contact information as well.

Ensure that incoming email is monitored while you are on holiday or otherwise absent for an extended period to ensure that emails that are official documents are dealt with in keeping with the timeframes specified in current legislation. (You will find instructions for sharing your mail box or forwarding email in the Staff Portal → Services and Support → IT and Telephony Services → IT Support → Email.)

The use of organisational addresses is recommended especially for functions that involve the exercise of official authority.

Security

Emails with unknown contents or attached files must be treated with caution.

If possible, avoid opening suspicious communications – the subject line or a preview of the first few lines of the communication can help you decide whether the communication is genuine.

Never reply to advertisements/unsolicited email (spam). A reply is a confirmation to the sender that the address is active.

Do not open attached files if you are uncertain what they may contain.

If an attachment that is opened requests that you activate a macro, refuse to do so. Macros in Word, Excel or Adobe PDF, for example, are common ways for attackers to spread viruses or steal information.

Never disclose passwords or codes to anyone.

Email with suspicious contents may involve phishing, ransomware, economic fraud, viruses, etc. If you suspect attempted phishing, err on the side of caution and send the email as quickly as possible to the Information Security Department at the Security and Safety Division (security@uu.se).

If an email contains threats, save the message and contact the Security and Safety Division (security@uu.se).

Cessation of employment

If your employment at Uppsala University ends (for whatever reason), you are personally responsible for ensuring that all emails that you have received and that should be taken care of, but have not yet been dealt with, are passed on to your line manager.

Uppsala University does not assist in any transfer of selected email messages to external email systems or other exports.

Email messages in mail boxes belonging to accounts that have been inactive for four years are deleted.

See also *Procedures for information security: management of electronically stored information when employment, academic study or official duties at Uppsala University end* (UFV 2012/415).

Logging and checking of email use

All email and computer traffic in the University’s networks is logged. The University has a right, as employer, to go through these logs and to access the contents of email to check compliance with rules laid down in legislation or in the University’s own guidelines and to be able to fulfil the University’s obligations, as well as to identify, manage or prevent threats to information security.

In order as far as possible to respect personal privacy, the University as employer does not regularly check the contents of employees’ computers, email messages or internet traffic. However, the University may check data contained in a computer, email messages and internet traffic if necessary for the following purposes:

- Performance of the University’s obligations as a public authority, such as public access to official documents
- In the event of an information security risk
- On behalf of the police or other law enforcement authorities
- In the event of danger to anyone’s life or health
- For the sake of internal inquiries at the University

Responsibilities

It is the responsibility of managers at the University as a public authority to ensure that all employees are acquainted with the University’s procedures for managing email, but it is the responsibility of each individual to follow these procedures.

Failure to comply with the provisions in effect may lead to measures being taken under labour law or otherwise. If a state employer finds reason to suspect that an employee has committed certain offences that may be subject to penalties other than fines, the employer is required under Section 22 of the Public Employment Act (1994:260) to report the suspected offence for prosecution. Other cases may also be reported to the police for investigation.