Procedures for e-mail management

The attached "Procedures for e-mail management" are hereby approved. The procedures come into effect immediately.

The decision in this case was taken by the undersigned university director based on advice from the University’s chief legal officer Per Abrahamsson.

Katarina Bjelke

Per Abrahamsson
Procedures for e-mail management

Background

Uppsala University’s e-mail management guidelines describe how staff and other parties who have access to the authority’s e-mail system are to manage their e-mail and the University’s e-mail system to ensure it is a secure and time-saving tool that is used in accordance with the regulation on the use of e-mail. This is accomplished by informing the staff and avoiding e-mail management problems, such as overflowing inboxes that can lead to stress or the loss of important e-mail messages.

To meet the requirements of the General Data Protection Regulation and facilitate e-mail management, only use e-mail as a means of sharing information and not for the storage of or processing of crucial information. For e-mail to be an effective tool, the user should make sure to limit the amount of unwanted e-mail and minimise the size of e-mail messages through the restrictive use of attachments and other measures.

Additionally, all staff are to adhere to Uppsala University’s guidelines for security and all use of the University’s IT resources.

Purpose

The purpose of these e-mail management guidelines is to provide concrete recommendations and support to staff for the use of e-mail within the authority. This is because e-mail messages are to adhere to any relevant legal requirements and function as a time-saving tool. All staff are informed in its use.

General information

Everyone within Uppsala University is to use the e-mail system provided by the authority when sending e-mail as part of work, both for internal and external communications. It is the responsibility of each user to speak to any immediate supervisor if the user needs support in certain areas of e-mail management. It is the supervisor’s responsibility to inform subordinates about the available training resources in how to manage e-mail effectively.

E-mail management

- Incoming e-mail messages should be checked regularly and always handled in accordance with current legislation regarding public information and privacy, for example, rules related to registering messages.
- All work-related e-mail correspondence is to be sent through the e-mail system provided by Uppsala University.
- It is not permitted to automatically forward e-mail to other e-mail systems.
- Private e-mail may only be received through and sent from Uppsala University’s e-mail system to a limited extent.
• E-mail containing sensitive personal data or confidential information should be encrypted. See Procedures for Data Security; secure data management, UFV 2018/668.

Limiting personal data in e-mail

• Reduce the disclosure of personal data by always considering whether personal data needs to be included in an e-mail message.

Sort your e-mail

• Archive or delete old e-mail. Do not leave e-mail in your inbox.

Use autoreply

• Activate an autoreply message when you are away for more than one business day and include information about when you expect to return so that individuals contacting you by e-mail will know that you will not answer before that date.

Security

• If possible, avoid opening suspicious messages. The subject line or preview of the first lines of the message can help determine if the message is authentic.
• Never reply to advertisements/unwanted e-mails (spam). A response confirms to the sender that the address is active.
• E-mail with unknown contents or attachments should be treated with caution. Do not open attachments if you are not sure what they contain.
• If you open an attachment that requests activation of a macro, deny this request. Macros in Word, Excel, Adobe PDF files and other programs are common ways for attackers to spread viruses or steal information.
• E-mail with suspicious content may expose you to phishing attempts, ransomware, financial fraud, viruses and so on. Send any e-mail of this type to security@uu.se. Never share passwords or codes with anyone else.
• If e-mail contains threats, save the message and contact security (security@uu.se).

Logging and checking the use of e-mail

All e-mail messages and data traffic in the University’s network are logged. As an employer, the University has the right to review these logs and to examine content in e-mail messages to check if legal regulations or government guidelines are followed and to perform the duties of the University as well as to identify, manage or counteract data security threats. The same applies to files and other materials stored in computers and transmitted through networks.
To respect the privacy of staff, the University as an employer does not regularly check the content of staff computers, e-mails or internet traffic. However, the University may check data contained in a computer, e-mail message and internet traffic if necessary for the following purposes:

- Compliance with the authority's responsibilities, such as public disclosure;
- When data security is threatened;
- On behalf of the police or other law enforcement agency;
- When the life or health of an individual is at stake;
- In connection with internal inquiries at the University.

**Responsibilities**

The authority’s managers are responsible for ensuring that all staff within the University are familiar with the authority’s e-mail management guidelines, but it is also the individual’s responsibility to comply with these guidelines.

Failure to comply with applicable regulations may impact employment or result in other measures. In cases where a government employer finds that an employee is reasonably suspected of crimes that may lead to a penalty other than a fine, the employer is required to report the suspected crime for prosecution pursuant to section 22 of the Public Employment Act (1994:260). Other cases may also be reported to the police for investigation.