# Guidelines on using email

Center for Information Technology, Kansai University

1 Purpose of these guidelines

Email is indispensable for daily learning, educational, and research activities. This is why email should be used in a secure way such that rules and manners are observed. Otherwise, many users could suffer harm. Plus, if email is not used correctly, it could cause the university to halt learning, educational, and research activities or lose the trust of society. The purpose of these guidelines is to reduce such risks, to protect information assets, and to provide instructions on how to use email securely.

2 Intended audience for these guidelines

The intended audience for these guidelines includes all users who use the email system maintained and provided by the Center for Information Technology.

3 Email software settings

(1) Email reception settings

1) It is recommended that users view received email messages in plain text format (including rich text format) and that they avoid using HTML email to the greatest extent possible, to prevent themselves from being directed to fake websites and prevent fraudulent scripts from being executed in advance.

2) It is recommended that users disable the HTML preview feature when using HTML email.

3) Users shall implement antivirus measures for email software, in addition to antivirus software, if it can be set.

(2) Email sending settings

1) As a general rule, it is recommended that users not send email messages in HTML format. If we send an email message in HTML format, it could lower the information security level of the recipient.

4 General precautions about email

(1) Prohibition against use of email for private purposes

1) Users shall use the email system only for purposes of performing learning, educational, and research activities, and not for private purposes.

(2) To automatically forward email messages to an email address other than one supplied by the Center for Information Technology (XXXXXXXX@kansai-u.ac.jp)

1) When automatically forwarding email messages to an email address other than one supplied by the Center for Information Technology, users shall first fully consider whether it is truly necessary. If they decide it is absolutely necessary, they shall make sure the forwarding address is not incorrect and that confidentiality is maintained on the side of the forwarding destination. In particular, when a forwarding address is changed or when it is no longer in use, users shall modify the auto-forwarding settings immediately.

(3) Monitoring email messages

1) To ensure proper use of the email system, its usage logs (e.g., destinations, messages, attachment files) may be obtained, stored, inspected, and analyzed. Users shall understand the purpose of such actions and be aware of the fact that email message content is subject to monitoring and audit.

(4) Managing email ID and email address

1) Users shall not use others' email IDs (IDs to log into the email server; same as below) and email addresses.

2) Users shall not share their email IDs or email addresses with others.

3) Users shall not leave the email IDs assigned to them in a state that allows those who do not need to know them somehow to learn them.

4) If an email address must be shared by multiple interested parties or taken over and used by successive staff members, such as in the case of an email assigned for a specific type of service, job position, or department, users shall consult with the Center for Information Technology regarding permissions and settings.

5 Managing passwords

(1) Managing email passwords

1) Users shall set their own passwords.

2) Users shall observe the Guidelines on Using Passwords to manage their passwords.

3) Users shall not save their passwords in email software permanently. However, if it is overly complicated to enter a password every time an email message arrives, it is permissible to use a mechanism to temporarily save the password in email software and enter it only after launching a mobile information terminal such as a client PC or a smartphone.

4) If users temporarily save passwords in email software, they shall consider mobile information terminals such as client PCs and smartphones as "subject authentication information storage devices" on which such passwords are temporarily saved and take into account the following points for safe and secure handling of such terminals.

i) Take safety measures to prevent mobile information terminals such as client PCs and smartphones on which passwords are saved from being used against their will.

ii) Do not provide or lend to others mobile information terminals such as client PCs and smartphones on which passwords are saved.

iii) Manage not to lose mobile information terminals such as client PCs and smartphones on which passwords are saved. If they are lost, report the matter to the Center for Information Technology immediately.

## 6 Receiving email messages

### (1) Checking incoming email messages

1) Users shall check incoming email messages on a regular basis.

### (2) Scanning a file attached to an email for a virus

1) Users shall perform automatic virus scans using antivirus software.

2) If users configure settings so that virus scans are automatically performed, or so that the latest data for virus scans are automatically updated, they shall not change such settings.

3) Users shall perform virus scans targeting files attached to emails in received email messages at all times. This is a measure to check file attachments in email messages received in the past for viruses using the latest virus pattern file. In case that the virus pattern file cannot be provided in a timely manner, it is important to keep current with new viruses and to be sure that no viruses are found when virus scans are performed upon the arrival of email messages that include files.

4) Users shall follow the instructions given by the Center for Information Technology in case that emergency measures should be taken.

### (3) Measures to be taken when receiving an email message sent to an unintended address

1) If users receive an email message sent to an unintended address and the sender needs to send it to the correct recipient again, they shall inform the sender to the extent practicable that the sender has sent the message to the wrong address.

2) When users receive an email message sent to an unintended address, they shall delete it.

### (4) Measures when a suspicious email message arrives

1) When users receive a suspicious email message, they shall not open the message, and they shall contact the Center for Information Technology for instructions.

2) When an email message includes a file, they shall not open the message, and they shall contact the Center for Information Technology for instructions.

### (5) Measures when the mobile terminal are infected with viruses

1) If a mobile information terminal such as a client PC or a smartphone is infected with a virus or is suspected of being so infected, users shall immediately isolate the mobile information terminal from the network and contact the Center for Information Technology for instructions, to prevent further infections in advance. More specifically, in the case of a PC, isolating it from the network means removing network cables, a wireless USB LAN adapter, and so on from it. If a wireless LAN adapter is built in, users shall stop the wireless LAN function. In the case of a mobile information terminal, users shall turn on its airplane mode or turn off wireless communications such as Wi-Fi and 4G.

### (6) Measures against spam emails

1) Users shall not disclose or inform others regarding email addresses to a greater extent than is necessary.

2) If users disclose or inform others regarding their email addresses over a network such as via a website, it is desirable to determine measures to prevent their email addresses from being automatically collected.

i) Attach the address as image information, display the address intentionally using full-byte characters, append meaningless strings to the front and end of the password, and so on.

3) Users shall ignore spam emails sent to them. If you send a stop request to the sender, this ends up letting the sender know that you are actually using your email address. This could have the

undesirable consequence of actually increasing spam emails.

7 Creating email messages

(1) Restrictions on To, CC, and BCC

1) Users shall limit the number of email destinations, including To (destination), Carbon Copy (CC), and Blind Carbon Copy (BCC), to keep them at the minimum level.

i) Network resources used are resources used for one email message x all destinations.

2) If users send an email message to a large number of people simultaneously, they shall consider measures such as using BCC or sending it to recipients separately. If TO or CC is used instead, others' email addresses would be exposed to those who receive this message.

(2) File size limit per email message

1) Users shall make sure that the total file size, with the email body and attachment file combined, does not exceed 25 MB.

i) The email system provided by the Center for Information Technology sets the maximum file size limit for sending at 25 MB.

2) If the total file size with the email body and attachment file combined exceeds 25 MB, users shall consider other options such as Kansai University File Transfer (the maximum file size limit is 1 GB) to provide information or conduct batch sending.

(3) Restrictions on email message formats

1) Users shall not send email messages in HTML format whenever possible. If we send an email message in HTML format, it could lower the information security level on the part of the recipient.

(4) Content of an email message

1) When sending information by email that should be treated as confidential, users shall take separately specified security measures.

i) When sending information by email that should be treated as confidential, users shall report it to their superiors and ask for permission.

ii) When sending information by email that should be treated as confidential, users shall ensure security and determine how it should be sent. Here are some examples:

a Kansai University File Transfer

b Information System's personal message service

c Encrypted communication channel (such as VPN)

d Network that does not pass through an external channel (e.g., a dedicated channel)

iii) When sending an attachment file that includes information that should be treated as confidential by email, users shall consider whether the following protection measures are necessary. If they decide these measures are necessary, they shall take such measures.

a Password protection for attachment files

b Encryption of attachment files (such as through use of encryption software)

2) When sending an attachment file that includes information that should be preserved by email, users shall consider whether adding an electronic signature is necessary. If they decide it is necessary, they shall add an electronic signature.

3) Users shall properly manage the key used to add an electronic signature.

4) Users shall not impersonate anyone else to create an email message.

5) When transferring an email message, users shall not change its content without permission from the author.

6) Users shall consider the protection of personal information and privacy.

7) Users shall not send an email message that falls under any of the following categories:

i) Breach of security (Observe the Kansai University Regulations of Document Handling and the Kansai University Regulations of Information System Usage)

ii) Violation of rights (e.g., intellectual property rights, copyrights, trademark rights, portrait rights, license rights)

iii) Content that concerns sexual harassment or racial issues

iv) Disrespectful attitudes or defamatory statements

v) Content that can be considered to constitute a pyramid scheme

vi) Content that can be considered to constitute a threat or pursuit of personal gain or solicitation

(5) Netiquette

1) Users shall not send or transfer chain emails (involving a request to forward the same email message to others).

2) Users shall not send spam emails (email messages such as direct emails sent randomly for commercial purposes) or junk email (email containing useless information).

3) Users shall add subjects to their email messages. They shall also specifically and briefly explain the subjects so the message can be easily understood.
4) Users shall not use slang expressions or non-predefined abbreviations.
5) Users shall not use environment-dependent character codes.
   i) When users are not sure about any of the above, they shall contact the Center for Information Technology for instructions.
6) Users shall enter line breaks wherever appropriate, roughly every 30-35 double-byte characters, when creating an email message.
7) Users shall be aware of how they should use TO and CC, and they shall use TO for requesting replies to messages that they are sending.

## 8 Sending email messages

(1) Precautions when sending an email message

1) Users shall make sure that the email destination address in the TO line is correct before sending a message.
2) When sending an email message with a file attachment, users shall perform virus scans targeting the file.

(2) Encrypting email messages

1) When sending an attachment file that includes information that should be treated as confidential by email, users shall consider whether encrypting the message is necessary. If they decide it is necessary, they shall encrypt the message.
   i) Encryption of communication channels (Kansai University File Transfer, Information System’s personal message service, and the like)
   ii) Encryption of attachment files (such as through the use of encryption software)
2) Users shall properly manage the key used to decrypt encrypted information.
3) Users shall obtain a backup of the key used to decrypt encrypted information.

(3) Password protection for attachment files

1) When sending an attachment file that includes information that should be treated as confidential by email, users shall consider whether the file should be password-protected. If they decide it should be password-protected, they shall set a password for the file.

[Procedures] How to set a password for a document file (Microsoft Word)
Choose [Save As] from the [File] menu, and then choose [General Options] from the [Tools] menu and set [Read-only Password].

2) Users shall use strings agreed upon with the recipients in advance for passwords or inform the recipients of passwords by other means such as telephone, instead of sending them by email.

(4) Things to confirm to prevent information disclosure when sending email messages

1) When sending an attachment file by email, users shall make sure that the information therein will not be inadvertently disclosed as additional electronic file information by checking the following:
   i) Whether information such as the names of the author and editor still remains on the [Properties] page
   ii) Whether information that should be treated as confidential is included in seemingly hidden parts (“hidden” settings, hidden comments, or sheets)
   iii) Whether track changes are saved to a greater extent than is necessary

(5) Adding signatures to email messages

1) When sending an attachment file that includes information that should be preserved by email, users shall consider whether adding an electronic signature is necessary. If they decide it is necessary, they shall add an electronic signature.
2) Users shall properly manage the key used to add an electronic signature.

(6) Restricted use of the feature to request delivery and read receipts when sending email messages

1) When sending email messages, users shall not use the feature to request delivery and read receipts unless otherwise absolutely necessary, in order to prevent traffic spikes.

(7) Measures when sending email messages by mistake

1) When sending email messages by mistake, users shall follow up with the receiving end (recipients) at their discretion as the senders.

(8) Measures when sending viruses

1) When users find that they have inadvertently sent viruses, they shall immediately contact and consult with the Center for Information Technology for instructions.

9 Saving or deleting email messages

(1) Saving or deleting email messages in the mailbox (on the server)

1) Users shall be aware of the maximum email size limit for email messages stored in individual mailboxes on the server and delete unneeded email messages as appropriate.

(2) Saving or deleting email messages in the mailbox (on mobile information terminals such as client PCs and smartphones)

1) When saving email messages that include information that should be treated as confidential in the body or attachment files, it is desirable that users take measures such as encryption before saving them.

2) Users shall back up email messages as appropriate if such messages include information that should be preserved in the body or attachment files.

3) Users shall quickly delete unneeded messages from mobile information terminals such as client PCs and smartphones.

4) When deleting email messages that include information that should be treated as confidential in the body or attachment files, users shall respect the confidential nature thereof and make it difficult to recover such messages.

10 Contact for these procedures

(1) Saving or deleting email messages in the mailbox (on the server)

1) If users need to cope with emergencies or take measures beyond the scope of these guidelines, they shall contact the Center for Information Technology for instructions.

2) If users have any questions about the content of these guidelines, they shall contact the Center for Information Technology for answers.

Supplementary provisions

1. These guidelines become effective on November 6, 2019.