ACCEPTABLE USE POLICY - EMAIL SERVICE

Applies to:
Faculty, staff members, students, and users of the University of Burgundy's information system
Hereafter "User/s"

By:
The University of Burgundy
Hereafter "the University"

Adopted by the Board of the University of Burgundy on December 16, 2015.
This Policy sets out the rules and regulations of the University with regard to the use of email and related services.

Preamble

The provision of services related to information and communication technology is part of the public service mission of higher education. It serves both educational and professional goals, and also private use, in accordance with the provisions protecting privacy (residual use).

The University provides its Users with a work environment using electronic communication services, notably in order to improve the flow of information within the education system, making it accessible to all, so as to strengthen the coherence and effectiveness of educational and administrative processes.

The Policy begins by setting out the legal framework. By reminding Users of the laws governing the internet, the goal is to raise their awareness and thus ensure responsible behaviour.

The Policy defines the rights and obligations that the University is committed to respecting, including the conditions and limits of potential controls on the use of the service.

This Policy is specific to the University's email service (email and mailing lists exclusively). It is complementary to the University's Terms of Use for Information and Communication Technologies (ICT), to which it is appended.

Users are reminded of the existence of disciplinary sanctions, applicable in the event of any violation of the rules established by this Policy, or recalled herein.

Contents

THE POLICY BEGINS BY REMINDING USERS OF THE NEED TO RESPECT THE LAW

Article 1. Compliance with legislation

The ease with which information circulates and the amount of information available via internet should not obviate the need to respect the law. Internet and digital communication networks are not zones of lawlessness.

This non-exhaustive reminder of the laws that apply chiefly to the use of internet and messaging services is proposed with the dual objective of raising awareness of their existence so that Users respect them, and of strengthening the prevention of unlawful acts.

Are thus particularly (but not exclusively) prohibited, and subject to penal sanctions:

- invasion of personal privacy;
- defamation and insult;
- inciting minors to commit illegal or dangerous acts, encouraging corruption of minors, the pornographic use of images of minors, the dissemination of violent or pornographic messages likely to be viewed by minors;
- incitement and justification of acts of terrorism;
- incitement to consume illegal substances;
- incitement to commit crimes and offenses, incitement to suicide, and incitement to discrimination, including racial hatred or violence;
- justifying crimes, including murder, rape, war crimes and crimes against humanity; denying crimes against humanity;
- trademark infringement;
- the reproduction, representation or distribution of an intellectual creation (e.g. musical excerpt, photography, literary excerpt, etc.) or provision of related rights (e.g. interpretation of a musical work by an artist, a sound recording, video-recording, or programme produced by a broadcasting company) in violation of copyright, the related rights of the holder and/or the owner of the intellectual property rights;
- copies of commercial software for any purpose whatsoever, except for one backup copy, as allowed under intellectual property laws.

THEN IT IS AGREED AS FOLLOWS

Article 2. Description of the service provided

The University provides Users with an email service for "professional and personal (residual privacy)" use, allowing internal or external communication between different users, in accordance with the technical standards applicable to digital communication networks.
The University provides Webmail (an online email service) access for Users.
Webmail here refers to an email service via internet that allows email to be sent and handled.

Article 3. Defining "Users"

Technical information is now to be found in the document entitled "Technical details for the email service."
The User is granted access to digital services, including the email service provided by the University, in conformity with the technical information specified in the document "Technical details for the email service." (See Appendix 1.)

Article 4. Usage rights and User access

The means made available to the User for email access consist of a user name and a password, which are strictly personal, confidential and non-transferable (and should therefore never be transmitted to a third party, not even someone in a supervisory category). Users must never respond to any email requesting access codes, even if the request seems to come from a University IT department, or from an administrative or legal authority. Such requests are, in fact, phishing attacks.
No staff member, no entity, nor any administrative authority is authorized or empowered to request such information.

4.1 - With the exception of rules regarding generic electronic mailboxes, the right of access to email is personal, non-transferable and temporary. It is subject to tacit annual renewal.
Access may be withdrawn in the cases described in Articles 10 and 11.
4.2 - A doctoral student is primarily a student user and is accordingly provided with a student email address. A doctoral student may also be given an address as a University staff member, providing that the conditions of Article 3 are fulfilled.
4.3 - Users can ask the University to communicate any personal information concerning them and have it corrected in accordance with Act 78-17 of 6 January 1978, on computers, files and freedom, or any present or future legal provision or regulation serving the same purpose. Under the laws and regulations currently in force, the release of such information may be ordered by the court.
4.4 - The User acknowledges and accepts that the University exercises no control (except via anti-spam and anti-virus software) over the content of messages sent or received in the context of its email service. The University may not, therefore, be held responsible for any content so exchanged.
4.5 - Students will be able to relay emails received on their university email account to an email service outside the University. In this case, the University cannot be held responsible for any loss of data through the external mailbox service. Use of this setting is, however, strongly discouraged, for reasons of security and confidentiality. For this reason, University staff members do not have access to this option, with the exception of a white list of well-defined domains.
4.5 - In the case of loss of access codes, Users can regain access to digital services, and thus to their email accounts, by contacting the appropriate service as indicated by their local IT officer. An identity check will be carried out before any operation to restore access to digital services.

Article 5. Commitments of the University

The University provides access to its email service to any person fulfilling the conditions set out above in Article 3 and Appendix 1.

5.1 Technical requirements and service availability

The service complies with current internet technical norms and standards. University policy is described in Appendix 1 "Technical details for the email service."

5.2 Protecting the User's personal data

Pursuant to the provisions of the Data Protection Act 78-17 of 6 January 1978 and the legislation in force, the University agrees to comply with the legal rules of protection of personal data. The University provides the following guarantees for the User:

- To use any personal data solely for the purposes for which they are required (opening account access, and technical checks as specified in Article 5-4.)
- To communicate where such information is recorded and how long it will be conserved, which may in no event extend beyond the time required to achieve the purposes for which such data were collected or processed.
- The right of access to these data, with rectification if necessary.

5.3 Data retention

The University will archive for the legally required length of time, the date, sender and recipients of any messages that have transited via the system. Currently, this period is:

- 3 months; then, as anonymised data, for 1 year.

Message content (e.g. subject, message body, attachments, etc.) will not be subject to special archiving without the permission of the User (apart from system backups).

5.4 Technical inspections

The following technical means can be used to carry out checks on the use of University services:

- data storage control;
- data stream control;
- security control.

The User accepts *a posteriori* control of the use of the email service, that will cover only general indications of frequency, volume, message size, attachment format, without there being any control over the content of the messages exchanged.
The University guarantees that only these checking processes will be implemented.
These technical checks are justified:

- **either by concern for network security and/or IT resources;**

For maintenance, and technical and security management issues regarding the network and information system, the use of services including hardware and software resources, as well as exchanges via the network, can be analysed and verified, in compliance with applicable legislation, notably the rules relative to the protection of privacy and respect for private communications. In this context, the University reserves the right to collect and retain any information necessary for the smooth running of the system.

- **or to verify that the use of services is coherent with the objectives recalled in the Preamble and the rules set out in this Policy.**

Only email system administrators are authorised, for technical reasons, to carry out such checks, but they are bound to secrecy and are subject to the obligation of confidentiality. Access to the data recorded by University staff members (including personal correspondence) can only be justified in the case of a major incident.

Article 6. User Commitments

6.1 Compliance with legislation

The User undertakes to comply with current legislation, referred to non-exhaustively in Article 1. In particular:

- The User undertakes to use the service:
  - in compliance with the laws relating to literary and artistic intellectual property rights;
  - in compliance with the laws relating to IT files and freedoms;
  - in compliance with the rules relating to the protection of privacy and image rights of others, in particular.

- Users also undertake to send no messages of a racist, pornographic, paedophilic, defamatory or abusive nature, nor any message provoking or inciting terrorism, and to ensure, more generally, that no information of a delictual nature is disseminated by them.

  Are also (but not exclusively) prohibited and subject to penal sanctions:

  - Infringement of trademarks, designs, databases, patents or other intellectual property rights;
  - The reproduction, representation or distribution of an intellectual creation (e.g. music, photography, software, audio-visual or cinematographic works, etc.) or provision of related rights (e.g. interpretation of a musical work by an artist, a sound recording, video-recording, or programme produced by a broadcasting company) in violation of copyright, the related rights of the holder and/or of the owner of the intellectual property rights, or images of people without permission.

- When Users need to create files containing personal data, as defined by the Act of 6 January 1978 and the legislation in force, they will be very careful:
  - to follow the preliminary procedures set out by the CNIL (www.cnil.fr);
  - to provide prior information to the persons concerned regarding the ends to which such information will be used;
  - not to collect any information from minors about their family environment, the lifestyle of their parents, or their socio-professional status;
  - to provide prior information to the persons concerned about the risk, inherent to internet, that these data may be used in countries that do not provide an adequate level of protection for personal data.

6.2 Preserving service integrity

Users are responsible for their use of the service. Users will ensure the security of the email service, at their level, and undertake never to voluntarily disrupt its operation.

Users agree never to voluntarily use procedures that may affect email service operation. In particular, Users undertake:

- to send messages only to recipients actually interested or concerned in the subject matter, in order to avoid network and server congestion, and not force recipients to read messages of no interest to them;
- not to send bulk (or mass) emails;
- to prevent the risk of saturation of mailboxes and servers by not sending too many large documents in the same email, and using compression tools wherever possible;
- not to interrupt the normal operation of the network or connected systems;
- not to develop, install or copy programs to bypass security, or saturate resources;
- not to introduce viruses, but to adopt at least minimum antivirus security provisions;

- to immediately inform the University of any loss, any attempted violation, or anomaly regarding use of personal access codes or the email service.

- to use generic mail addresses whenever possible, to ensure continuity of service [1] especially in case of termination or extended absence.

6.3 Normal service procedures

The User undertakes to use the service in the most reasonable way possible. It is recommended not to transmit messages outside working hours.
It is recalled that sending a message does not imply an immediate response. The recipient should be allowed a reasonable response time.

To facilitate the flow of information, it is recommended:

- to indicate explicitly the object of each message, to address only one topic at a time, and to deal with that topic by a short message.
- for staff members, during non-professional exchanges, to indicate specifically and explicitly in the header that the message is private (e.g. "personal and confidential", or "private"). This rule is not applicable to students.
- to flag a message as "Urgent" only when really necessary, to prevent the tag rapidly losing all meaning.
- to insert the User's name in the body of the message sent, as a signatory, notably with the "insert signature" button.
- to indicate in the body of the message a brief description of any attachments;
- to send a link to a given document rather than to send it as an attachment.
- to use standard exchange formats (RTF, HTML, PDF, etc.) for attachments.
- to restrict the use of upper case characters. A text written in upper case is difficult to read and may be misinterpreted by the correspondent.

Email may cause stress and suffering. Better use of the service improves the quality of life at work. The CHSCT recommendations are provided in Appendix 2.

6.4 Procedure in case of absence or transfer of the User

In case of absence, Users agree to make use whenever possible of the out-of-office assistant from the email service, to generate the message of their choice, to be sent automatically in reply to any message received, specifying in particular the period of absence and other addresses where the message can be sent if necessary.

Upon the transfer of a User, steps should be taken to prevent that User's mailbox continuing to receive messages related to the position occupied before the transfer.
In case of final departure from the University, to ensure that emails do not remain unread, nor mailboxes unused, nor that personal or confidential messages be read by anyone but the intended recipient, Users agrees to the following procedure:

- Users will send a message to all their usual correspondents, indicating the date of departure, and informing them where to send any work-related messages from that date for the position previously occupied by the User (the email address of their successor, if known, the email address of the contract worker, or the generic email address).
- Just before their final departure, staff members will place all messages that are to be transmitted to their successor in a folder, to be left with the secretariat, or their immediate supervisor (this is not applicable to students).
- Users agree to re-route all messages received during the period when their email address remains active (Article 10) after departure, if intended for the position they previously occupied (this is not applicable to students).

In the event of the death of a User or if the User is absent without notice and cannot be contacted, the University reserves the right to remove any automatic reply or redirection message that would affect proper functioning of the services. Another auto-reply message may be added as required, at the University's discretion. The email service, on written request of the President, and in the manner defined in Article 6.5, may access the User's inbox to transmit any messages needed to ensure continuity of service. This is why it is recommended to use generic rather than personal mail addresses

6.5 In the event of death or departure of the User

In the case of death or departure of a User, and in particular for the purposes of continuity of service, the University may need to remove all previously drafted auto-reply messages, and replace them by a new message indicating where messages should now be sent. Any previous email transfer service may also be cancelled.

In addition, the User's email account will be sealed, and access to digital services from that account will be blocked, no more than 24 hours after notification of death or severance has been integrated into the human resources database or the tuition database by authorized services.

User information is, however, retained, in order for it to be available in case of legal requisition, or at the request of the President of the University, to ensure continuity of service. Data storage time cannot exceed the normal term of the account unless by court order.

In case of death, the User's family may not ask to recover any data without a court order.

6.6 Accessing a User's mailbox

At the request of the President of the University, in the event of the prolonged absence or death of a staff member, by invoking continuity of service to justify the transmission of certain messages, strictly controlled email access may be obtained, in the presence of witnesses (at least 2 people), to guarantee the procedure. Messages where the header contains "private", "confidential" or "personal" or where the purpose is unrelated to the continuity of service request cannot be accessed.

6.7 Fair and reasonable use of the service

The user agrees to fair and reasonable use of the email service, in order to avoid saturation, or misuse for personal purposes.

Users are required to log out of the service and close their browser immediately after accessing their email, especially if using public computer equipment. The University cannot be held liable for non-compliance with this obligation.

The User accepts that the institution may have knowledge of information necessary for the administration of the service (volume of data, incidents, nature of the traffic generated) and may take urgent measures to stop any disturbance caused. The University particularly reserves the right to stop access to the service in case of excessive use or use not in accordance with its purpose, as recalled in the Preamble.

The User agrees not to use email address lists or mailing lists, other than for administrative, educational or training purposes, as recalled in the present Policy.
The User is prohibited from advertising products or services by means of the email service offered by the University.

It is forbidden for the User to transmit an email after editing it or one of its attachments, without explicitly mentioning the changes made. When reusing only a portion of the text, such use must be clear and must not alter the original meaning of the document.

Users agree whenever possible to have anti-virus protection on the computer resources they use and to disable any functions that could expose the system to viruses. If Users are the victims of a virus in an attachment, they must stop using the email service and inform the IT manager for their service, and those to whom infected files have been sent, even those who sent the initial infected message.

The User specifically undertakes to destroy any alarming messages that prompt massive resending, to avoid the risk of infection by computer viruses. The mass transfer of such messages may result in saturation of the email service.

The User also agrees to comply with the procedures set up by the University to fight against malware and attacks by computer programs.

6.8 Specific conditions of use for the directory

In no case may personal data from the directory on which the email service relies be extracted, reproduced or distributed to third parties, without the express consent of the person concerned. Nor may such information be otherwise used for bulk emailing that is not strictly justified, for educational or administrative purposes, in particular in the case of a commercial or advertising approach, or for messages of a political or religious nature, contrary to the principles of neutrality of the French National and Higher Education Services.

Article 7. Generic mailing lists and email addresses

7.1 Generic addresses or lists

Within the limit of its technical means, the University may make available services that require one or more generic email addresses. Once created, these addresses allow the distribution of email messages to one or more people and thus allow collective work and continuity of service in case of absence or departure of staff.

Naming conventions for generic email addresses are described in Appendix 1: "Technical details for the email service."

Managing the address (adding/deleting subscribers) thus created is the sole responsibility of the person who requested its creation. Generic email addresses are established with the prior agreement of the staff members concerned.

The manager of the list must be in the University's personnel database and have an email address ending "u-bourgogne.fr".
It is up to the list manager to keep the recipient list updated. It is also possible to feed the subscriber list automatically (via database, LDAP directory etc.).

Email addresses of subscribers that do not have the ending "u-bourgogne.fr" will be accepted only if no u-bourgogne.fr exists for those subscribers.

Only a list manager or supervisor may request list manager changes. If a list manager resigns and cannot be contacted, a new list manager may be appointed by decision of the President or the Director General of the Service.

Messages sent to generic email addresses are subject to automatic archiving. Such archives cannot be kept for more than 3 years.

7.2 University mailing lists

University mailing lists are the sole responsibility of the University. All staff members and students are enrolled in these lists and do not have the power to unsubscribe from them.

The University allows unions occasional use of University mailing lists for general messages of union information. Usage rules are specified in the specific policy for unions.

University mailing lists are subject to moderation under the responsibility of the President and the Director General of the Service. However, the University cannot block the transmission of a message, except in the following cases:

- exceeding the allocated number of messages;
- content clearly in violation of the legislation on defamation and insults, or content not in compliance with standards of morality or the present Policy.

Article 8. Special duty of confidentiality and discretion

Safeguarding both University heritage and interests requires compliance by the User with a general and permanent obligation of confidentiality and discretion with regard to electronic information and documents available on the internal network, which implies that the User should:

- verify the level of confidentiality of documents before releasing them (by following the guidelines contained in an email if there are any);
- ensure that unauthorized parties cannot read such information on computer screens;
- never search for or open a message that was not sent to the User, without the recipient's permission.
- re-route any message received by mistake to the correct recipient, or return it to the sender, without reading it.
- check that there are no errors in the list of recipients;

Users agree whenever possible not to communicate their university email address on web servers that request it (especially when filling out forms), to avoid exposing such addresses to numerous advertising messages.

Article 9. How the red list works

The User may choose not to appear in the public directory of the University by using the red list. This red list is described in Appendix 1: "Technical details for the email service", which also sets out the procedure for joining the red list.

Article 10. Procedures for closing an account

Unless otherwise decided by the President or Director General of the University's services, the User's email account remains accessible:

- For one year after departure from the University, for University staff members;
- Until December 31 of the year after the student's final administrative registration, for students.

In exceptional circumstances, an email account may be closed no more than 24 hours after death or removal has been notified in the human resources database or the tuition database by the authorized services:

- In case of death, departure, or expulsion (only applicable to students)
- At the express request of the User to the President of the University (upon leaving the University).

The University will notify Users by email 45, 30 and 15 days before closing their email account. The procedure for extending the deadline will be indicated in the email.

The University cannot be held responsible if this message is placed in the User's spam folder and remains unread.

Email access may be extended to allow the User time to complete the necessary procedures with the Human Resources service, if so requested by the administrative head of the service. This type of extension is temporary and for a set length of time only.

Faculty members having filed for emeritus status upon retirement will retain access to their email account. For research associates, it will be necessary to provide the Human Resources service with an invitation letter signed by the head of the laboratory.

10.1 In case of access code disclosure

If a User has communicated account access credentials to a third party, account access may be blocked immediately for safety reasons. Access will be restored in the manner indicated in Article 4.6.

If a user communicates access codes, particularly by responding to the type of email message described in Article 4 (phishing email), it exposes the University to blacklisting by external email service providers (e.g. hotmail, orange, gmail, etc.). Messages from the University are thus rejected by these providers, with serious consequences affecting the entire University.
The account will be blocked immediately for safety reasons, and disciplinary sanctions may be imposed for repeat offenders.

10.2 In case of account inactivity

If a staff member's email account remains inactive during the two months following its creation, the account will be blocked for security reasons. Access will be restored in the manner set out in Article 4.6.

FINALLY IT IS STATED THAT NON-COMPLIANCE WITH THE CONTENTS OF THIS POLICY WILL BE SUBJECT TO THE FOLLOWING LIMITATIONS AND SANCTIONS

Article 11. Limitation of use

Particularly in the case of non-compliance with the rules defined in the present Policy and the procedures set out in the User guides, the "person legally responsible" may limit access as a precautionary measure, without prejudice to prosecution or whatever disciplinary sanctions may be brought against the User.

The "person legally responsible" means any person having the responsibility of representing the University, namely the President and the Director General of Services.

The University reserves the right to remove, without notice, any redirection that could cause a malfunction to the services, whether for security reasons or for contravening the Acceptable Use Policy.

Any abusive use, for non-academic purposes, of the resources made available to the User, is subject to sanctions.

Article 12. Sanctions

Failure to comply with rules set out or recalled in this Policy may result in suspension of access to the email service, and to disciplinary sanctions, independently of any legal action, including penal sanctions.

Article 13. Exemptions

Each request for exemption from the present Policy shall be addressed to the President of the University for validation. The President remains sole judge of such matters.

Article 14. Date of effect of the Policy

This Policy stipulates the rules and regulations regarding the use of email and related services, in force from this date.

Dijon, December 17, 2015

The President of the University of Burgundy

Alain Bonnin

Appendix 1: Technical details for the email service
Appendix 2: Recommendations by the CHSCT about email use

---

[1] To enable requests to be dealt with without interruption and without jeopardizing University operations, thus ensuring normal service.