

Policy on the use of information and communication technologies (ICT)

This document serves as the internal regulations governing the use of ICT.

Foreword

The information system comprises all the hardware, software, applications, databases and telecommunications networks that may be available to the user.

Mobile devices such as laptops, mobile phones and tablets are also included in the information network.

To ensure the smooth operation of the information system, it is essential to comply with the relevant legal and regulatory provisions, especially those relating to security, processing performance and the storage of personal data.

This document defines the regulations governing use and security that both the institution and the user undertake to follow: it specifies the rights and obligations of each party.

The policy may be supplemented by an appendix defining the main usage practices.

Users are informed of this policy by L'Institut Agro Dijon.

Statutory provisions

The main legal provisions in force governing this policy are as follows:

- law no. 78-17 of 6 January 1978, amended by the law of 6 August 2004, relating to information technology, files and civil liberties;
- law no. 2004-575 of 21 June 2004 on confidence in the digital economy;
- the provisions of the French Intellectual Property Code;
- the provisions of the French Penal Code;
- the provisions of the French Post and Telecommunications Code (in particular Book II on electronic communications);
- the provisions of the French Education Code (in particular Article L.123-3);
- the internal regulations of L'Institut Agro Dijon, Article 15-1.2.

The present policy remains subject to all other future legislative and regulatory provisions.

Definitions

"*IT resources*" refer to: networks, local computing or management resources, as well as those that can be accessed remotely, directly or by cascading from the organisation's network, software, applications, databases, etc.

"*Internet services*" refer to the provision by local or remote servers of various means of exchanging information: web, messaging, forums, IP (Internet Protocol) telephony, videoconferencing, etc.

The "*user*" is any person authorised by the Information Systems Department (ISD) to access and/or use the IT resources and Internet services, whatever their status: permanent or contract staff of L'Institut Agro Dijon, students, external persons hosted either permanently or temporarily, etc.).

The "*systems and networks administrator*" is any person with full administrative access to the processing, storage and routing of information.

Systems and network administrators are required by their very duties to have access to all user information (email, Internet connections, logs) including that stored on the workstation hard drive. Such access is not in breach of any provision of the law of 6 January 1978.

However, said user information may not be used, whether on one's own initiative or by instruction from management, for purposes other than those relating to the normal operation and security of the applications.

Similarly, system and network administrators, who are bound by professional confidentiality, must not disclose any information that may have come to their knowledge in the course of their duties, in particular when such information is covered by the confidentiality of correspondence or concerns the private lives of users and does not jeopardise the normal technical performance of the applications, their security or the interests of the establishment. Nor can they be compelled to do so, unless specifically required by law.

Institutional commitment

L'Institut Agro Dijon undertakes to implement the necessary measures to ensure the security of its information system and to protect its users. It provides users with easy access to information system resources used for teaching, research, archiving and the administration of the institution. The resources provided are mainly for professional use, but the institution is obliged to respect everyone's privacy.

User commitment

Users must read this policy and agree to abide by it.

They are responsible for the use of the IT resources to which they have access. They have an obligation of discretion and confidentiality with regard to the information and documents to which they have access. This obligation implies compliance with ethical and professional standards.

Users are especially responsible for their use of the resources made available to them by L'Institut Agro Dijon. In any case, the user is subject to the obligations resulting from their status, contract or hosting agreement.

Article 1: scope

The rules of use and security set out in this policy apply to the institution and to all users, whether on-site or working remotely.

For users with IT system administrator responsibilities, their rights and obligations are stipulated in the appendix.

Article 2: conditions of use of IT facilities

2.1 Personal use

The institution's IT facilities are provided to users for work-related use.

Personal use, however, is permitted provided that it is reasonable in terms of both frequency and time, and is not for commercial use. It must not be detrimental to the quality of the user's work, to the time he or she devotes to it or to the smooth running of the service and the IT facilities.

All information is deemed to belong to L'Institut Agro Dijon, with the exception of data explicitly designated by the user as personal information. Accordingly, it is the user's responsibility to store private data in a space specifically provided for this purpose, and to ensure that it is backed up (see appendix).

The institution does not cover the cost of storing and processing staff members' private data.

2.2 Management of continuity of service for absences and departures

Users are responsible for their private data space, which they must delete when they leave permanently.

When processing personal data, L'Institut Agro Dijon undertakes to comply with European Regulation (EU) 2016/679 (GDPR) of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as well as with applicable national laws on the protection of personal data.

All questions relating to access, amendment or removal of personal data should be sent to: dpo@agrosupdijon.fr

L'Institut Agro Dijon undertakes to protect and secure this data using all appropriate technical and organisational measures.

Article 3: security guidelines

3.1 Applicable security rules

The institution will implement appropriate safeguarding measures on the information systems provided to users.

Users are informed that passwords are a security measure designed to prevent malicious use or misuse.

Levels of user access available are defined according to role (see appendix). Information systems security requires users to:

- comply with security instructions, especially the rules relating to password management;
- keep their password(s) strictly confidential and not disclose them to third parties;
- ensure compliance with login management rules, and especially not to use or try to discover other users' names or passwords.

Furthermore, the security of the resources provided to users requires a number of precautions:

- by the institution:
 - ensure that sensitive and/or confidential materials are not accessible during absences (apart from continuity measures put in place by management);
 - limit access only to resources for which the user is specifically authorised.
- by the user:
 - if the user does not have specific authorisation, he/she is not permitted to access or attempt to access information system resources, even if such access is technically possible;
 - not to connect directly to the local networks any equipment not provided by or authorised by the institution;
 - not to install, download or use software or software packages on the institution's equipment without permission (this rule may vary depending on the user's access level - see appendix);
 - comply with the institution's measures to prevent viruses and attacks by computer programs.

3.2 Obligation to report and inform

The institution must inform the user of any factors that may help him/her to assess the level of risk involved in using the information system.

Users must notify their superiors as soon as possible of any problems observed or any anomaly discovered, such as an unauthorised access to the information system, etc. They must also inform the site manager of the possibility for access to a resource that is not authorised for their role.

3.3 Security verification measures

The user is advised:

- that in order to carry out corrective, remedial or upgrading maintenance, the institution reserves the right to service the resources provided (remotely if necessary);
- that remote maintenance is preceded by notifying the user, except in an emergency,
- that any information that is preventing the user from accessing the system, or that presents technical difficulties in being forwarded to the intended recipient, may be isolated and, if necessary, deleted;
- that the information system may be monitored and inspected for statistical, traceability, optimisation, security or misuse detection purposes.

The details will be specified in the appendix.

Article 4: electronic communications

4.1 Email service

The use of email is a key element in optimising work and sharing information within the institution.

Email is a work tool that has professional and educational uses. However, it may be used for private communication (within the limits of restricted use set out in article 2.1).

Specific rules - which may be found in additional appendices to this policy - concern the use of email for:

- a) the attribution of email addresses;
- b) the content of electronic messages;
- c) sending and receiving messages: redirecting messages from the professional mailbox;
- d) the legal status and content of messages;
- e) storage and archiving of messages in strict compliance with the allocated quota;
- f) closing email accounts.

In this regard, the rules applied at L'Institut Agro Dijon are as follows:

- when the user leaves the establishment (transfer, retirement, end of contract, etc.), the maintenance of email access rights will be subject to a written request to the manager of the unit where the user worked and to the specific approval of the Director of L'Institut Agro Dijon and the Director of Information Systems.

In this case, in order to ensure continuity of service and activity, a person authorised by the unit manager may be designated to have access to the messaging system.

Email access may be retained for a maximum of 2 (two) months, at the end of which time access to the account will be completely and permanently withdrawn.

- students and doctoral students will retain their email account until the end of the year following their graduation or thesis defence. After this period, the email account is deleted;
- redirection from a professional mailbox to a personal mailbox is prohibited.

4.2 Internet

Please note that the Internet network is subject to all current legal regulations. The use of Internet technology (by extension the intranet) is a key element in optimising work, sharing information and making it accessible both within and outside the institution.

The institution will provide users with Internet access whenever possible.

The Internet is a working tool for professional use (administrative and educational): it may be used for private purposes in compliance with current legislation and the limits set out in article 2.1.

The institution reserves the right to filter access to sites of an illicit nature, and to carry out a priori or a posteriori checks on the sites visited and the corresponding access durations.

This access is only authorised through the security systems implemented by the institution. Users are informed of the risks and limits inherent in the use of the Internet through training or awareness campaigns.

4.3 Downloads

When downloading files from the Internet, particularly sound and image files, users must comply with intellectual property rights.

The institution reserves the right to restrict the downloading of certain files, such as those that are very large or present a risk to information systems security (viruses likely to alter the normal operation of the information system, malicious code, spyware, etc.).

Article 5: data storage

Under the terms of articles L.34-1 and R.10-13 of the French Post and Electronic Communications Code, L'Institut Agro Dijon is legally obliged to retain technical data relating to the use of networks (internet, electronic mail, etc.). The data will therefore be kept for one year from the date it was saved. The methods and duration of data retention may be amended in accordance with the prevailing legislation.

Article 6: intellectual property rights

The institution gives a reminder that the use of IT resources implies compliance with the intellectual property rights of the institution, its partners and, more generally, all third parties holding such rights.

Consequently, all users must:

- use the software in accordance with the subscription conditions;
- not reproduce, copy, distribute, modify or use the software, databases, web pages, texts, images, photographs, videos or other creations protected by intellectual property law (copyright, etc.) without obtaining prior authorisation from the holders of these rights.

Article 7: compliance with the Data Protection Act

The user is reminded of the need to comply with the legal provisions relating to the automatic processing of personal data, in accordance with the French Data Protection Act no. 78-17 of 6 January 1978, as amended.

Article 8: restrictions on use and penalties

Should users fail to comply with the rules defined in this policy and the terms and conditions defined in the appendix, the "*person legally responsible*" may, without prejudice to any legal proceedings or sanctions that may be taken against users, limit use as a precautionary measure.

The "*person legally responsible*" is understood to mean any person with responsibility for representing L'Institut Agro Dijon, in this case its director and his/her delegates.

Any misuse of the resources provided to the user, for non-institution purposes, may, in addition to any criminal sanctions, result in the suspension of access to the information service and in disciplinary sanctions.

Article 9: enforcement of the policy

This policy and its appendix serve as the internal regulations governing the use of information systems.

This document supersedes all other documents or policies relating to the use of information systems.

Dijon 20 September 2023

The Director of L'Institut Agro Dijon

François Roche-Bruyn

*Policy accepted by the Dijon Site Specialised Panel on 19 September 2023
and for information by the Academic Council*

<p style="text-align: center;"><u>Appendix</u> to the policy for the use of information and communication technologies at L'Institut Agro Dijon</p>

The purpose of this appendix is to clarify certain provisions of the IT policy.

1. Storage of private data (article 2 of the policy)

It is the user's responsibility to create a folder called PERSO in the D workspace drive: (DATA).

It is also the user's responsibility to create a PERSO folder in their inbox for storing private messages.

2. Electronic communications (article 4 of the policy)

a) Attribution of email addresses

Each person who uses the school's information system is assigned an institutional email address.

This address is used by the administration and students for professional communications.

Users have a quota for their institutional address. If this quota is reached, messages can no longer be received. It is therefore the user's responsibility to manage their inbox in such a way that the quota is never reached.

Regarding the use of other addresses (e.g. educagri.fr), the user must refer to the rules in force relating to the use of this messaging system.

b) Email content

An email is a professional document, the content of which is subject to confidentiality or professional discretion.

c) Sending and receiving emails

L'Institut Agro Dijon cannot guarantee the timeliness or even the delivery of an email. If necessary, the user must ensure that the email is received, where applicable by contacting the addressee(s) if a reply is expected.

Internal rules for the use of computer rooms and self-access areas

Foreword

The computer rooms and self-access areas are multimedia spaces dedicated to the use of information and communication technologies (ICT).

Why a user policy?

The aim of these rules is to provide users with the information they need to make the best use of the Internet and the IT resources available in these rooms. They present the responsible behaviour that everyone at L'Institut Agro Dijon should adopt.

The purpose of these rules is to ensure that members and users have long-term access to equipment that is in good condition, so that they can make full use of the facilities.

Misuse of or damage to equipment can have consequences for everyone, including you, as the use of the room may be affected.

We rely on everyone's civic-mindedness to ensure that these rules are observed by all. Failure to comply may result in a penalty and/or a ban on access to the room.

The user is solely responsible for the content of data passing through L'Institut Agro Dijon's network.

Liability

As the Internet is based on the free circulation of data, no legal action may be taken against L'Institut Agro Dijon as a result of said content.

Users are responsible for the sites and documents they consult or download.

Internet viewing

It is forbidden to visit sites:

- that are discriminatory in nature;
- relating to procuring and similar offences;
- relating to gambling and trading;
- infringing on privacy;
- undermining a person's reputation;
- containing slanderous statements;
- involving an automated processing system for data that is pornographic, paedophilic, terrorist-related, xenophobic, contrary to public decency or contrary to public order.

The retrieval, dissemination or storage of illicit information constitutes an offence which may be punishable by law. L'Institut Agro Dijon may under no circumstances be held liable for the authenticity of information accessed on the Internet.

The deliberate installation of spyware programmes, viruses or software that emits viruses, or programmes to bypass software security and protection is prohibited.

In accordance with article L 112-2 of the French Intellectual Property Code, software is considered to be a work of authorship and is therefore subject to copyright legislation as defined in article L 111-1 of the French Intellectual Property Code.

Personal safety

Users must respect the calm atmosphere inside the premises and computer rooms.

Public users

The consumption of food, drinks and cigarettes by users is prohibited in the room.

Animals are not allowed in the room, except for service animals.

All users agree to use the equipment supplied with care and in accordance with their rights.

Use of computers

Should technical problems arise, users must not attempt to repair the equipment themselves. They must inform the Education Department staff.

Personal equipment may not be connected to the school's hard-wired computer network.

Cables and peripherals must not be disconnected by users.

Saving of personal or confidential documents is not recommended but is permitted and must be done on the server to the folder you have been allocated.

You are not permitted to delete, enter or modify contents on your computer (images, shortcuts, text files, sounds, etc.) outside your personal sessions.

You may not modify the configuration of the hardware outside your personal sessions (including display configurations: screen background, screensavers, icons, cursor, etc.).

All access to or maintenance of the information system (in its entirety or even just one of the devices made available by L'Institut Agro Dijon) falls under article L.323-1 of the French Penal Code and is punishable by law.