CEDEFOP’s
INFORMATION & COMMUNICATIONS TECHNOLOGY FACILITIES USE POLICY

1. PREFACE

1.1. ABOUT THIS DOCUMENT

The purpose of this document is to define the proper use of and set guidelines, rules and limits to the computing and networking infrastructure of Cedefop.

This policy is complementary to and applies in combination with the various existing policies of Cedefop.

1.2. GENERAL DEFINITIONS

In the text appear certain phrases with specially defined meaning, as follows:

1.2.1. The “ORGANISATION” or “Cedefop” is the European Center for the Development of Vocational Training.

1.2.2. A “USER” is every person who utilizes in any way an IT system or the Networking Infrastructure of the Organization. Users can be the Cedefop employees, managers, etc., as well as contractors, external consultants and temporary staff that use the Cedefop/IT Infrastructure.

1.2.3. “Cedefop/IT” is the department of Information Technologies and Telecommunications of Cedefop, its Head, permanent and temporary staff and the Helpdesk service, telephone ext. 119, e-mail helpdesk@cedefop.eu.int

1.2.4. “ADMINISTRATION” refers to the Head of Administration and the Directorate of Cedefop.

1.2.5. “ICT FACILITIES” or “ICT INFRASTRUCTURE” (Information & Telecommunication Technology Facilities or Infrastructure), refers to the computer systems, all peripheral equipment, the printers, the network services offered by computer servers of Cedefop, the access to the Internet, the installed software on computer workstations and servers, the telephony and the video-conferencing devices and services.

1.3. Cedefop/IT PROVISIONS

Cedefop/IT provides for the following:

1.3.1. Strategic planning and policy making for the Information and Telecommunication Technology in Cedefop.

1.3.2. Installation, maintenance, configuration, integration and upgrade of the IT Infrastructure, the hardware (computers and peripherals, printers) and the operating system.

1.3.3. Acquisition, maintenance, design, installation, deployment, configuration and customization, integration, evaluation and testing of software (office automation, business applications, collaborative software, server software). Purchase, maintenance and follow-up of software licenses.

1.3.4. Tele-communications and networks infrastructure, Internet connections, network security (Antivirus protection, network protection "Firewall").

1.3.5. System and network IT services and administration (E-mail, Microsoft Exchange collaboration services, network file storage, computer server administration, periodic data backup to magnetic tapes).

1.3.6. Development, implementation, maintenance and integration of IT applications.

1.3.7. Management of Telephony and Tele- & Videoconferencing audiovisual systems

1.3.8. First and second level technical support and assistance for all IT services, through the Helpdesk service, and through its permanent and temporary staff.

1.4. IT SECURITY MONITORING

Cedefop/IT maintains automated machine-based mechanisms which monitor and log network and Internet traffic/activities. The incoming-logging provides statistics on the use of Cedefop's web sites by the Internet. The monitoring is used to protect the security of the IT Facilities against network-oriented threats (viruses, malicious software, etc). Manual intervention to this information (internet traffic/activities) will happen only for technical or security reasons and only under the written request of the Administration and full knowledge of the person(s) concerned.

1.5. LIMITATION OF LIABILITY

1.5.1. The Organization provides the IT Facilities to users but will not be held responsible for any direct or indirect loss or damage caused by its use by the Users, either to the users themselves or to a third party.

1.5.2. Cedefop/IT strives to all technical and physical extend for the establishment of the good operation of all components of the Infrastructure, the seamless provision of services and for strong security protection. However it should be understood that the possibility of failures cannot be ruled out. Cedefop/IT will assume responsibility for such failures only when it can be proved that there was a serious miscarriage of Cedefop/IT's designated duties.

1.5.3. Cedefop/IT will notify the users for all scheduled downtime and for any exceptional outages of its services, using appropriate means (eg. the Intranet, or email to Cedefop users).

2. GENERAL IT USE

2.1. Users should make use of the IT infrastructure resources for professional purposes, with a sense of responsibility and with respect to the rights of others.

2.2. Users should not misuse the shared IT Infrastructure resources in any way, (e.g. overuse, monopolization or waste of storage space, network bandwidth, printers, printer toner and paper, clogging of the servers' CPUs, causing servers to hang, disrupting services etc.). Users should use the "duplex print" feature present to all Cedefop printers when possible.

2.3. Users should make use of the IT Infrastructure in accordance to local and European legislation (e.g. Greek Law 2121/1993 and 3057/2002 on copyrights, EU Copyright Directive 2001/29/EC, etc.) and should not use it to perform illegal activities.

2.4. Use of the IT Infrastructure for purposes of gaining financial of other personal profit is prohibited.

2.5. Users should not perform changes to the IT Infrastructure (eg. hardware changes, software installations, configuration changes, etc.), without the consent of Cedefop/IT.

2.6. Users should make good use of the parts of the IT Infrastructure (computer hardware, monitor and peripherals, etc.) that is assigned to them so that it is kept clean and it is not damaged in any way. In case of any damage caused or loss, Cedefop/IT should be notified immediately.

2.7. Use of the Organization's IT Infrastructure by the users should not oppose or harm the Organization's interests, should not damage or put in stake its reputation or public image and should be compliant to its regulations, rules and existing policies.

2.8. Any user that uses the Internet through the Infrastructure of the Organization should presume that he/she represents, to an extent, the Organization itself on the Internet, even in the case that this representation is not explicitly mentioned.

2.9. When Cedefop's computer network is being used to access another network, any abuse of the acceptable use policy of that network will be regarded as unacceptable use of Cedefop's network.

2.10. IT SECURITY

Users should not try to take advantage of Operation System flaws or other security vulnerabilities in order to circumvent the security policies, access other users' files, e-mail boxes, private data, or purposely exhaust the resources of computer systems, within the Organization or anywhere on the Internet (cracking and Denial of Service).

2.11. Users should not test the security of the computer systems without prior approval from Cedefop/IT. These procedures can cause "False alarms" and useless mobilization of the responsible mechanisms of the organization. Also, there should not be testing of viruses and other dangerous malware.

2.12. Cedefop/IT provides a schedule of regular copying of data from computer disks to tertiary storage (magnetic tapes), from where they can be retrieved in case of accidental loss or system damage. Data that need backup protection should be stored in the designated locations indicated by Cedefop/IT.

2.13. COPYRIGHTED MATERIAL,

Cedefop licenses the use of computer software from a variety of outside companies. Cedefop does not own this software or its related documentation and unless authorized by the software developer, does not have the right to reproduce it except for backup purposes.

2.14. Users should not make, acquire, use, make publicly available, sell or by way of trade expose copies of any material in electronic form (software, documents, images, graphics, audio and video files, etc.), contrary to the terms of their licensing agreement or to their intellectual property protection rights (copyright).

2.15. Any doubts concerning whether a User may copy or use a given material should be raised with a responsible manager and/or with Cedefop/IT before proceeding.

2.16. Users should regard all material downloaded from the Internet as subject to owner rights unless there is a specific statement clearly stating otherwise.

2.17. Cedefop discourages and reserves the right to block the exchange of material with specific, non-business related subjects, as listed in Table 1, Section 6.

2.18. USE FOR PERSONAL REASONS

Users are permitted limited use of the Internet and the IT infrastructure for personal needs, but only during free time, outside working hours and as long as the operational cost to Cedefop is negligible, normal activity is not affected and the use for business reasons takes precedence. This privilege may be revoked or limited at any time if deemed necessary for administrative of technical reasons.

3. E-MAIL AND MESSAGE POSTING

3.1. EMAIL ACCOUNT

All Cedefop employees are eligible for a personal electronic mail account. Cedefop provides electronic mail services to its employees for professional and for limited personal use if and only if there is no interest conflict and the reputation of the Organization is not damaged. When using the email services, users should also observe the rules of Section 2.

3.2. Users should not use the email services to send unsolicited bulk (massive) e-mail messages to other people, even if it is supposed to have good intention. “Unsolicited” stands for “without their permission or consent”.

3.3. Users should be suspicious when receiving emails with attachments and should verify that they know the sender and that the sender has intentionally sent this message. When in doubt, Users should not open the attachment and should consult the Helpdesk.

3.4. CONTENT OF PERSONAL MESSAGES

The Internet users of the Organization can declare their relationship with Cedefop through the Internet. In any instance this relationship is declared, it should also be explicitly stated that the user’s views are personal and do not necessarily represent those of Cedefop.

3.5. No declarations of support should be made for particular political viewpoints, products-services of other companies and generally declarations that could have a legal or other effect e.g. to the public image of the Organization.

3.6. The posting through the Internet of messages or announcements that defame, slander, threat or in any way harass any natural or legal persons, states, nations, races etc. is not permitted.

3.7. EMAIL CONFIDENTIALITY

In order to discourage the breaking of email confidentiality, any email sent by an e-mail address of the Organization may contain the following statement. “The information contained within this message are confidential and their use is only permitted by the intended recipient. In case you are not the intended recipient we inform you that revelation, reproduction, distribution or any other form of use of its contents is prohibited. If you have received the message in error or you think that errors have occurred during its delivery please notify the sender immediately by return e-mail and delete all copies of this message and any attachments. Thank you."

3.8. COUNTER UCE (UNSOLICITED COMMERCIAL EMAIL) MEASURES

Users should protect the privacy of their email address. Don't give it away to public web site registration pages or to mailing lists, as these may be archived and be accessible via public web pages.

3.9. In no case should you reply to UCE messages, even if they mention "click here to unsubscribe".

3.10. CHAIN-MAILS

E-mail/Internet users of the Organization should not participate in "chain-mails". Chain-mails are created through the posting of messages not related to professional activity (marketing material, jokes etc) that either contain pleas to the recipient to reproduce them many times or the recipient thinks that they have to be sent to many others. Such procedures are considered particularly dangerous since they waste valuable resources they are a common method for viruses and other malware spreading.

4. USER ACCOUNT AND PASSWORD POLICY

Every user that wishes to connect to the Cedefop IT Infrastructure or network is assigned an account and should use a password.

4.1. USER IDENTITIES ARE STRICTLY PERSONAL

Users should use only their own personal accounts provided by Cedefop to access the network and should not use any other account except of their own (see exception of paragraph 4.7).

4.2. The falsification, concealment or substitution of a user identity is prohibited. User names, e-mail addresses, titles and other related information included in email messages or announcements should accurately reflect on the real sender.

4.3. A legal account owner is responsible for all activities originating from his/her personal account and is liable in the case that his/her personal account is used for misconduct or illegal use of the network and the computing infrastructure. In case a user notices or suspects that someone not authorized to do so uses his/her account, he/she should notify Cedefop/IT immediately.

4.4. ACCOUNT LIFETIME

Users who leave Cedefop have the right to keep their account and have their e-mails forwarded to a new address for a specific, limited amount of time decided by Cedefop/IT, after which the account and the forwarding will be removed.

4.5. USER PERMISSIONS

Users are supplied permissions to the computers and the file system according to the needs of their duties and in coordination with the appropriate member of the administration hierarchy, e.g. the Head of the Department.

4.6. Users are prohibited from trying to circumvent IT security mechanisms in order to gain unauthorized access to another account and should not try to guess passwords.

4.7. USE OF AN ACCOUNT BY ANOTHER INDIVIDUAL

The use of an employee account in the computing and network infrastructure from an individual that is not the legal owner is allowed only for authorized personnel for conducting technical support or investigating security incidents. However, there can be an explicit statement by the legal owner of the account to Cedefop/IT that she/he wishes to grant specific rights of her/his account to someone else, eg. to temporarily receive a copy of her/his emails when absent.

4.8. PASSWORD GENERAL GUIDELINES

4.8.1. The Password belongs exclusively to each user, it is strictly personal and it is forbidden to be disclosed to anyone and for any reason.

4.8.2. The passwords should be memorized and not be written down on any means.

4.8.3. It is not recommended to use the Cedefop account passwords to systems or applications that do not belong to the network infrastructure of the organization. (e.g. private Internet accounts, web sites subscription, etc.)

4.8.4. Users should take special notice against “social engineering” techniques used to trick them into giving away their password, e.g. by pretending to be a System Administrator.

4.9. PASSWORD SELECTION GUIDELINES

4.9.1. The password size should be at least six (6) characters.

4.9.2. The password should have lower and upper case letters, numbers and punctuation marks or other symbols (e.g. @,#,&,$).

4.9.3. The password should change every six (6) to nine (9) months and should not be the same with the previous ones.

5. HANDLING OF SENSITIVE INFORMATION

5.1. INTERNET IS AN UNSAFE MEDIUM. Any information obtained from the Internet should be regarded as suspicious and incorrect until proved correct by comparing it to equivalent information from another, reliable, source. The Internet does not support a-priori protection mechanisms against the confidentiality and the integrity of the data transmitted through it. The personnel with access to Internet through the Organization’s Infrastructure should keep in mind that the data, which are exchanged through Internet, are not automatically protected from people who may “watch” the communication channel.

5.2. INTERNAL INFORMATION TRANSMISSION. Internal information or documents of any kind concerning the Organization, having a sensitive nature regarding their exposure to third parties, is permitted to be transmitted or to be rendered accessible from the Internet only after explicit authorization by Cedefop Administration and by Cedefop/IT.

5.3. RECIPIENT IDENTITY VERIFICATION. Before any user sends internal information of the Organization, enters any agreement or orders any product through the Internet on behalf of Cedefop, the identity of all parties involved should be verified using hard-copy letters, faxes or telephone verification and email delivery receipts.

5.4. FINANCIAL TRANSACTIONS THROUGH THE INTERNET. Users should be very careful when conducting personal or professional financial transactions via the Internet, as this is an insecure medium, as explained in previous paragraphs (5.1, 5.2, 5.3). If it is necessary to do so via Cedefop’s network infrastructure, users should be certain that (a) a secure channel is used (HTTPS) and (b) that passwords for sensitive transactions are not automatically stored on the computer.

6. WORLD WIDE WEB BROWSING

6.1. All Users have the ability of web browsing for professional and limited personal use only if none of the Organization’s interests is staking or Organization’s reputation is damaged. Web browsing is subject to the personal use limits described in paragraph 2.18 and to the general use rules of Section 2.

6.2. Cedefop discourages the visiting of Internet Sites with specific, non-business related subjects, as listed for example in Table 1, and reserves the right of restricting staff access to them.

- Adult Entertainment, Sex – Porn – XXX
- Computer Hacking – Underground
- Illegal Music – pirated Software
- Illegal Drugs
- Gambling
- On-line Games

- Militancy – Weapons – Violence - Racism/Hate.
- Personals/Dating

7. TELEPHONY AND VIDEO-CONFERENCING

Use of the telephony and video-conferencing service is also subject to the general use rules of Section 2. Users of telephony services should be polite when talking on the phone, should use their Personal Identification Number (PIN) for personal calls and should report any problems that appear to Cedefop/IT's Helpdesk.

Video-conferencing sessions are to be done after proper arrangement with the Conferencing service, by acquiring and completing the appropriate application form.

8. INCIDENT HANDLING

Users should notify Cedefop/IT immediately when they notice or suspect that

8.1.1. Sensitive organizational information is lost or leaked to unauthorized recipients.

8.1.2. Unauthorized access to an Organization's computing system has occurred, or any access codes or "proofs" of identity authentication leak, are lost or stolen.

8.1.3. Unusual behavior–activity of the computing systems occurs, since it might be an indication of security risk. Unusual behavior samples can be considered lost files, unusual system breakdowns, important error messages, etc.

8.1.4. A virus infection has occurred.

Cedefop/IT, which will then advise the user or take the necessary measures to handle the case.

9. TREATMENT OF INFRINGEMENTS

9.1. It is understood that policy infringements can occur out of ignorance or due to insufficient technical knowledge. In these cases the issues will be dealt with unofficially, with the necessary guidelines and directions given for the remedy.

9.2. In serious cases were an infringement is continuing or repeating, where there are stolen data, or are illegal actions, and in other serious incidents, Cedefop/IT will notify the Administration and according to the severity there will follow disciplinary sanctions:

9.2.1. *For Internal staff (officials, temporary, auxiliary, local, temporary agents,* sanctions will be according to the Regulations and Rules of the European Communities.

9.2.2. *For External staff (Contractors: external, interim, consultants, trainees, companies),* sanctions will range from verbal reprehension to financial penalties, suspension and termination. Where the Law is found to be broken, legal prosecution may also follow.