CEDEFOP | European Centre for the Development of Vocational Training

DIR/CFL/SAN/tsoba/RB(2013)00055
Thessaloniki, 16 January 2013

ACTING DIRECTOR

Information and Communication Technology (ICT) Use and Security policy

REFERENCE: This policy replaces Cedefop's ICT user policy of 25/09/2009 – RS/IT/2009/046

1. PURPOSE AND DEFINITIONS

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

1.1. General Definitions

The terminology used in this text is as follows:

1.1.1. 'ICT INFRASTRUCTURE' (Information and Communication Technology Infrastructure) refers to the computer systems, all peripheral equipment, printers, network services provided via computer servers of Cedefop, access to the Intranet and Internet, installed software on computer workstations and servers as well as telephony and video-conferencing devices and services.

1.1.2. A 'USER' is any person who utilises in any way an IT system or the networking infrastructure of Cedefop. Users are Cedefop staff members or external users (contractors, visitors, conference attendees, etc.).

1.1.3. 'Cedefop/ICT' is the Information and Communication Technology (ICT) service, which is part of the Area 'Resources' of Cedefop, its Head of Service, staff and the Helpdesk service, telephone extension 119, e-mail address: helpdesk@cedefop.europa.eu

1.1.4. 'ADMINISTRATION' refers to the Administration of Cedefop, represented by the Head of Resources and the Directorate of Cedefop.

Europe 123, 570 01 Thessaloniki (Pylea), GREECE | Postal address: PO Box 22427, 551 02 Thessaloniki, GREECE
Tel. +30 2310490111 | Fax +30 2310490049 | E-mail: info@cedefop.europa.eu | **www.cedefop.europa.eu**

Direct line: +30 2310490169 | Fax +30 2310490102 | christian.lettmayr@cedefop.europa.eu

16/1/13

1.2. CEDEFOP/ICT SERVICES

Cedefop/ICT provides the following:

1.2.1. Strategic planning and policy development for the information and communication technology in Cedefop.

1.2.2. Installation, maintenance, configuration, integration and upgrading of the ICT Infrastructure, hardware (computers and peripherals, printers) and operating systems.

1.2.3. 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.

1.2.4. Telecommunications and networks infrastructure, Internet connections, network security (Antivirus protection, network protection 'firewall').

1.2.5. System and network ICT services and administration (e-mail, Microsoft Exchange collaboration services, fax service, voice mail, network file storage, computer server administration, periodic data backup to magnetic tapes).

1.2.6. Development, implementation, maintenance and integration of ICT applications.

1.2.7. Management of telephony and videoconferencing audiovisual systems.

1.2.8. Technical support and assistance for all IT services by the Helpdesk service, and other ICT staff.

1.2.9. Cedefop/ICT will notify Users of all scheduled downtime and of any exceptional outages of its services, using appropriate means (e.g. via Intranet or e-mail to Cedefop Users).

1.3. ICT SECURITY MONITORING

Cedefop/ICT maintains automated machine-based mechanisms which monitor and log network and Internet traffic/activities. Inbound logs provide statistics on the use of Cedefop's web sites and services via the Internet and feed data to the Key Performance Indicators. Outbound traffic is logged through the proxy system and registers all user Internet access. The content of the information logged on the proxy system includes personal data such as user identification, volume of data exchanged from the Internet, date and time of the access to the Internet, IP address of the PC, content filter category etc. All categories of data processed and detailed information regarding the respective procedure and legal aspects

related to the Cedefop proxy system can be found in the "Note to the Data Protection Officer" and the "Privacy Statement" documents accessible on the Intranet. Monitoring is used to protect the security of the ICT Infrastructure against network-oriented internal and external threats (viruses, malicious software, etc.). Manual processing of this information (internet traffic/ICT activities) will occur only for professional, technical or security reasons at the written request of the Administration and with the full knowledge of the person or persons concerned.(also see Section 4.1.3.)

2. GENERAL ICT USE

2.1. General principles

2.1.1. All ICT equipment is subject to a common general use policy; the equipment is made available to members of staff to allow them to perform their professional duties at Cedefop. The use of the ICT equipment of Cedefop, in particular the e-mail server and Internet access, is in principle restricted to official use. However, incidental personal use of the e-mail and Internet servers of Cedefop are permitted as long as such utilisation is not contrary to the interests of Cedefop and the European Union and remains within reasonable limits.

2.1.2. Users shall not misuse the shared ICT infrastructure resources in any way, e.g. overuse, monopolisation and/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 available on all Cedefop printers whenever possible.

2.1.3. Use of Cedefop's ICT Infrastructure for the purposes of performing illegal activities and for financial or other personal profit is prohibited.

2.1.4. Users shall not perform changes to the ICT Infrastructure (e.g. hardware changes, software installations, configuration changes, etc.) without the prior authorisation of Cedefop/ICT.

2.1.5. Users shall use the parts of the ICT Infrastructure (computer hardware, monitor and peripherals, etc.) assigned to them in a diligent manner. In the event of any damage or loss, Cedefop/ICT shall be notified immediately.

2.1.6. When using the e-mail system and the Internet server, every member of Cedefop staff must at all times 'carry out his duties and conduct himself solely with the interests of the Communities in mind' (Article 11(1) of the Staff Regulations)

and 'refrain from any action or behaviour which might reflect adversely upon his position' (Article 12 of the Staff Regulations). These obligations are designed primarily to ensure that officials and other staff of Cedefop conduct themselves in a dignified manner consistent with the correct and respectable behaviour expected of Cedefop staff in carrying out their professional duties.

2.1.7. Users shall not test the security of the computer systems without the prior authorisation of Cedefop/ICT. Such tests could cause false alarms and unnecessarily trigger the response mechanisms of the Centre. Moreover, no viruses and other dangerous malware may be tested.

2.1.8. Cedefop/ICT schedules regular back-ups of data from computer disks to tertiary storage media from where they can be retrieved in case of accidental loss or system damage. Data that need backup protection should be stored in the locations designated by Cedefop/ICT.

2.2. INTELLECTUAL PROPERTY RIGHTS

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

2.2.2. Users must 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 agreements or to their intellectual property rights (copyright).

2.2.3. Users shall seek clarifications from their supervisors and/or from Cedefop/ICT when in doubt about copyright questions.

2.3. USE FOR PERSONAL REASONS

2.3.1. Users are permitted limited use of the Internet and the ICT infrastructure for personal needs, as stated above (2.1.1.) However, this permission applies only if the operational costs to Cedefop are negligible, regular ICT activity is not affected and use for business reasons takes precedence. This privilege may be revoked at any time if deemed necessary for professional, administrative or technical reasons.

3. ELECTRONIC MAIL

3.1. E-MAIL ACCOUNT

3.1.1. All Cedefop staff members are assigned a personal electronic mail account on taking up their duties at Cedefop. When using e-mail services, users must comply with the provisions of Section 2.

3.1.2. As is the practice at the Commission, external users who are required to use Cedefop e-mail services will be assigned e-mail accounts under the ext.cedefop.europa.eu domain.

3.1.3. Requests to open or close an e-mail account (of a staff member or external users) should be made by HR or the project manager by submitting the annexed form to the Head of Area for approval by the Head of Resources.

3.2. E-MAIL USE

3.2.1. Cedefop e-mail services shall be used mainly for professional purposes and shall not adversely affect the interests of Cedefop or the European Communities.

3.2.2. Users shall not use the e-mail services to send unsolicited bulk (massive) e-mail messages. 'Unsolicited' is defined as sent 'without the permission or consent of the recipient or recipients'.

3.2.3. Users should exercise caution when receiving e-mails with attachments and should verify the identity of the sender. In cases where they have doubts about the sender and/or the content, Users must not open the attachment and should consult the Helpdesk immediately.

3.2.4. Users should protect the privacy of their e-mail address. It should not be made public on non-professional web site registration pages or on mailing lists, as these may be archived and be accessible through public web pages.

3.2.5. Users shall not reply to UCE messages, even if they bear the words 'click here to unsubscribe'.

3.2.6. E-mail/Internet users of the organisation shall not participate in 'chain-mails'. Chain-mails are created by sending messages unrelated to professional activity (marketing material, jokes, etc.) and requesting the recipient to either reproduce them or to send them to others. Such requests are considered particularly dangerous since they are a common method of spreading viruses and other malware.

3.3. E-MAIL CONFIDENTIALITY

3.3.1. In order to discourage breaches of e-mail confidentiality, any e-mail sent from a Cedefop e-mail address to an external addressee must contain the following statement: 'This message may contain personal data and other confidential data that are entrusted to the recipients specified in the header of the message. The recipient(s) of this message shall not process the present message in ways contrary to EU legislation on the protection of personal data or jeopardise the confidentiality of the message content.'

4. USER ACCOUNT AND PASSWORD POLICY

Every user who wishes to connect to the Cedefop ICT Infrastructure is assigned an account and should use a password.

4.1. USE AND ACCESS OF PERSONAL ACCOUNTS

4.1.1. Users shall use only their own personal accounts provided by Cedefop to access the network.

4.1.2. Only authorised personnel providing technical support or investigating security incidents may use another person's account to access the computing and network infrastructure. However, legal owners of accounts can expressly inform Cedefop/ICT that they wish to grant specific rights over their accounts to another person, so that, for example, that person can access their e-mails temporarily during periods of absence.

4.1.3. The Administration of Cedefop may access the personal accounts of any staff members at any time for justified reasons, namely suspected illegal activities, suspected irregularities, improper conduct or other suspected wrongdoings or by having the written consent and agreement of the user involved. Access can take place only in cases where there is a reasonable suspicion of wrongdoing in the framework of an administrative investigation. Access should be limited to a closed number of competent persons under a strict need to know basis. (Data Protection Officer, Administration).

4.1.4. If Users notice or suspect that an unauthorised person has used or attempted to use their personal accounts, they shall immediately notify Cedefop/IT.

4.2. PASSWORD - GENERAL GUIDELINES

4.2.1. Individual passwords belong exclusively to each User, are strictly personal and, for security reasons, shall not be disclosed to anyone for any reason.

4.2.2. Passwords should be memorised and not written down or filed.

4.2.3. Users should be especially on their guard against 'social engineering' techniques used to trick them into disclosing their password, e.g. by pretending to be a system administrator.

4.3. PASSWORD - SELECTION GUIDELINES

4.3.1. The password should contain at least six (6) characters.

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

4.3.3. The password should be changed every six to nine months and should not be the same as the previous passwords.

5. OBLIGATIONS WHEN LEAVING CEDEFOP

When staff members leave Cedefop (on termination of their employment contracts, re-assignment, etc.), they must return the ICT equipment issued to them during their period of employment.

5.1. HARDWARE

5.1.1. Users must return any ICT equipment provided by Cedefop for the accomplishment of their professional duties no later than the end of their last working day. ICT infrastructure includes desktop PCs, laptops, desktop phones, DECT wireless phone devices, GSM phones, personal digital assistants (PDA) as well as any other accessories and peripherals (USB flash memories, SD cards, headsets, microphones, speakers, chargers, laptop cases, etc.).

5.2. SOFTWARE

5.2.1. Users are required to return any software provided by Cedefop which was installed on their personal computers, laptops, PDAs, GSM OS enabled phones, etc. on their last working day at the latest.

5.2.2. They are also required to return all software media (CDs, DVDs, ZIP, diskettes, SDs, MMCs) borrowed during their period of employment.

5.3. ACCOUNTS

5.3.1. When staff members leave Cedefop, their computer accounts expire at the end of their last working day. Access to accounts, computer files and the Intranet are not permitted after the accounts have expired.

5.3.2. Users are advised to inform their contacts well in advance that their e-mail addresses at Cedefop will no longer be available and that their accounts will be closed.

5.3.3. A message announcing the expiry of a User's account may refer to his or her new e-mail address. At the User's request and with the approval of the User's supervisor and the Head of Resources, this message may be available on Cedefop's system for up to three months.

6. USE OF THE INTERNET

6.1. The Internet is an insecure environment. Any information obtained from the Internet should be carefully checked. The Internet does not in principle have mechanisms to protect the confidentiality and integrity of data transmitted through it. Staff with access to the Internet via Cedefop's Infrastructure should bear this in mind.

6.2. Verification of recipient's identity. Before any User sends internal Cedefop information, enters into any agreement or orders any product on behalf of Cedefop through the Internet, the identity of all parties concerned should be verified by letter sent by post or fax or by telephone verification and e-mail delivery receipts.

6.3. Financial translations through the Internet. Users should be very wary when conducting professional or personal financial transactions via the Internet as it is an insecure medium. If the use of Cedefop's network infrastructure for financial transactions is unavoidable, Users should ensure that (a) a secure channel is used (HTTPS) and (b) that passwords for sensitive transactions are not automatically stored on the computer.

6.4. All Users may browse the web for professional and limited personal use.. Web browsing is subject to the restrictions on personal use set out in paragraph 2.18 and to the general use rules laid down in Section 2.

6.5. With respect to Internet use, the Cedefop ICT equipment may not be used to access offensive, racist, discriminatory, sexually explicit, obscene, and pornographic or other equally inappropriate web sites or for personal uses that exceeds reasonable limits. The reasonable limits have been setup to denote a threshold that is defined as twice the standard deviation of the monthly average use of the Cedefop users. Use which exceeds this threshold is deemed to be considered excessive. Users who find themselves over the threshold may be considered to have excessively used the Internet and this may lead to an administrative investigation and/or disciplinary action under the Staff Regulations. In this connection, Cedefop reserves the right to block access to certain web sites and categories of web sites.

7. USE OF TELEPHONY AND VIDEO-CONFERENCING

7.1. The use of the telephony and video-conferencing service is also subject to the provisions on general use laid down in Section 2. Users of telephony services shall behave in accordance with the Code of Good Administrative Behaviour of Cedefop.

7.2. Staff members are required to use their Personal Identification Numbers (PIN) for personal calls.

7.3. Video-conferencing sessions will be facilitated where appropriate, following timely arrangement with the Conference Service, by submitting the application form for this purpose seven working days before the planned event

7.4. Cedefop Mobile devices and SIM cards are assigned to Cedefop staff members after a request to the Head of Resources and the approval of the Directorate. The ICT Service provides tips on the intranet advising users on how to avoid excessive or unnecessary charges. These concern mostly roaming charges. As these are especially high outside of the EU, use in such locations should be restricted mainly to phone services and the absolute necessary. All calls business/personal have to be classified in the dedicated Fibus application by the respective users of the devices/SIMs.

8. PROVISION OF PRINTING INFRASTRUCTURE

8.1. The use of the printing services is also subject to the provisions on general use laid down in Section 2. The ICT service provides central printing stations in all floors/and cluster of offices. The central printing stations support A4 and A3 printing, in single and double sided, in grey scale and colour print outs.

8.2. All central printing stations support confidential and secure printing using PIN technology.

8.3. The ICT Service discourages the use of personal printers. Personal printers may only be used in exceptional cases and only after the approval of the Head of Resources or the Director.

9. INCIDENT HANDLING

Users shall notify Cedefop/ICT immediately if they notice or suspect that:

9.1. sensitive information or the organisation has been lost or leaked to unauthorised recipients;

9.2. unauthorised access to Cedefop's ICT Infrastructure has occurred, or any access codes or 'proofs' of identity have been leaked, lost or stolen;

9.3. unusual activity has occurred on Cedefop's ICT Infrastructure as this might be an indication of a security risk.. Examples of unusual activity include lost files, system breakdowns, important error messages, etc.

9.4. A virus infection has occurred

Cedefop/ICT will take the necessary measures in a timely manner to deal with the incident and will advise the User appropriately.

10. LOST OR STOLEN HARDWARE

In the event of case of loss or theft, users e obliged to take the following steps as soon as possible:

10.1. inform Cedefop/ICT immediately and follow their instructions;

10.2. make a detailed declaration of theft to the local authorities and inform ICT in writing;

10.3. in the case of an embedded services device (e.g. GSM device, GPRS-enabled laptop or mobile telephone), contact the service provider to have the services (GSM voice, GPRS data, etc.) temporarily or permanently blocked. Cedefop/ICT will assist in this matter.

11. TREATMENT OF INFRINGEMENTS

Any infringements of the rules laid down in this policy committed by staff members will be reported to the Administration. The Administration will assess the infringements in the light of the Staff Regulations and Cedefop's rules and

regulations and may decide take appropriate measures. Serious infringements may lead to administrative inquiries and/or disciplinary actions in accordance with the Staff Regulations.
Moreover, any infringements by external users will be dealt with in accordance with the provisions of the Greek Law on copyright (Law 2121/1993 as subsequently amended by Law 3057/2002 to transpose the provisions of Directive 2001/29/EU into national law). Depending on the severity of the case, the infringement will be prosecuted under national criminal or civil law.

Christian F. Lettmayr
Acting Director
Directorate

Contact:
Spyros Antoniou, Telephone: 30 2310490182, spyros.antoniou@cedefop.europa.eu