SUMMA College
middelbaar beroepsonderwijs
Brainport regio Eindhoven

Regulations and code of conduct

Use ICT - resources

Contents

1. Definition

ICT - resources:	The computer and network facilities made available to users by or on behalf of Summa College, including hardware, such as computers and printers; Software, such as computer programs and computer operating systems, communication facilities, etc.
User:	The person who makes use of the ICT - resources and/or the person in whose name the account with which the ICT - resources is used is registered.
Facilities Department:	The department within Summa College that is responsible for setting up, maintaining and securing the ICT resources. In the event that a project - network has been set up, the managers of this network are regarded as employees of the Facilities Department for regulatory purposes.
Supervisor:	The officer charged by or on behalf of Summa College with supervising the educational environment (in the broadest sense of the word).

2. Considerations

This text describes the use of ICT - resources by users at Summa College.
The following points have been considered in establishing this Code of Conduct:

1. The use of ICT - resources is necessary for Summa College users to support work or learning. However, incorrect use of these resources costs time and capacity of Summa College employees and equipment. Improper handling entails additional risks for this environment.
2. The use of ICT resources is subject to risks per manifestation that require the setting of rules of conduct and use. Risks include damage to the network by viruses, mallware or hacking software. This also includes leaking trade secrets and discrediting the good name of Summa College.
3. To avoid such risks, the Summa Board may issue regulations for the use of ICT resources and take measures to promote good order in the organisation. The rules set out below fall under this provision.
4. Against the background of the risks associated with the use of ICT resources, the user is expected to act with care and integrity.
5. The use of ICT - resources is committed. This registration is done to guarantee the continuity of the technical infrastructure, to prevent disruption of the business processes and other (financial) damage and to monitor compliance with the rules of conduct and use by the user.
6. Employees of the Facilities department generally supervise the use of ICT resources. If there is a suspicion of actions by the user that are contrary to the rules of conduct and use, an additional targeted investigation can take place as described in Article 6. If it appears that actions have been taken in violation of these rules, this can lead to disciplinary measures.
7. This code of conduct on the use of ICT resources:
    a. The rules the user must observe when using the ICT resources provided by Summa College.
    b. The circumstances under which the Summa Board decides to use the data traceable to persons regarding the use of the ICT resources.

3. Scope

This arrangement shall apply to:

1. Everyone who works for Summa College and makes use of the ICT resources made available by Summa College.
2. Anyone who, as a participant, has entered into an educational agreement with Summa College and makes use of the ICT resources made available by Summa College.
3. Anyone to whom Summa College has issued a user code.
4. Anyone who does not belong to the above categories, but to whom the Summa Board has granted permission to make use of the ICT resources made available by the Summa Board.

All of the above categories fall under the term user.
These regulations apply to both internal and external access to the Summa Board's ICT resources.

4. Authorized use

1. The persons referred to in Article 3 (Privacy) may use the ICT resources for work or learning and to a limited extent for personal purposes. In doing so, they must comply with the rules and procedures drawn up by Summa Board.
2. A user shall do everything that may reasonably be required of him/her to guarantee the confidentiality, integrity and availability of the data present on the information systems accessible to him/her.
3. A computer should not be left behind without locking/unlocking it.
4. The user will immediately report all (alleged) information security incidents that come to his/her attention to the Service Desk (applies to employees) or instructor (applies to participants).
5. When using the facilities and/or facilities, everyone must identify themselves using the means of authentication personally provided by Summa College, such as the user code and (strictly confidential) password.
6. The personally provided means of authentication may not be used to give third parties access to the ICT - means without the permanent supervision of the logged in user.
7. At the request of a supervisor, one must identify oneself by means of one's identity card or student card. Those who are unable or unwilling to identify themselves or who are not entitled to use the ICT resources are requested to stop using them immediately and to remove themselves. If this request is not complied with, coercive measures, such as those included in the Summa College Student Charter and the Cao Bve, may be used.
8. The user is obliged to take all reasonable precautions to prevent theft of any equipment, media and/or token issued to him/her by Summa College.

5. Unauthorized use

It is not permitted to use the ICT resources of Summa College:

1. Summa College or third parties to cause material or immaterial damage.
2. Infringe the rights of Summa College or third parties.
3. To cause nuisance or inconvenience or disturb public order.
4. To act contrary to applicable law, arising from, among other things:
    a. The Copyright Act.
    b. The Benelux Trademark Act.
    c. The Neighbouring Rights Act.
    d. The Data Files Act.
    e. The Penal Code.
    f. The Computer Crime Act.
    g. The Personal Data Protection Act.

   h. The Civil Code.
5. To do or refrain from doing so contrary to the written and unwritten law (customary law) which causes damage to another person (tort, art. 6:162 paragraph 2 of the Civil Code).
6. Use someone else's user code, password and/or E-mail address.
7. Use a different or fake user code, password and/or Email address, or otherwise attempt to conceal his identity.
8. By breaking or cracking a security code or not, to gain unauthorized access to other people's data, files and/or computer systems or to attempt to do so.
9. Intentionally (attempt to) break or crack a security or security code.
10. Send, post, make accessible by means of hyperlinks or otherwise make public any message or communication, the content of which may be considered offensive, immoral, discriminatory, inflammatory, defamatory, insulting, offensive, indecent or otherwise contrary to public order or morality.
11. Send, post, make accessible by means of hyperlinks or otherwise make public large quantities of messages (spam) or messages of a large size, of which the user knows or could or should have known that this disturbance, nuisance and/or delay can cause within the system, or at the recipient(s).
12. Send unsolicited messages, place them, make them accessible by means of hyperlinks or otherwise make them public, of which the person concerned knows, or could or should have known, that the messages are not for the benefit of the recipient(s) or were not made in the context of the training or the performance of the position.
13. Intentionally send, post, make accessible by means of hyperlinks or otherwise make public any message or communication of which the person concerned knows, could or should have known that its content is incorrect.
14. Send chain letters, external advertising messages, political announcements and similar messages, make them accessible by means of hyperlinks or otherwise make them public.
15. Generate incoming private messages by participating in non-business newsgroups, subscriptions to e-zines, newsletters and the like.
16. Make the facilities or facilities available to unauthorized third parties.
17. Make changes to the hard- or software, connect it, install it, or use it in any other way without indicating / allowing this use from the provided ICT.

It is also not allowed:

1. On the Internet:
   a. Visit sites that contain pornographic, racist, discriminatory, abusive or offensive material.
   b. View or download pornographic, racist, discriminatory, offensive or objectionable material.
   c. Unauthorized access to non-public resources on the Internet.
   d. Intentionally altering or destroying information accessed via the Internet without permission.
2. By e-mail:
   a. Send messages anonymously or under a fictitious name.
   b. Send or forward threatening, offensive, sexually-orientated, racist or discriminatory messages and chain mail.
   c. Harassing someone electronically.

If unsolicited information of this nature is offered, this must be reported to the teacher or confidential adviser as soon as possible, possibly supplemented by a written report to the Director of the School or Service concerned.

6. Powers of the Facilities department employees

The facilities department will apply the following approach to the management of ICT resources in general, both in general and in specific situations:

1. The Facilities department employees are charged with general supervision of the use of ICT resources for the purpose of system and network security. General supervision includes ensuring that the continuity of the services offered and the integrity and availability of the data offered are guaranteed, as well as excluding unauthorised access to the ICT environment.
2. The staff of service facilities are not authorised to view user data, unless the above mentioned point (1) applies or unless the user has given instructions himself, for example to solve technical problems. In doing so, confidentiality will be observed.
3. The employees of the Facilities Service are not authorised to remove undesired user data from the networks unless to avert a threat to the operation of the ICT resources or that it concerns data equivalent to data obtained through unauthorised use (see chapter 5). It is also possible to issue notifications to the user in order to remove unwanted data.
4. At least an anonymized virus scan is performed on user data. If there is reasonable suspicion of the presence of network threatening data (viruses, malware, hacking tools), an additional virus scan can be carried out. If network-threatening data is found, the data will be safeguarded and the user will be informed that this has been done with the question which solution directions will be chosen in consultation.
5. Group folders are limited in size by the Facilities department and are managed by specifically designated staff from the school or department concerned.
6. The employees of the Facilities department are authorised to take over a user's screen in the event of incidents, provided agreement has been reached with the user beforehand.
7. However, if it has been established with reasonable certainty that the user's actions seriously threaten the ICT infrastructure, the Facilities service can take over the screen without agreement in order to avert the threat. This will be reported in writing to the director of the school or service in question and recorded electronically in the central registration system for incidents and changes to the Facilities service (Topdesk).
8. The employees of the Facilities department are authorised to perform a file type scan on the personal folder and group folders, as well as to detect malware, hacking software, etc. using automated software. However, they are not authorised to carry out a manual scan of the content of files.
9. The employees of the Facilities department can grant rights to a personal folder of a staff member in the following cases:
    a. In (written) instructions from the Executive Board on the personal folder of a director.
    b. In (written) assignment of directors on the personal folder of their own employees and students.

    The granting of rights takes place in case of force majeure in case of urgent business interest (this can be understood to mean vacation of user, illness of user, dismissal etc.), legal coercion, or threat to the continuity of the service.
10. Employees of the Facilities service have an inherent duty of confidentiality in relation to data traceable to persons. Employees of the Facilities service take such measures that an appropriate level of security is achieved in view of the risks associated with the processing and the nature of the data to be protected.
11. If there is reasonable doubt that these regulations are being contravened, a specific investigation may be initiated at the request of a director of the school or department or on the instructions of the Board of Governors. In this specific investigation the user need not be known. The specific investigation will be reported to the applicant and the result of the investigation will be recorded in writing.

12. Targeted research will only take place as a result of justified suspicions or observation of incorrect use as referred to in article 5. The research will in principle be limited to traffic data of the use of e-mail and internet and will take place after written instruction from the head of ICT. The

Executive Board will receive a copy of this instruction and a written report of the results of the investigation. If the investigation does not give rise to any further action, the written report will be destroyed.

13. Only in the case of compelling reasons will a specific investigation into the content of e-mail be carried out with the written permission of the portfolio holder in the Executive Board. The written consent shall state these reasons.
14. E-mail messages from ©MR members in position, company doctors and other employees in a position involving confidentiality are in principle excluded from targeted research. This does not apply to the general supervision of system and network security.
15. In the event of a suspicion of incorrect use as referred to in these regulations, the relevant user will be held accountable for his/her behaviour by the manager as soon as possible.
16. The user in respect of whom a specific investigation has been or is being carried out may lodge a written and substantiated objection with the Executive Board within four weeks after the user has been informed about the investigation. A submitted objection does not suspend measures taken or to be taken.
17. The Executive Board shall respond in writing, stating its reasons, within four weeks after receipt of the objection. If the objection as referred to in the previous paragraph is declared well-founded, the data obtained by means of the investigative measures will be destroyed immediately. In addition, any measures will be revoked if - as the further investigation has shown - they were wrongly taken.

7. Powers of other employees

Because of the educational process and associated tasks, the following powers have been arranged:

1. Other employees are not granted any rights to the personal folders of other users.
2. Teachers and specially designated staff are authorised to take over a participant's screen for assistance in lessons, provided this has been communicated verbally in advance. In doing so, the students' right to privacy is taken into account.
3. Teachers can always view group folders of students. The structure of the educational data storage provides teachers with access to relevant data.
4. Designated persons can change student passwords when the student is legitimate.

8. Liability

1. Summa College excludes all liability for damage resulting from the use of the ICT resources.
2. Summa College excludes any liability for the quality and availability of the ICT resources and/or the information that is disseminated via this route.
3. Summa College excludes all liability in the event that the user does not comply with the laws and regulations generally applicable in the Netherlands.
4. User is liable for all damage that he inflicts on the ICT resources through intent or deliberate recklessness. User must compensate this damage to Summa College.
5. The User is liable for any damage caused to Summa College or third parties as a result of the sanctions taken by Summa College against the User and must compensate the User for such damage.
6. The User indemnifies Summa College against claims from third parties based on infringement by the User of third party rights.

9. Sanctions against users of ICT - resources

In the unlikely event that it is established and proven that these regulations have been violated or that the codes of conduct have not been adhered to, the following sanctions may be imposed:

1. The conditional or unconditional denial of access to and/or the use of ICT resources and/or the use of the user code, password and/or e-mail address.

2. Deleting or blocking information without delay. In doing so, other user information may also be deleted or blocked. The user is liable for all damages resulting from the deletion or blocking of information as referred to in this article, even if information other than the user's information is deleted or blocked in the process.
3. Students may be subject to disciplinary measures in accordance with the provisions set out in the Teaching Agreement and the Student Charter.
4. The provisions of the Collective Labour Agreement Bve are fully applicable to the employees of Summa College and the measures and sanctions referred to therein may also be taken.
5. Reporting an offence.
6. If a third party proves that his rights have been violated by the user, the identity of the user can be disclosed to this third party by the director.
7. The Board of Governors or the management of the school or service reserves the right at all times to take measures other than those mentioned here. If this is the case, this will be laid down in writing.

10. Lock

1. In all cases not provided for in these regulations, the Summa Board of Governors shall decide.
2. These regulations have been adopted by Summa College's Executive Board in consultation with the Participation Bodies.
3. **This scheme shall enter into force on 1 August 2014**