SUMMA College

middelbaar beroepsonderwijs
Brainport regio Eindhoven

Reglement en gedragscode

Gebruik ICT - middelen

Inhoudsopgave

1. Begripsomschrijving

ICT – middelen:	De door of namens het Summa College aan gebruikers ter beschikking gestelde computer- en netwerkfaciliteiten, waaronder hardware, zoals computers en printers; Software, zoals computerprogramma's en computerbesturingssystemen, communicatie-voorzieningen, etc.
Gebruiker:	Degene die van de ICT – middelen gebruik maakt en/of degene op wiens naam het account staat waarmee gebruik wordt gemaakt van ICT – middelen.
Dienst Facilities:	De dienst die binnen het Summa College belast is met het inrichten, onderhouden en beveiligen van de ICT – middelen. In het geval dat er een project – netwerk is ingericht, worden voor de regelgeving de beheerders van dit netwerk gezien als medewerkers van de Dienst Facilities.
Toezichthouder:	De functionaris die door of namens het Summa College is belast met het houden van toezicht in de onderwijsomgeving (in de breedste zin des woords).

2. Overwegingen

Deze tekst omschrijft het gebruik van ICT – middelen door gebruikers bij het Summa College.
De volgende punten zijn overwogen bij het vaststellen van deze gedragscode:

1. Het gebruik maken van de ICT – middelen is voor gebruikers van het Summa College nodig om werk of leren te ondersteunen. Maar onjuist hiermee omgaan kost tijd en capaciteit van medewerkers van het Summa College en apparatuur. Onjuiste omgang brengt extra risico's voor deze omgeving met zich mee.
2. Aan het gebruik van ICT – middelen zijn, per verschijningsvorm, risico's verbonden die nopen tot het stellen van gedrags- en gebruiksregels. Bij risico's valt te denken aan beschadiging van het netwerk door virussen, mallware of hacking software. Ook het uitlekken van bedrijfsgeheimen en het in diskrediet brengen van de goede naam van het Summa College valt hieronder.
3. Ter vermijding van dergelijke risico's kan het Summa College voorschriften geven voor het gebruik van de ICT – middelen en maatregelen nemen ter bevordering van de goede orde in de organisatie. De hierna weergegeven regels vallen onder deze bepaling.
4. Tegen de achtergrond van de risico's van het gebruik van ICT – middelen, wordt van de gebruiker zorgvuldig en integer handelen verwacht.
5. Het gebruik van ICT – middelen wordt vastgelegd. Deze registratie geschiedt om de continuïteit van de technische infrastructuur te waarborgen, verstoring van de bedrijfsprocessen en andere (financiële) schade tegen te gaan en om toezicht te houden op de naleving van de gedrags- en gebruiksregels door de gebruiker.
6. Door medewerkers van dienst Facilities wordt algemeen toezicht gehouden op het gebruik van ICT – middelen. Indien sprake is van een vermoeden van handelingen van de gebruiker die in strijd zijn met de gedrags- en gebruiksregels kan er een additioneel gericht onderzoek plaatsvinden zoals omschreven in artikel 6. Indien blijkt dat in strijd met deze regels is gehandeld, kan dit leiden tot disciplinaire maatregelen.
7. Deze gedragscode omtrent gebruik van ICT – middelen betreft:
    a. De regels die de gebruiker dient na te leven bij het gebruikmaken van de door het Summa College ter beschikking gestelde ICT – middelen.
    b. De omstandigheden waaronder het Summa College besluit tot het benutten van de tot personen herleidbare data omtrent gebruik van de ICT – middelen.

3. Werkingssfeer

Deze regeling geldt voor:

1. Iedereen die voor het Summa College werkzaam is en gebruik maakt van de door het Summa College beschikbaar gestelde ICT-middelen.
2. Iedereen die als deelnemer een onderwijsovereenkomst is aangegaan bij het Summa College en gebruik maakt van de door het Summa College beschikbaar gestelde ICT-middelen.
3. Iedereen aan wie door het Summa College een gebruikerscode is verstrekt.
4. Iedereen die niet tot de bovenstaande categorieën behoort, maar aan wie door het Summa College toestemming is verleend om gebruik te maken van de door het Summa College beschikbaar gestelde ICT-middelen.

Alle hiervoor genoemde categorieën vallen onder het begrip gebruiker.
Deze regeling is van toepassing op zowel interne als externe toegang tot de ICT-middelen van het Summa College.

4. Geoorloofd gebruik

1. De in Artikel 3 (Werkingssfeer) bedoelde personen mogen voor werken of leren en in beperkte mate voor persoonlijke doeleinden gebruikmaken van de ICT-middelen. Daarbij dienen zij zich te houden aan de door Summa College opgestelde regels en procedures.
2. Een gebruiker zal al hetgeen redelijkerwijs van hem/haar mag worden verlangd, doen om de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens die aanwezig zijn op de voor hem/haar toegankelijke informatiesystemen te waarborgen.
3. Een computer mag niet achtergelaten worden zonder deze te vergrendelen/uit te zetten.
4. De gebruiker zal alle (vermeende) informatiebeveiligingsincidenten, die hem/haar ter kennis komen direct melden aan de Servicedesk (geldt voor medewerker) of docent (geldt voor deelnemer).
5. Iedereen dient zich bij gebruik van de faciliteiten en/of voorzieningen te identificeren met behulp van de door het Summa College persoonlijk verstrekte authenticatiemiddel zoals de gebruikerscode en (het strikt geheim te houden) wachtwoord.
6. Het persoonlijk verstrekte authenticatiemiddel mag niet gebruikt worden om derden toegang te verschaffen tot de ICT – middelen zonder blijvend toezicht van de ingelogde gebruiker zelf.
7. Op verzoek van een toezichthouder dient men zich te legitimeren met behulp van zijn legitimatiebewijs of leerlingenpasje. Diegenen die zich niet kunnen of willen legitimeren of niet gebruiksgerechtigd blijken te zijn, wordt verzocht het gebruik van de ICT-middelen terstond te staken en zich te verwijderen. Indien aan dit verzoek geen gehoor wordt gegeven, kunnen dwangmiddelen, zoals onder meer opgenomen in het studentenstatuut Summa College en de Cao Bve, worden aangewend.
8. De gebruiker is verplicht alle redelijke voorzorgsmaatregelen te treffen ter voorkoming van diefstal van eventueel aan hem/haar door Summa College uitgereikte apparatuur, media en/of token.

5. Ongeoorloofd gebruik

Het is bij het gebruik van de ICT-middelen van Summa College niet toegestaan om:

1. Summa College of derden materiële of immateriële schade te berokkenen.
2. Inbreuk te maken op rechten van Summa College of derden.
3. Overlast of hinder te veroorzaken of de openbare orde te verstoren.
4. In strijd te handelen met het geldende recht, voortvloeiend uit onder andere:
    a. De Auteurswet.
    b. De Benelux Merkenwet.
    c. De Wet op de Naburige rechten.
    d. De Wet op de Databestanden.
    e. Het Wetboek van Strafrecht.
    f. De Wet Computercriminaliteit.
    g. De Wet Bescherming Persoonsgegevens.
    h. Het Burgerlijk Wetboek.
5. Te doen of na te laten in strijd met het geschreven en ongeschreven recht (gewoonterecht) waardoor een ander schade wordt aangedaan (onrechtmatige daad, art. 6:162 lid 2 BW).
6. Gebruik te maken van andermans gebruikerscode, wachtwoord en/of E-mailadres.
7. Gebruik te maken van een andere of geveinsde gebruikerscode, wachtwoord en/of Emailadres, of op andere wijze zijn identiteit trachten te verhullen.
8. Zich al dan niet door middel van het doorbreken of kraken van een beveiligingscode, ongeoorloofd de toegang te verschaffen tot andermans gegevens, bestanden en/of computersystemen of pogingen daartoe te ondernemen.
9. Een beveiliging of beveiligingscode doelbewust (pogen) te doorbreken of te kraken.
10. Berichten of mededelingen te verzenden, te plaatsen, toegankelijk te maken door middel van hyperlinks of anderszins openbaar te maken, waarvan de inhoud aanstootgevend, onzedelijk, discriminerend, opruiend, lasterlijk, beledigend, kwetsend, onbetamelijk of op andere wijze in strijd met de openbare orde of goede zeden kan worden beschouwd.
11. Grote hoeveelheden berichten (spam) of berichten van grote omvang te verzenden, te plaatsen, toegankelijk te maken door middel van hyperlinks of anderszins openbaar te maken, waarvan de gebruiker weet dan wel kon of behoorde te weten dat deze storing, overlast en/of vertraging kan veroorzaken binnen het systeem, of bij de ontvanger(s).
12. Ongevraagd berichten te verzenden, te plaatsen, toegankelijk te maken door middel van hyperlinks of anderszins openbaar te maken, waarvan de betrokkene weet, dan wel kon of behoorde te weten dat de berichtgeving niet ten behoeve van ontvanger(s) is noch is gedaan in het kader van de opleiding of de uitoefening van de functie.
13. Opzettelijk berichten of mededelingen te verzenden, te plaatsen, toegankelijk te maken door middel van hyperlinks of anderszins openbaar te maken waarvan betrokkene weet, kon of behoorde te weten dat de inhoud ervan niet juist is.
14. Kettingbrieven, externe reclameboodschappen, politieke mededelingen en daarmee vergelijkbare berichten te verzenden, te plaatsen toegankelijk te maken door middel van hyperlinks of anderszins openbaar te maken.
15. Inkomende privé-berichten te genereren door deel te nemen aan niet-zakelijke nieuwsgroepen, abonnementen op e-zines, nieuwsbrieven en dergelijke.
16. De faciliteiten of voorzieningen beschikbaar te stellen aan onbevoegde derden.
17. Wijzigingen door te voeren in de hard- dan wel software, deze aan te sluiten, te installeren, of anderszins te gebruiken zonder dat uit de ter beschikking gestelde ICT - middelen dit gebruik wordt aangegeven / toegestaan.

Tevens is het niet toegestaan dat:

1. Op internet:
   a. Sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten.
   b. Pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal te bekijken of te downloaden.
   c. Zich ongeoorloofd toegang te verschaffen tot niet openbare bronnen op het internet.
   d. Opzettelijk informatie waartoe men via internet toegang heeft verkregen zonder toestemming te veranderen of te vernietigen.
2. Door middel van e-mail:
   a. Berichten anoniem of onder een fictieve naam te versturen.
   b. Dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten en kettingmailberichten te verzenden of door te sturen.
   c. Iemand elektronisch lastig te vallen.

Indien ongevraagd informatie van deze aard aangeboden wordt, moet dit zo snel mogelijk aan de docent of vertrouwenspersoon worden gemeld, eventueel aangevuld door een schriftelijke melding te doen aan de directeur van de betreffende School of Dienst.

6. Bevoegdheden medewerkers dienst Facilities

De dienst facilities zal de volgende handelwijze toepassen bij het beheren van de ICT-middelen in het algemeen, zowel in het algemeen als in specifieke situaties:

1. De medewerkers van dienst Facilities zijn belast met het algemeen toezicht op het gebruik van ICT middelen met als doel systeem- en netwerkbeveiliging. Algemeen toezicht houdt in het zorgdragen dat de continuïteit van de aangeboden diensten alsmede de integriteit en beschikbaarheid van aangeboden data gewaarborgd blijft alsmede tot het uitsluiten voor toegang van onbevoegden tot de ICT omgeving.
2. De medewerkers van dienst facilities zijn niet bevoegd om gebruikersdata in te zien, tenzij het hierboven genoemd punt (1) aan de orde is of tenzij de gebruiker zelf opdracht heeft gegeven, bijvoorbeeld bij het oplossen van technische problemen. Hierbij zal geheimhouding betracht worden.
3. De medewerkers van de Dienst Facilities zijn niet bevoegd om ongewenste gebruikersdata van de netwerken te verwijderen tenzij om een bedreiging voor de werking van de ICT middelen af te wenden of dat het data betreft gelijk aan data verkregen door ongeoorloofd gebruik (zie hoofdstuk 5). Ook kunnen meldingen aan gebruiker worden afgegeven om ongewenste data te verwijderen.
4. Op gebruikersdata wordt tenminste een geanonimiseerde virusscan uitgevoerd. Indien er gerede verdenking bestaat op het aanwezig zijn van netwerkbedreigende data (virussen, malware, hacking tools) dan kan een additionele virusscan gemaakt worden. Indien netwerkbedreigende data word aangetroffen, wordt de data veilig gesteld en gemeld aan de gebruiker dat zulks is geschied met de vraag welke oplossingsrichtingen in overleg worden gekozen.
5. Groepsmappen worden door de dienst Facilities qua omvang gelimiteerd en worden beheerd door daartoe specifiek aangewezen personeel van betreffende school of dienst.
6. De medewerkers van de dienst Facilities zijn bevoegd om bij incidenten het scherm van een gebruiker over te nemen, mits vooraf hierover overeenstemming is bereikt met de gebruiker.
7. Indien echter met een gerede zekerheid geconstateerd is dat de gebruiker met zijn handelen de ICT infrastructuur ernstig bedreigt, kan de dienst Facilities zonder overeenstemming het scherm overnemen om de bedreiging af te wenden. Hiervan wordt schriftelijk melding gedaan aan de directeur van de betreffende school of dienst en elektronisch opgetekend in het centrale registratiesysteem incidenten en wijzigingen van dienst Facilities (Topdesk).
8. De medewerkers van de dienst Facilities zijn wel bevoegd om op de persoonlijke map en groepsmappen een bestandstype scan uit te voeren, alsmede met geautomatiseerde software malware, hacking software enzovoorts te detecteren. Zij zijn echter niet bevoegd om een handmatige scan op de inhoud van bestanden uit te voeren.
9. De medewerkers van de dienst Facilities kunnen in onderstaande gevallen rechten toekennen op een persoonlijke map van een personeelslid:
    a. In (schriftelijke) opdracht van het College van Bestuur op de persoonlijke map van een directeur.
    b. In (schriftelijke) opdracht van directeuren op de persoonlijke map van de eigen medewerkers en studenten.

    Het toekennen van rechten geschiedt in geval van overmacht bij dringend bedrijfsbelang (hieronder kan worden verstaan vakantie van gebruiker, ziekte van gebruiker, ontslag etc.), juridische dwang, of bedreiging van de continuïteit van de dienstverlening.
10. Medewerkers van de dienst Facilities hebben inherent aan hun functie geheimhoudingsplicht met betrekking tot gegevens over data die tot personen herleidbaar is.Medewerkers van de dienst Facilities nemen zodanige maatregelen dat een passend beveiligingsniveau wordt bereikt gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.
11. Indien er gerede twijfel bestaat dat er in strijd met dit reglement wordt gehandeld, kan op verzoek van een directeur van school of dienst of in opdracht van het College van Bestuur, een gericht onderzoek worden ingesteld. In dit gericht onderzoek hoeft de gebruiker niet te worden gekend. Het gericht onderzoek wordt gemeld bij de verzoeker en het resultaat van het onderzoek wordt schriftelijk vastgelegd.

12. Gericht onderzoek vindt slechts plaats naar aanleiding van gerechtvaardigde vermoedens dan wel constatering van onjuist gebruik zoals bedoeld in artikel 5. Het onderzoek beperkt zich in principe tot verkeersgegevens van het gebruik van e-mail en internet en vindt plaats na schriftelijke opdracht van het diensthoofd ICT. Het College van Bestuur ontvangt een afschrift van deze opdracht en een schriftelijk verslag van de resultaten van het onderzoek. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt het schriftelijk verslag vernietigd.
13. Alleen bij zwaarwegende redenen vindt na schriftelijke toestemming van de portefeuillehouder in het College van Bestuur gericht onderzoek naar inhoud van e-mail plaats. In de schriftelijke toestemming worden deze redenen genoemd.
14. E-mailberichten van ©MR-leden in functie, bedrijfsartsen en andere medewerkers met een vertrouwensfunctie zijn in beginsel uitgesloten van gericht onderzoek. Dit geldt niet voor het algemene toezicht op de systeem- en netwerkbeveiliging.
15. Bij een vermoeden van onjuist gebruik als bedoeld in deze regeling wordt de betreffende gebruiker zo spoedig mogelijk door de leidinggevende op zijn/haar gedrag aangesproken.
16. De gebruiker ten aanzien van wie gericht onderzoek is of wordt uitgevoerd kan daartegen schriftelijk en gemotiveerd bezwaar aantekenen bij het College van Bestuur binnen vier weken nadat de gebruiker is ingelicht over het onderzoek. Een ingediend bezwaar schort getroffen of te treffen maatregelen niet op.
17. Het College van Bestuur reageert schriftelijk en gemotiveerd binnen vier weken na ontvangst van het bezwaar. Indien het bezwaar als bedoeld in het vorige lid gegrond wordt verklaard, worden de door middel van de onderzoeksmaatregelen verkregen gegevens terstond vernietigd. Tevens worden eventuele maatregelen ingetrokken indien deze - naar achteraf blijkt uit het nader onderzoek - ten onrechte zijn genomen.

7. Bevoegdheden overige medewerkers

Vanwege het onderwijsproces en bijbehorende taken zijn de volgende bevoegdheden geregeld:

1. Overige medewerkers krijgen geen rechten op de persoonlijke map van andere gebruikers.
2. Docenten en speciale daartoe aangewezen medewerkers zijn bevoegd om ter assistentie in lessen het scherm van een deelnemer over te nemen, mits dit vooraf mondeling gecommuniceerd is. Hierbij wordt rekening gehouden met het recht op privacy van studenten.
3. Docenten kunnen groepsmappen van studenten altijd inzien. De structuur van opslag van de educatieve data voorziet in het inzien door docenten van relevante data.
4. Daarvoor aangewezen personen kunnen wachtwoorden van studenten aanpassen wanneer de student zich legitimeert.

8. Aansprakelijkheid

1. Summa College sluit iedere aansprakelijkheid uit voor schade die voortvloeit uit het gebruik van de ICT-middelen.
2. Summa College sluit iedere aansprakelijkheid uit voor de kwaliteit en beschikbaarheid van de ICT-middelen en/of de informatie die via die weg wordt verspreid.
3. Summa College sluit iedere aansprakelijkheid uit ingeval de gebruiker zich niet conformeert aan de algemeen in Nederland geldende wet- en regelgeving.
4. Gebruiker is aansprakelijk voor alle schade die hij door opzet, of bewuste roekeloosheid aan de ICT-middelen toebrengt. Gebruiker dient deze schade aan Summa College te vergoeden.
5. Gebruiker is aansprakelijk voor de schade die ontstaat voor Summa College of derden als gevolg van de door Summa College jegens gebruiker genomen sancties en dient deze schade te vergoeden.
6. Gebruiker vrijwaart Summa College voor aanspraken van derden op grond van inbreuk door de gebruiker op rechten van derden.

9. Sancties tegen gebruikers van ICT - middelen

Indien onverhoopt geconstateerd en bewezen wordt dat er sprake is van het overtreden van dit reglement of het niet aanhouden van de gedragscodes kunnen onderstaande sancties worden opgelegd:

1. Het voorwaardelijk of onvoorwaardelijk ontzeggen van de toegang tot en/of het gebruik van ICT-middelen en/of het gebruik van de gebruikerscode, wachtwoord en/of e-mailadres.
2. Het onverwijld verwijderen of blokkeren van informatie. Daarbij kan ook andere informatie van gebruiker worden verwijderd of geblokkeerd. De gebruiker is aansprakelijk voor alle schade die voortvloeit uit het verwijderen of blokkeren van informatie als bedoeld in dit artikel, ook wanneer hierbij andere informatie dan de informatie van gebruiker wordt verwijderd of geblokkeerd.
3. Voor studenten kunnen disciplinaire maatregelen getroffen worden conform de bepalingen zoals opgenomen in de onderwijsovereenkomst en het studentenstatuut.
4. Op de medewerkers van Summa College zijn de bepalingen van de CAO Bve onverkort van toepassing en kunnen ook de daarin genoemde maatregelen en sancties worden genomen.
5. Het doen van aangifte van een strafbaar feit.
6. Indien een derde aannemelijk maakt dat zijn rechten door de gebruiker zijn geschonden, kan de identiteit van de gebruiker aan deze derde kenbaar worden gemaakt door de directeur.
7. Het College van Bestuur of de directie van de school of dienst behoudt zich te allen tijde het recht voor om ook andere dan de hier genoemde maatregelen te treffen. Wanneer dit het geval is, wordt dit schriftelijk vastgelegd.

10. Slot

1. In alle gevallen waarin deze regeling niet voorziet, beslist het College van Bestuur van het Summa College.
2. Deze regeling is in overleg met de Medezeggenschapsorganen vastgesteld door het College van Bestuur van Summa College.
3. **Deze regeling treedt in werking op 1 augustus 2014**