Helicon
Opleidingen

Gedragscode

informatie- en communicatiesystemen

2016

Definitieve besluitvorming CvB	06-07-2016
1.1.1/201600322	

INHOUDSOPGAVE

VOORAF

De Gedragscode informatie- en communicatiesystemen geldt voor leerlingen en medewerkers van Helicon Opleidingen.
De Gedragscode geldt ook voor andere personen die de informatie- en communicatiesystemen van Helicon gebruiken. De regeling is onderdeel van het schoolveiligheidsbeleid van Helicon Opleidingen.

Het Bevoegd Gezag stelt de leerlingen en medewerkers in staat gebruik te maken van professionele communicatie- en informatiesystemen. Het Bevoegd Gezag verwacht op zijn beurt van de gebruikers een professionele en integere houding bij gebruikmaking van deze voorzieningen.
Dat wil zeggen dat leerlingen en medewerkers zich onthouden van gedragingen, die schade toebrengen aan materialen en middelen, die afbreuk doen aan het normale functioneren, die opzettelijk schade toebrengen aan de werkzaamheden of die in strijd zijn met de gangbare opvattingen van fatsoen en behoorlijk gedrag.

We gaan met elkaar om op basis van vertrouwen, gelijkwaardigheid en hoge verwachtingen en een gezamenlijke verantwoording voor het onderwijs.

Deze gedragscode geeft leerlingen en medewerkers inzicht in gewenst gebruik van informatie- en communicatiesystemen, waarbij gestreefd is naar een goede balans tussen controle op verantwoord gebruik, eigen verantwoordelijkheid en bescherming van de privacy van leerlingen en medewerkers.

Deel 1 van de gedragscode heeft betrekking op de medewerkers en deel 2 op de leerlingen.

's-Hertogenbosch, 6 juli 2016

dr.ir. A.F. Groen,
voorzitter College van Bestuur

Deel 1 Medewerkers

Deze gedragscode stelt regels aan het gebruik van informatie -en communicatiesystemen binnen de instelling en geeft voorschriften over de wijze waarop toezicht en controle op de naleving ervan plaatsvindt.
Controle op persoonsgegevens vindt plaats met als hoofddoel het tegengaan van misbruik.

Onder misbruik wordt verstaan:

a. handelingen die het normaal functioneren van werkplekken, het netwerk of onderdelen daarvan en de op het netwerk aangesloten systemen kunnen verstoren, zoals handelingen die de hardware en/of software kunnen beschadigen, die virussen kunnen introduceren, of die het inbreken ("hacken") op systemen als gevolg kunnen hebben;
b. het illegaal kopiëren, downloaden of verspreiden van software;
c. het gebruik van het netwerk voor of ter ondersteuning van activiteiten die in strijd zijn met enige wet;
d. het lastig vallen van andere gebruikers;
e. het verspreiden van voor personen of groepen beledigende, smadelijke of lasterlijke gegevens;
f. alle andere handelingen met gebruikmaking van de informatie- en communicatiesystemen of het netwerk die kunnen leiden tot schade aan de instelling of anderen.

Deze gedragscode geldt voor een ieder die werkzaam is bij de instelling en/of toegang heeft gekregen tot informatie- en communicatiesystemen van de instelling.

Hoofdstuk 1. Algemene uitgangspunten

1.1 De instelling kan het recht tot gebruik van (een deel van) een systeem of gegevensbron toestaan, maar ook altijd weer intrekken. Zonder dat recht is gebruik van (een deel van) een systeem niet toegestaan.

1.2 De gedragscode geldt voor gebruik van informatie- en communicatiesystemen binnen en buiten de gebouwen van de instelling.

1.3 De vastgestelde regels die momenteel gelden voor het vertegenwoordigen van de instelling en voor het verzenden van post (zoals correct taalgebruik) zijn ook van toepassing op digitale communicatie- en informatiesystemen (zoals e-mail, chatrooms, nieuwsgroepen, telefoneren via het internet enz.)

Hoofdstuk 2. Informatie- en communicatievoorzieningen

2.1 De door de instelling aan medewerkers verleende accounts zijn strikt persoonlijk. Het is dan ook niet toegestaan informatie over de gebruikersnaam of wachtwoord/toegangscodes aan anderen te verstrekken. Degene aan wie een account is verstrekt, blijft te allen tijde verantwoordelijk voor de wijze waarop onder haar/zijn naam van de netwerken en systemen gebruik wordt gemaakt.

2.2 De door de instelling beschikbaar gestelde informatie- en communicatievoorzieningen dienen te worden gebruikt ten behoeve van de functie-uitoefening.

2.2 Het is medewerkers daarnaast toegestaan deze voorzieningen in beperkte mate te gebruiken voor privé-doeleinden, mits dit niet storend is voor de dagelijkse functie-uitoefening van hen of anderen en voor zover anderen er geen aanstoot aan kunnen nemen.

2.4 Onder aanstootgevend gebruik wordt onder andere verstaan het bewust en stelselmatig opvragen en/of doorsturen van dreigende, (seksueel) intimiderende, pornografische dan wel racistische of anderszins discriminerende informatie.

2.5 Het is niet toegestaan om andere dan door de instelling geaccordeerde software op te slaan en/of te installeren en/of te verspreiden. Onder de afdeling automatisering worden ook begrepen de systeembeheerders op de vestigingen.

2.6 Medewerkers moeten zorgvuldig omgaan met vertrouwelijke gegevens en bedrijfsgevoelige informatie. Deze informatie en gegevens mogen niet toegankelijk worden voor onbevoegden.

2.7 Inbreuken op beveiliging van binnenuit de instelling of vanuit de buitenwereld dienen zo spoedig mogelijk aan de afdeling automatisering gemeld te worden via de helpdesk.

2.8 Het is niet toegestaan om op of via het internet:
- Sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
- Pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal te bekijken of te downloaden;
- Indien ongevraagd gegevens van deze aard worden aangeboden, dan dient dit zo spoedig mogelijk aan de leidinggevende gemeld te worden.

2.9 Het is niet toegestaan om door middel van digitale media:
- Niet zakelijke berichten intern te verspreiden;
- Berichten anoniem of onder een fictieve naam te versturen;
- Dreigende, beledigende seksueel getinte, racistische dan wel discriminerende berichten te versturen.
- Iemand op andere wijze dan hierboven vermeld lastig te vallen.
  Indien de gebruiker ongevraagd berichten van deze aard aangeboden krijgt, dan dient de gebruiker dit zo spoedig te melden aan de leidinggevende.

2.10 Een uitzonderingssituatie in verband met te verrichten werkzaamheden moet worden gemeld bij het CvB. Het CvB houdt hiervan een lijst bij.

Hoofdstuk 3. Handhaving

3.1 Handhaven van het beleid en de daaruit vloeiende maatregelen wordt uitgeoefend door de direct leidinggevende van de medewerker. Daarnaast neemt de afdeling automatisering organisatorische en technische maatregelen om te voorkomen dat onbevoegden toegang krijgen tot (persoons)gegevens, systemen en netwerken.

3.2 Internet, e-mail en overig dataverkeer wordt zo goed mogelijk gecontroleerd op virussen. Mocht blijken dat een bestand virussen bevat, dan wordt het automatisch tegengehouden. Mocht er onverhoopt toch een bestand met virus worden aangetroffen dan dient de ontvanger direct contact op te nemen met de helpdesk.

3.3 Er geldt een geheimhoudingsplicht met betrekking tot gegevens die tot personen herleidbaar zijn. De afdeling automatisering neemt 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.

3.4 Verkeersgegevens (gegevens over afzender, bestemming, datum en tijd) worden in beginsel niet langer bewaard dan zes maanden. Ingeval van een vermoeden van misbruik kunnen deze gegevens langer worden bewaard totdat de noodzaak daartoe is vervallen, hetgeen conform de Wet bescherming persoonsgegevens wordt gemeld bij het College Bescherming Persoonsgegevens en de betrokken medewerker.

3.5 Gericht onderzoek vindt slechts plaats naar aanleiding van vermoedens dan wel constatering van misbruik. Het onderzoek beperkt zich tot verkeersgegevens en vindt plaats na schriftelijke opdracht van de direct leidinggevende, de directeur van de betrokken medewerker of het College van Bestuur. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt het verslag uiterlijk na 6 maanden vernietigd. Alvorens tot vernietiging van het verslag over te gaan dient de betrokken medewerker de mogelijkheid te krijgen het verslag in te zien of in kopie te ontvangen. Uitgangspunt is dat de betreffende medewerker zo spoedig mogelijk wordt geïnformeerd en op zijn/haar gedrag wordt aangesproken. Indien besloten wordt de medewerker niet meteen te informeren dient in de schriftelijk opdracht de reden(en) daarvoor opgenomen te worden.

3.6 Controle van inhoud van e-mail, computer en bestanden vindt alleen bij zwaarwegende redenen en na schriftelijke toestemming van de direct leidinggevende, de directeur van de betrokken medewerker of het College van Bestuur (zie 3.5) plaats. In de schriftelijke toestemming worden deze redenen genoemd. De beoordeling wordt uitgevoerd door of onder verantwoordelijkheid van de direct leidinggevende. Uitgangspunt is dat de betreffende medewerker binnen een maand op zijn/haar gedrag wordt aangesproken.
Indien besloten wordt de medewerker niet meteen te informeren dient in de schriftelijke opdracht de reden(en) daarvoor opgenomen te worden.

3.7 De medewerker ten wiens laste een onderzoek als bedoeld in artikel 3.5 plaatsvindt, wordt zo spoedig mogelijk schriftelijk geïnformeerd over de aanleiding, uitvoering en het resultaat van het onderzoek. De medewerker wordt in de gelegenheid gesteld de aangetroffen gegevens te verklaren. Het verstrekken van informatie aan de medewerker wordt uitgesteld indien het onderzoek daardoor wordt geschaad. Indien besloten wordt de medewerker niet meteen te informeren dient in de schriftelijke opdracht de reden(en) daarvoor opgenomen te worden.

3.8 De medewerker ten aanzien van wie gericht onderzoek als bedoeld in artikel 3.4 of 3.5 is of wordt uitgevoerd kan daartegen binnen vier weken nadat hij op de hoogte is gebracht schriftelijk en gemotiveerd bezwaar aantekenen bij de direct leidinggevende of de persoon die in dat geval daartoe gemachtigd is.
De direct leidinggevende of daartoe gemachtigde persoon reageert schriftelijk en gemotiveerd binnen vier weken na ontvangst van het bezwaar. Indien het bezwaar gegrond wordt verklaard, worden de betreffende gegevens terstond vernietigd. Tevens worden eventuele maatregelen ingetrokken indien deze naar achteraf blijkt uit nader onderzoek ten onrechte zijn genomen.

3.9 De medewerker ten aanzien van wie gericht onderzoek als bedoeld in artikel 3.4 of 3.5 is of wordt uitgevoerd en wie zich onheus behandeld voelt of zich onterecht beschuldigd weet kan hierover een klacht indienen bij het College van Bestuur.

3.10 Digitaal materiaal dat zich bevindt op het netwerk of de daarop aangesloten computers of randapparatuur en dat in strijd is met de uitgangspunten van het informatiebeveiligingsbeleid of de gedragscode (zoals illegale software) wordt na overleg met de betrokken leidinggevende, de directeur of het College van bestuur verwijderd. De medewerker wordt hierover vooraf geïnformeerd, tenzij het onderzoek daardoor wordt belemmerd of het netwerk of andere informatie- en communicatiesystemen direct schade oplopen van dit digitaal materiaal en er direct actie moet worden ondernomen.

Hoofdstuk 4. Sancties

Het door medewerkers niet naleven van de gedragscode inzake het gebruik van informatie- en communicatievoorzieningen de instelling kan rechtspositionele gevolgen hebben. De werkgever kan bij overtreding van deze gedragscode de medewerker een disciplinaire maatregel opleggen.
De disciplinaire maatregel kan variëren van een schriftelijke berisping, schorsing of tot ontslag.
De disciplinaire maatregel dient evenredig te zijn met het gepleegde plichtsverzuim. Het opleggen van een disciplinaire maatregel is uitsluitend mogelijk indien voldoende bewijsmiddelen aanwezig zijn over het plichtsverzuim waaraan betrokkene zich schuldig heeft gemaakt.

Deel 2 Leerlingen

Deze gedragscode stelt regels aan het gebruik van informatie -en communicatiesystemen binnen de instelling en geeft voorschriften over de wijze waarop toezicht en controle op de naleving ervan plaatsvindt.
Controle op persoonsgegevens vindt plaats met als hoofddoel het tegengaan van misbruik.

Onder misbruik wordt verstaan:

a. handelingen die het normaal functioneren van werkplekken, het netwerk of onderdelen daarvan en de op het netwerk aangesloten systemen kunnen verstoren, zoals handelingen die de hardware en/of software kunnen beschadigen, die virussen kunnen introduceren, of die het inbreken ("hacken") op systemen als gevolg kunnen hebben;
b. het illegaal kopiëren, downloaden of verspreiden van software;
c. het gebruik van het netwerk voor of ter ondersteuning van activiteiten die in strijd zijn met enige wet;
d. het lastig vallen van andere gebruikers;
e. het verspreiden van voor personen of groepen beledigende, smadelijke of lasterlijke gegevens;
f. alle andere handelingen met gebruikmaking van de informatie- en communicatiesystemen of het netwerk die kunnen leiden tot schade aan de instelling of anderen.

Deze gedragscode geldt voor een ieder die een opleiding volgt bij de instelling en/of toegang heeft gekregen tot informatie- en communicatiesystemen van de instelling.

Hoofdstuk 1. Algemene uitgangspunten

1.1 De instelling kan het recht tot gebruik van (een deel van) een systeem of gegevensbron toestaan, maar ook altijd weer intrekken. Zonder dat recht is gebruik van (een deel van) een systeem niet toegestaan.

1.2 De gedragscode geldt voor gebruik van informatie- en communicatiesystemen binnen en buiten de gebouwen van de instelling.

1.3 De vastgestelde regels die momenteel gelden voor het vertegenwoordigen van de instelling en voor het verzenden van post (zoals correct taalgebruik) zijn ook van toepassing op digitale communicatie- en informatiesystemen (zoals e-mail, chatrooms, nieuwsgroepen, telefoneren via het internet enz.)

Hoofdstuk 2. Informatie- en communicatievoorzieningen

2.1 De door de instelling aan leerlingen verleende accounts zijn strikt persoonlijk. Het is dan ook niet toegestaan informatie over de gebruikersnaam of wachtwoord/toegangscodes aan anderen te verstrekken. Degene aan wie een account is verstrekt, blijft te allen tijde verantwoordelijk voor de wijze waarop onder haar/zijn naam van de netwerken en systemen gebruik wordt gemaakt.

2.2 De door de instelling beschikbaar gestelde informatie- en communicatievoorzieningen dienen te worden gebruikt ten behoeve van de functie-uitoefening.

2.3 Het is leerlingen daarnaast toegestaan deze voorzieningen in beperkte mate te gebruiken voor privé-doeleinden, mits dit geen onevenredige belasting vormt voor de informatie- en communicatievoorzieningen van de instelling en dit niet in strijd is met onderwijsbelangen van hen of anderen en voor zover anderen er geen aanstoot aan kunnen nemen.

2.4 Onder aanstootgevend gebruik wordt onder andere verstaan het bewust en stelselmatig opvragen en/of doorsturen van dreigende, (seksueel) intimiderende, pornografische dan wel racistische of anderszins discriminerende informatie.

2.5 Het is niet toegestaan om andere dan door de instelling geaccordeerde software op te slaan en/of te installeren en/of te verspreiden.

2.6 Inbreuken op beveiliging van binnenuit de instelling of vanuit de buitenwereld dienen zo spoedig mogelijk aan de afdeling automatisering gemeld te worden via de helpdesk.

2.7 Het is niet toegestaan om op of via het internet:
- Sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten;
- Pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal te bekijken of te downloaden;
- Indien ongevraagd gegevens van deze aard worden aangeboden, dan dient dit zo spoedig mogelijk aan de directeur gemeld te worden.

2.8 Het is niet toegestaan om door middel van digitale media:
- Niet zakelijke berichten intern te verspreiden;
- Berichten anoniem of onder een fictieve naam te versturen;
- Dreigende, beledigende seksueel getinte, racistische dan wel discriminerende berichten te versturen.
- Iemand op andere wijze dan hierboven vermeld lastig te vallen.
- Indien de gebruiker ongevraagd berichten van deze aard aangeboden krijgt, dan dient de gebruiker dit zo spoedig te melden aan de directeur.

Hoofdstuk 3. Handhaving

3.1 Handhaven van het beleid en de daaruit vloeiende maatregelen wordt uitgeoefend door de directeur van de leerling. Daarnaast neemt de afdeling automatisering organisatorische- en technische maatregelen om te voorkomen dat onbevoegden toegang krijgen tot (persoons)gegevens, systemen en netwerken.

3.2 Internet, e-mail en overig dataverkeer wordt zo goed mogelijk gecontroleerd op virussen. Mocht blijken dat een bestand virussen bevat, dan wordt het automatisch tegengehouden. Mocht er onverhoopt toch een bestand met virus worden aangetroffen dan dient de ontvanger direct contact op te nemen met de helpdesk.

3.3 Er geldt een geheimhoudingsplicht met betrekking tot gegevens die tot personen herleidbaar zijn. De afdeling automatisering neemt 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.

3.4 Verkeersgegevens (gegevens over afzender, bestemming, datum en tijd) worden in beginsel niet langer bewaard dan zes maanden. Ingeval van een vermoeden van misbruik kunnen deze gegevens langer worden bewaard totdat de noodzaak daartoe is vervallen, het geen conform de Wet bescherming persoonsgegevens wordt gemeld bij het College Bescherming Persoonsgegevens en de betrokken leerling.

3.5 Gericht onderzoek vindt slechts plaats naar aanleiding van vermoedens dan wel constatering van misbruik. Het onderzoek beperkt zich tot verkeersgegevens en vindt plaats na schriftelijke opdracht van de directeur. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt het verslag uiterlijk na 6 maanden vernietigd. Alvorens tot vernietiging van het verslag over te gaan dient de betrokken leerling de mogelijkheid te krijgen het verslag in te zien of in kopie te ontvangen. Uitgangspunt is dat de betreffende leerling zo spoedig mogelijk wordt geïnformeerd en op zijn/haar gedrag wordt aangesproken. Indien besloten wordt de leerling niet meteen te informeren dient in de schriftelijk opdracht de reden(en) daarvoor opgenomen te worden.

3.6 Controle van inhoud van digitale media vindt alleen bij zwaarwegende redenen en na schriftelijke toestemming van de directeur (zie 3.5) plaats. In de schriftelijke toestemming worden deze redenen genoemd. De beoordeling wordt uitgevoerd door of onder verantwoordelijkheid van de directeur. Uitgangspunt is dat de betreffende leerling binnen een maand op zijn/haar gedrag wordt aangesproken. Indien besloten wordt de leerling niet meteen te informeren dient in de schriftelijke opdracht de reden(en) daarvoor opgenomen te worden.

3.7 De leerling ten wiens laste een onderzoek als bedoeld in artikel 3.5 plaatsvindt, wordt zo spoedig mogelijk schriftelijk geïnformeerd over de aanleiding, uitvoering en het resultaat van het onderzoek. De leerling wordt in de gelegenheid gesteld de aangetroffen gegevens te verklaren. Het verstrekken van informatie aan de leerling wordt uitgesteld indien het onderzoek daardoor wordt geschaad. Indien besloten wordt de leerling niet meteen te informeren dient in de schriftelijke opdracht de reden(en) daarvoor opgenomen te worden.

3.8 De leerling ten aanzien van wie gericht onderzoek als bedoeld in artikel 3.4 of 3.5 is of wordt uitgevoerd kan daartegen binnen vier weken nadat hij op de hoogte is gebracht schriftelijk en gemotiveerd bezwaar aantekenen bij de directeur. De directeur reageert schriftelijk en gemotiveerd binnen vier weken na ontvangst van het bezwaar. Indien het bezwaar gegrond wordt verklaard, worden de betreffende gegevens terstond vernietigd.
Tevens worden eventuele maatregelen ingetrokken indien deze naar achteraf blijkt uit nader onderzoek ten onrechte zijn genomen.

3.9 De leerling ten aanzien van wie gericht onderzoek als bedoeld in artikel 3.4 of 3.5 is of wordt uitgevoerd en wie zich onheus behandeld voelt of zich onterecht beschuldigd weet kan hierover een klacht indienen bij het College van Bestuur.

3.10 Digitaal materiaal dat zich bevindt op het netwerk of de daarop aangesloten computers of randapparatuur en dat in strijd is met de uitgangspunten van het informatiebeveiligingsbeleid of de gedragscode (zoals illegale software) wordt na overleg met de directeur verwijderd. De leerling wordt hierover vooraf geïnformeerd, tenzij het onderzoek daardoor wordt belemmerd of het netwerk of andere informatie- en communicatiesystemen direct schade oplopen van dit digitaal materiaal en er direct actie moet worden ondernomen.

Hoofdstuk 4. Sancties

De directeur kan bij het niet naleven van de gedragscode door leerlingen inzake het gebruik van informatie- en communicatievoorzieningen bij een instelling een disciplinaire maatregel opleggen. De disciplinaire maatregel kan variëren van een schriftelijke berisping, schorsing of verwijderen van school. De disciplinaire maatregel dient evenredig te zijn met het gepleegde plichtsverzuim. Het opleggen van een disciplinaire maatregel is uitsluitend mogelijk indien voldoende bewijsmiddelen aanwezig zijn over het plichtsverzuim waaraan betrokkene zich schuldig heeft gemaakt.