

ICT-gedragscode leerlingen van de VMBO Scholen

Auteur(s): Bram Bogers, Niels Dutij

Vastgesteld: CvB/1718.053

Datum: 23 april 2018

Dit reglement is gebaseerd op Model reglementen voor het Hoger Onderwijs, een gezamenlijk product van SURFnet en SURFibo.



Deze publicatie is gelicenseerd onder een Creative Commons Naamsvermelding 3.0 Unported licentie
Meer informatie over deze licentie vindt u op <http://creativecommons.org/licenses/by/3.0/deed.nl>

Preambule

Onder Onderwijsgroep Tilburg vallen de VMBO-scholen: Campus 013, Schakelcollege Tilburg en Reeshof College (hierna te noemen: de school). De school biedt aan al haar leerlingen de mogelijkheid internet en netwerkvoorzieningen te gebruiken ten behoeve van hun opleiding. Tevens worden aan leerlingen voor persoonlijk gebruik een instellingsgebonden mailbox en mogelijkheden tot opslag van bestanden en persoonlijke studiegegevens beschikbaar gesteld ten behoeve van de opleiding. Aan het gebruik van deze faciliteiten (hierna te noemen: faciliteiten) zijn regels verbonden, welke zijn verwoord in dit reglement. Dit reglement geldt voor alle leerlingen van de school. Een 'leerling' is degene die is ingeschreven bij de school.

Afspraken in het kader van privacy worden separaat in het "Privacyreglement deelnemersgegevens" geregeld.

Artikel 1. Gebruik van faciliteiten

- 1.1 Computer- en netwerkfaciliteiten (zoals openbare computers, draadloze en bedrade netwerkaansluitingen, e-mail en internettoegang, opslagcapaciteit, printers en elektronische leeromgevingen) worden aan de leerling beschikbaar gesteld, onder meer voor het kunnen maken van opdrachten, verslagen en werkstukken, het bijhouden van de studievoortgang, het raadplegen van bronnen en het communiceren met docenten en medeleerlingen.
- 1.2 Het gebruik van eigen apparatuur en toepassingen op de faciliteiten van de school is toegestaan zolang dit gebruik voldoet aan de regels van dit Reglement. Het veranderen van instellingen in apparatuur en toepassingen beschikbaar gesteld door de school is alleen toegestaan met aparte toestemming van de ict-beheerder. Het aansluiten van eigen netwerkapparatuur waarmee de verbinding kan worden gedeeld met derden op de bedrade of draadloze netwerkaansluitingen, is te allen tijde verboden.
- 1.3 De aangeboden faciliteiten zijn alleen toegankelijk met behulp van een gebruikersnaam en wachtwoord. Deze zijn persoonsgebonden en mogen niet met anderen worden gedeeld. De leerling zal bij constatering of vermoeden van enig misbruik van zijn of andermans account direct melding maken bij de Servicedesk. De leerling is ook verplicht andere mogelijke beveiligingsincidenten zo snel mogelijk te melden bij de Servicedesk.
- 1.4 De ict-beheerder kan nadere eisen stellen aan de kwaliteit van wachtwoorden en andere beveiligingsaspecten. Bij een vermoeden van misbruik van een account kan de ict-beheerder per direct het betreffende account ontoegankelijk maken.
- 1.5 ICT-beheerders verschaffen zich slechts toegang tot accounts of computers van de leerling als de leerling daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan bij een duidelijk vermoeden van schending van dit Reglement, zoals nader bepaald in dit Reglement. De leerling zal in dat geval achteraf worden geïnformeerd.

Artikel 2. Intellectueel eigendom en vertrouwelijke informatie

- 2.1 De leerling maakt geen inbreuk op de intellectuele eigendomsrechten van de school en derden en respecteert de licentieafspraken zoals die van toepassing zijn binnen de school. De zeggenschap over de informatie van de school berust bij de school. De leerling heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend door de school.
- 2.2 Indien de leerling in het kader van zijn studie of het uitvoeren van taken voor de school toegang krijgt tot vertrouwelijke informatie of privacy gevoelige informatie waaronder persoonsgegevens, dient de leerling die informatie strikt vertrouwelijk te behandelen.
- 2.3 De leerling besteedt bijzondere aandacht aan het treffen van maatregelen zoals in dit Reglement genoemd, indien in het kader van het uitvoeren van deze taken de verwerking van vertrouwelijke informatie buiten de school noodzakelijk is zoals via e-mail, in niet instellingsgebonden Cloud-toepassingen, op externe opslagmedia of eigen client-apparatuur (USB-apparaten, Tablets, etc.).
- 2.4 Indien de school met betrekking tot het waarborgen van de vertrouwelijkheid en de intellectuele eigendomsrechten voorschriften heeft opgesteld, dient de leerling deze stipt op te volgen.

Artikel 3. Beveiliging door de school én de leerling

- 3.1 De school hanteert een streng beveiligingsbeleid en neemt adequate technische en organisatorische maatregelen om de infrastructuur te beveiligen tegen verlies, diefstal, criminele activiteiten, verlies van vertrouwelijkheid, schending van privacy-rechten en schending van intellectuele eigendomsrechten.

- 3.2 De school verlangt van de leerling een proactieve houding en serieuze stappen om de eigen computer en andere eigen apparatuur (zoals smartphones of tablets) adequaat te beveiligen. De leerling is te allen tijde zelf verantwoordelijk voor het gebruik van de eigen apparatuur en de op deze apparatuur opgeslagen gegevens.
- 3.3 In het bijzonder dient de leerling, indien met zijn apparatuur gebruikt wordt gemaakt van faciliteiten van de school, in het kader van beveiliging:
- deze apparatuur te voorzien van een up-to-date virusscanner en firewall;
 - regelmatig reserve kopieën te maken van alle relevante data en kopieën van data veilig op te slaan;
 - moeilijk te raden wachtwoorden te gebruiken en deze regelmatig te veranderen;
 - deze apparatuur up-to-date te houden wat betreft software-instellingen.

Artikel 4. Privégebruik en overlast

- 4.1 Beperkt privégebruik van de faciliteiten die door de school aan de leerling ter beschikking worden gesteld is toegestaan. Ieder gebruik, privé of voor studie, mag niet storend zijn voor de goede orde bij de school en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van de school of derden of de integriteit en de veiligheid van het netwerk aantasten.
- 4.2 Onder storend en/of overlast veroorzakend gebruik wordt in ieder geval verstaan:
- het raadplegen van internetdiensten met een pornografische, racistische, discriminerende, beledigende of aanstootgevende inhoud of het verzenden van berichten met een dergelijke inhoud;
 - het verzenden van berichten met een (seksueel) intimiderende inhoud of van berichten die (kunnen) aanzetten tot discriminatie, haat en/of geweld;
 - het versturen van berichten aan grote aantallen ontvangers tegelijk, het versturen van kettingbrieven of het verspreiden van kwaadaardige software zoals virussen, wormen, Trojaanse paarden en spyware;
 - filesharing- of streamingdiensten (zoals internetradio of Uitzendinggemist) te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de faciliteiten in gevaar kan brengen;
 - films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer de leerling weet/moet weten dat dit in strijd met auteursrechten is;
 - films, muziek, software en overig auteursrechtelijk beschermd materiaal te verspreiden (uploaden) naar derden zonder toestemming van de rechthebbenden.
- 4.3 Het gebruik van computer- en netwerkfaciliteiten voor commerciële activiteiten is uitsluitend toegestaan wanneer de school hiervoor schriftelijk toestemming heeft verleend.

Artikel 5. Monitoring door de school

- 5.1 Controle van gebruik van de faciliteiten vindt slechts plaats in het kader van handhaving van de regels uit dit Reglement en de wet- en regelgeving, ten behoeve van de goede orde op de school en de bewaking van de integriteit en de veiligheid van het netwerk en de computerfaciliteiten van de school.
- 5.2 Voor de in het voorgaande lid bedoelde controle worden geautomatiseerd gegevens verzameld (gelogd). Deze gegevens zijn alleen toegankelijk voor de direct verantwoordelijke systeembeheerders en worden alleen in geanonimiseerde vorm aan overige beheerders en andere verantwoordelijken beschikbaar gesteld. Deze kunnen tot nadere technische maatregelen besluiten, zoals een blokkade van de toegang tot een bepaalde dienst of het beperken van de mogelijkheden van het apparaat in kwestie om het netwerk te kunnen gebruiken.
- 5.3 In het bijzonder kan bij overlast, veroorzaakt door apparatuur van leerlingen, worden overgegaan tot uitschakeling van de netwerktoegangsmogelijkheden. Indien mogelijk wordt de leerling vooraf gewaarschuwd, zodat hij de gelegenheid heeft de overlast te staken. Wanneer dit wegens de vereiste spoed niet voorafgaand aan het nemen van de maatregel mogelijk is, doet de school zo snel mogelijk melding van de maatregel aan de desbetreffende leerling.
- 5.4 Bij vermoedens van overtreding van de regels kan controle worden uitgevoerd op het niveau van individuele verkeersgegevens van het gebruik van de faciliteiten. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats conform het bepaalde in artikel 6 van dit Reglement.
- 5.5 De school houdt zich bij het controleren op het niveau van verkeersgegevens of de inhoud onverkort aan de wet- en regelgeving. In het bijzonder beveiligt de school de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en worden personen met toegang daartoe contractueel verplicht tot geheimhouding.

Artikel 6. Procedure bij gericht onderzoek

- 6.1 Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens van de leerling worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit Reglement door die leerling.
- 6.2 Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van het College van Bestuur na advies van juridische zaken waarbij de reden vermeld zal worden waarom tot dit gerichte onderzoek zal worden overgegaan. Het onderzoek wordt uitgevoerd door één of meer daartoe aangewezen werknemer(s) van de afdeling ICT Services.
- 6.3 Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de faciliteiten. Als gericht onderzoek nader bewijs oplevert, kan de school na voorafgaande aparte toestemming hiervoor van het College van Bestuur, overgaan tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging direct vernietigd.
- 6.4 De leerling wordt zo spoedig mogelijk schriftelijk geïnformeerd door de schooldirecteur over de aanleiding, de uitvoering en het resultaat van het onderzoek. De leerling wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens. Uitstel van het informeren mag alleen als informeren het onderzoek daadwerkelijk zou schaden.

Artikel 7. Consequenties van overtreding

- 7.1 Bij handelen in strijd met dit Reglement of algemeen geldende (wettelijke) regels, kan de school afhankelijk van de aard en de ernst van de overtreding (disciplinaire) maatregelen treffen richting de leerling. Hieronder vallen in elk geval de navolgende straffen: een waarschuwing, een schorsing, een tijdelijke afsluiting of beperking van de faciliteiten (maximaal een jaar) en in ernstige gevallen verwijdering van de leerling.

Artikel 8. Slotbepalingen

- 8.1 Dit Reglement treedt in werking per 1 augustus 2018. De Gemeenschappelijke Medezeggenschapsraad heeft op 5 juli 2018 ingestemd met artikel 5 en 6 van dit reglement. Wijzigingen worden alleen ingevoerd nadat de Gemeenschappelijke Medezeggenschapsraad hiermee heeft ingestemd.
- 8.2 In gevallen waarin dit Reglement niet voorziet, beslist het College van Bestuur.
- 8.3 Dit Reglement komt ter vervanging van de ICT gedragscode voor leerlingen.