Gedragscode gebruik ICT en social media studenten

Versie: schooljaar 2020/2021.
Auteurs: Joris Weel (Security Officer), Jan van den Hazelkamp (Coördinator IPB) en Carol van Lent (Functionaris Gegevensbescherming).
Onderdeel van het IBP beleid van Curio.

Dit reglement vervangt de versie 2019 en treedt in werking na vaststelling door de Raad van Bestuur en na instemming door de aangewezen organen.

17-11-2020	De Raad van Bestuur stelt de herziene versie van het Informatie- en privacybeleid inclusief bijlagen vast voor Curio ,met instemming van de Studentenraad, de Ondernemingsraad en de Ouderraad vmbo scholen. Uitgezonderd zijn nog het Graaf Engelbrecht en het Stedelijk Gymnasium.
09-02-2021	Vastgesteld voor Graaf Engelbrecht.

Inhoud

1. Inleiding

1.1 Aanleiding

Curio biedt aan studenten[1] de mogelijkheid computers en internet te gebruiken ten behoeve van de studie. Tevens worden aan studenten voor persoonlijk gebruik een instellingsgebonden mailbox en mogelijkheden tot opslag van bestanden en persoonlijke studiegegevens beschikbaar gesteld ten behoeve van de studie. Aan het gebruik van deze faciliteiten zijn regels verbonden.

1.2 Scope

Deze gedragscode stelt regels aan:

- Het gebruik van ICT faciliteiten van Curio;
- Het gebruik van (privé) ICT-middelen waarmee de student is aangesloten op het computernetwerk van Curio;
- ICT middelen waarop je gegevens van Curio verwerkt;
- Het gebruik van Social Media met betrekking tot Curio;
- De inrichting van de werkplek waarbinnen je ICT-middelen en gegevens van Curio gebruikt;
- Regels met betrekking tot les op afstand.

Deze gedragscode geeft daarnaast voorschriften over de wijze waarop toezicht op en onderzoek naar de naleving ervan plaats vindt.

1.3 Doel

Doel van deze regels en voorschriften is de goede orde te bepalen ten aanzien van onder andere:

- Bescherming van (privacy gevoelige) gegevens van Curio en haar studenten;
- Bescherming van vertrouwelijke informatie van Curio en haar studenten;
- Bescherming van de intellectuele eigendomsrechten van Curio en derden waaronder het respecteren van de licentie-afspraken die van toepassing zijn binnen Curio;
- Tegengaan van (seksuele) intimidatie, discriminatie en andere strafbare feiten;
- Voorkomen van negatieve publiciteit;
- Voorkomen van schade aan en misbruik van ICT-middelen.

1.4 Reikwijdte

Dit Reglement geldt voor iedere student die bij Curio lessen volgt (studeert). Wijzigingen worden alleen bij het begin van een collegejaar doorgevoerd, behalve in dringende gevallen of wanneer Curio door omstandigheden van buitenaf gedwongen is tot een snellere invoering.

[1] Daar waar in dit reglement wordt gesproken over studenten worden ook leerlingen in de zin van de Wet op het Voortgezet Onderwijs (WVO) bedoeld.

2. Reglement

2.1 Gebruik van computernetwerk account

2.1.1 Toelichting

De student krijgt een account, waarmee toegang tot het computernetwerk kan worden verkregen.

2.1.2 Uitgangspunten

- De student dient te allen tijde zorgvuldig om te gaan met aan hem persoonlijk toegekende inloggegevens en aanvullende authenticatiemiddelen (zoals bijvoorbeeld smartcards en tokens).
- De door Curio aan student verleende accounts zijn strikt persoonlijk;
- Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld;
- Degene aan wie de accounts zijn verstrekt, is verplicht al hetgeen te doen dan wel na te laten wat redelijkerwijs van hem/haar mag worden verwacht om misbruik van de verstrekte accounts te voorkomen;
- Indien door nalatigheid, hetzij door opzet van de gebruiker systemen of het netwerk (deels) wordt platgelegd of hieraan op andere wijze schade wordt veroorzaakt zal de gebruiker het gebruik van deze voorzieningen worden ontzegd. Schade en kosten kunnen door Curio op de gebruiker worden verhaald;
- In gevallen waarin dit Reglement niet voorziet, beslist de Raad van Bestuur.

2.2 Gebruik van faciliteiten

2.2.1 Toelichting

ICT-faciliteiten, zoals (openbare) computers, draadloze en bedrade netwerkaansluitingen, e-mail, internettoegang, opslagcapaciteit, printers en elektronische leeromgevingen, worden aan de student 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 medestudenten.
Het gebruik van eigen apparatuur en toepassingen op de faciliteiten van Curio is toegestaan zolang dit gebruik voldoet aan de regels van dit Reglement.

2.2.2 Uitgangspunten

- Het veranderen van instellingen in apparatuur en toepassingen beschikbaar gesteld door Curio is alleen toegestaan met aparte toestemming van de IT-beheerder.
- Het aansluiten van **eigen** (netwerk-)apparatuur (zoals bijvoorbeeld servers, networked attached storage, access points en routers) is niet toegestaan.
- Het aansluiten van eigen client-apparatuur (zoals, laptops, tablets en telefoons) is alleen toegestaan op de daarvoor beschikbaar gestelde (wireless) netwerkaansluitingen. De IT-beheerder kan aan de toegang tot deze aansluitingen regels verbinden ter handhaving van dit reglement, zoals het moeten installeren van mobile device management (MDM), certificaten, virusscanners en eisen stellen aan de beveiligingsinstellingen, zoals bijvoorbeeld wachtwoordvereisten.
- Bepaalde faciliteiten zijn alleen toegankelijk met behulp van een gebruikersnaam en wachtwoord. Deze zijn persoonsgebonden en mogen niet met anderen worden gedeeld.
- De IT-beheerder kan nadere eisen stellen aan de kwaliteit van wachtwoorden en andere beveiligingsaspecten.
- Bij een vermoeden van misbruik van een wachtwoord kan de IT-beheerder per direct het betreffende account ontoegankelijk maken.
- De maker dan wel verzender van een elektronisch bericht vermeldt altijd zijn volledige naam en een onderwerp waarover het bericht gaat;
- Het is absoluut niet toegestaan internetsites te bezoeken, bestanden op het schoolnetwerk te plaatsen, of e-mailberichten te verzenden die godslasterlijk, (kinder-) pornografisch, racistisch of anderszins discriminerend materiaal bevatten;
- Opslag en verwerking van onrechtmatig verkregen informatie of informatie waarvan het bezit strafbaar is, zijn niet toegestaan, ook niet voor privédoeleinden.

- Het gebruik van computer, e-mail en internet mag geen onevenredige belasting vormen voor de IT-infrastructuur van Curio;
- Het is niet toegestaan software te gebruiken welke niet door Curio is aangeleverd of waarvoor vooraf geen schriftelijke toestemming tot gebruik is verkregen van Curio;
- Het is niet toegestaan handelingen te verrichten welke gericht zijn op het aanmaken, binnenhalen, en/of verspreiden van virussen in welke vorm dan ook, almede handelingen te verrichten welke gericht zijn op het ongewenst benaderen en/of binnendringen van computers en computersystemen (hacken);

2.3 Social Media gebruik

2.3.1 Toelichting

Bij het gebruik van sociale media gaat het om programma's waarmee online informatie kan worden opgezocht, gedeeld en gepresenteerd zonder of met minimale tussenkomst van een professionele redactie. Hoofdkenmerken zijn interactie en dialoog tussen de gebruikers. Denk bijvoorbeeld aan Facebook, Twitter, Instagram, YouTube, Snapchat, Whatsapp en alle hiermee vergelijke programma's en apps. Sociale media spelen een belangrijke rol in het dagelijkse leven. Sociale media kunnen helpen om het onderwijs te verbeteren en de lessen interessanter te maken, om contact te houden met vrienden en grenzen te verleggen. Aan het gebruik van sociale media kleven ook risico's, zoals pesten en het ongewild delen van foto's of andere gegevens. De afspraken zijn van toepassing op alle studenten van Curio.

2.3.2 Uitgangspunten

- We behandelen elkaar netjes en met respect, en laten iedereen in zijn waarde. Daarom pesten, kwetsen, stalken, bedreigen en beschadigen we elkaar niet. We maken elkaar niet zwart.
- Iedereen is verantwoordelijk voor wat hij/zij zelf plaatst op sociale media, en kan daarop aangesproken worden. Ook het doorsturen (forwarden) en herplaatsen (retweeten) zijn handelingen waar je op aangesproken kunt worden.
- Zorg dat je weet hoe de sociale media werken voordat je ze gebruikt, zorg dat de instellingen goed staan en je niet meer informatie deelt dan je wilt.
- Bij het gebruik van internet en sociale media houden we rekening met de goede naam van Curio en iedereen die daarbij betrokken is zoals docenten, onderwijsondersteunend personeel en externen ingehuurd door Curio.
- We helpen elkaar om goed en verstandig met sociale media om te gaan, en we spreken elkaar daarop aan. Als dat niet lukt, dan vragen we daarvoor hulp aan onze leraar of mentor, afdelingscoördinator of directeur/rector.
- De docent moet vooraf toestemming geven om een mobiele telefoon of sociale media in de les te gebruiken. Tijdens examens, toetsen, overhoringen en proefwerken gelden aangepaste regels.
- We respecteren elkaars privacy. Bij het gebruik van internet en sociale media worden er daarom geen informatie, foto's of video's verspreid over anderen, als zij daar geen toestemming voor hebben gegeven, of als zij daar negatieve gevolgen van kunnen ondervinden.
- Internet en sociale media worden alleen gebruikt voor acceptabele doeleinden. Het is daarom niet toegestaan om op school:
    - Sites te bezoeken of informatie te downloaden en te verspreiden die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend zijn;
    - Te hacken en ongeoorloofd toegang te krijgen tot niet-openbare sites of programma's;
    - Informatie, foto's of video's te delen waarvan duidelijk is dat die niet bedoeld is om verder te verspreiden, houd daarom je wachtwoorden geheim;
    - Verzonnen berichten te versturen of een fictieve naam te gebruiken als afzender;
    - Iemand lastig te vallen of te achtervolgen.

  Als iemand over de voorgaande punten informatie krijgt aangeboden, wordt dat gemeld aan de mentor.

Als er geconstateerd wordt dat de afspraken niet worden nageleefd, wordt dit eerst met de betrokkene besproken. Bij een ernstige overtreding kan de directie van Curio besluiten een maatregel op te leggen, die kan bestaan uit het uitsluiten van toegang tot het netwerk van de school, het in beslag nemen van de telefoon, het geven van een disciplinaire maatregel (straf) of in het uiterste geval het schorsen of verwijderen van de student van school. Daarnaast kan de directie contact opnemen met de politie indien er (mogelijk) sprake is van een strafbaar feit. Zo nodig wordt aangifte gedaan.

2.4 Les op afstand

2.4.1 Toelichting

Er zijn verschillende manieren om les op afstand te geven. Deze verschillende manieren hebben ook ieder een eigen impact op de privacy van zowel de student als de docent. Dit document geeft de richtlijnen aan voor het geven van les op afstand zoals Curio deze hanteert.

2.4.2 Algemene richtlijnen

- Zorg ervoor dat er geen privacygevoelige gegevens of andere personen ongewenst in beeld komen, zodra de camera aan staat.
- Bij voorkeur wordt de achtergrond vervaagt, middels de opties die de applicatie daarvoor biedt (blur functie).
- Bij voorkeur wordt er een headset of koptelefoon gebruikt.
- Bij voorkeur wordt de microfoon gedempt. Als de microfoon aan staat, zorgt de spreker ervoor dat er geen privégesprekken of andere storende geluiden hoorbaar zijn.

2.4.3 Voor studenten geldt:

- De studenten die thuis de les volgen, zijn niet verplicht gedurende de hele les de camera aan te zetten. Echter mag er van de studenten worden verwacht dat zij in beeld komen op de momenten dat de docent dit noodzakelijk acht.
- Studenten mogen de les niet opnemen en ook niet filmen.
- Studenten mogen geen foto's of screenshots van de les maken.

2.4.4 Voor docenten geldt:

- Docenten zijn niet verplicht om zichzelf in beeld te brengen, tenzij dit in het kader van het geven van onderwijs nodig is.
- Bij voorkeur worden de lessen niet opgenomen. Mocht dit toch nodig zijn, dan dienen de studenten te worden geïnformeerd over het doel en bewaartermijn van de opname. Deze opnames mogen niet openbaar gepubliceerd worden, niet met onbevoegden gedeeld worden en dienen na de afgesproken bewaartermijn verwijderd te worden.

Aanvullende richtlijnen bij het streamen van een les vanuit een locatie met studenten:

- Zorg ervoor dat de studenten die in de klas aanwezig zijn onherkenbaar in beeld zijn. Hang de camera bij voorkeur achter in de klas. Op die manier zijn gezichten niet zichtbaar in beeld.

2.5 Intellectueel eigendom en vertrouwelijke informatie

2.5.1 Toelichting

De student maakt geen inbreuk op de intellectuele eigendomsrechten van Curio en derden en respecteert de licentieafspraken zoals die van toepassing zijn binnen Curio.

2.5.2 Uitgangspunten

- De zeggenschap over de informatie van Curio berust bij Curio;
- De student heeft geen zelfstandige zeggenschap over de informatie behalve als hem dat expliciet is toegekend door Curio;
- Indien de student in het kader van zijn studie of het uitvoeren van taken voor Curio toegang krijgt tot vertrouwelijke informatie of privacy gevoelige informatie waaronder persoonsgegevens, dient de student die informatie strikt vertrouwelijk te behandelen (zie ook privacy reglement studenten);
- De student 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 Curio noodzakelijk is zoals via e-mail, in niet instellingsgebonden Cloud-toepassingen, op externe opslagmedia of eigen client-apparatuur (USB-apparaten, Tablets, etc.);
- Indien Curio met betrekking tot het waarborgen van de vertrouwelijkheid en de intellectuele eigendomsrechten voorschriften heeft opgesteld, dient de student deze stipt op te volgen.

2.6 Beveiliging door Curio én de student

2.6.1 Toelichting

Curio neemt informatiebeveiliging serieus. Curio 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.

2.6.2 Uitgangspunten

In het bijzonder dient de student, indien met zijn apparatuur gebruikt wordt gemaakt van de instellingsfaciliteiten, in het kader van beveiliging:

- Dat de apparatuur is voorzien van een adequate virusscanner en firewall;
- De eigenaar regelmatig reserve kopieën maakt van alle relevante data;
- Kopieën van data veilig opgeslagen worden;
- Moeilijk te raden wachtwoorden worden gebruikt en deze regelmatig worden veranderd;
- De apparatuur up-to-date wordt gehouden wat betreft software-instellingen.

2.7 Privégebruik en overlast

2.7.1 Toelichting

Beperkt privégebruik van de faciliteiten is toegestaan. Gebruik, privé of voor studie, mag niet storend zijn voor de goede orde binnen Curio en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van Curio of derden of de integriteit en de veiligheid van het netwerk aantasten.

2.7.2 Uitgangspunten

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 Uitzending gemist) 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 wanneer de student weet of had kunnen 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.

Het gebruik van computer- en netwerkfaciliteiten voor commerciële activiteiten is uitsluitend toegestaan wanneer Curio hiervoor schriftelijk toestemming heeft verleend.

2.8 Monitoring door Curio

2.8.1 Toelichting

Behoudens wettelijke uitzonderingen, vindt controle van gebruik van de faciliteiten slechts plaats in het kader van handhaving van de regels uit dit Reglement ten behoeve van de goede orde binnen Curio en de bewaking van de integriteit en de veiligheid van het netwerk en de computerfaciliteiten van Curio. Verboden gebruik van de faciliteiten wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

2.8.2 Uitgangspunten

- Voor deze 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.
- In het bijzonder kan bij overlast, veroorzaakt door apparatuur van studenten, worden overgegaan tot uitschakeling van de netwerktoegangsmogelijkheden. Indien mogelijk wordt de student 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 directeur/rector zo snel mogelijk melding van de maatregel.
- 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.
- Curio houdt zich bij het controleren op het niveau van verkeersgegevens of de inhoud onverkort aan de AVG en andere relevante regelgeving. In het bijzonder beveiligt Curio de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en worden personen met toegang daartoe contractueel verplicht tot geheimhouding.
- Algemeen toezicht door een daartoe aangewezen functionaris van de dienst IT en de andere IT- eenheden heeft als doel systeem- en netwerkbeveiliging te waarborgen. Algemeen toezicht houdt in het zorgdragen dat onbevoegden geen toegang krijgen tot (persoons)gegevens, systemen en netwerken;
- IT-functionarissen hebben geheimhoudingsplicht met betrekking tot gegevens over e-mail en internetgebruik die tot personen herleidbaar zijn.
- IT-functionarissen 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;
- Verkeersgegevens (gegevens over afzender, bestemming, datum en tijd) over e-mail- en internetgebruik worden in beginsel niet langer bewaard dan zes maanden. In geval van een vermoeden van onjuist gebruik kunnen deze gegevens langer worden bewaard totdat de noodzaak daartoe is vervallen;
- Bij een vermoeden van onjuist gebruik wordt de betreffende student zo spoedig mogelijk op zijn/haar gedrag aangesproken.
- Zaken die niet op Curio systemen en PC's thuishoren zoals eigen en/of illegale software, films en muziek, worden na overleg met de betrokken direct leidinggevende verwijderd. De student wordt hierover vooraf geïnformeerd tenzij het onderzoek daardoor wordt belemmerd;

2.9 Procedure bij gericht onderzoek

2.9.1 Toelichting

Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens van de student worden vastgelegd in het kader van een onderzoek naar aanleiding van een redelijke verdenking van een overtreding van dit Reglement door die student, dan wel andere misdragingen.

2.9.2 Uitgangspunten

- Gericht onderzoek vindt slechts plaats naar aanleiding van gerechtvaardigde vermoedens dan wel constatering van onjuist gebruik.
- Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de directeur/rector van de school, waarbij de reden vermeld zal worden waarom tot dit gerichte onderzoek zal worden overgegaan.
- De student te wiens laste een onderzoek plaatsvindt, wordt zo spoedig mogelijk schriftelijk geïnformeerd over de aanleiding, de uitvoering en het resultaat van het onderzoek. Het verstrekken van informatie aan de student wordt uitgesteld indien het onderzoek daardoor wordt geschaad;

    - Indien er sprake is van een redelijke verdenking van een overtreding van dit reglement of een andere misdraging is, dan wel het vermoeden bestaat dat een student zich schuldig maakt aan een **strafbaar feit**, kan er ook een heimelijke controle plaatsvinden. In dat geval zal de student pas achteraf, na afronding van het onderzoek, over de heimelijke controle worden geïnformeerd.
- De portefeuillehouder van de Raad van Bestuur ontvangt een afschrift van deze opdracht en een schriftelijk verslag van de resultaten van het onderzoek
- Gericht onderzoek beperkt zich in eerste instantie tot verkeersgegevens van het gebruik van de faciliteiten.
- Als gericht onderzoek nader bewijs oplevert, kan (namens) Curio na voorafgaande aparte toestemming van de Raad van Bestuur hiervoor, worden overgegaan tot het kennisnemen van de inhoud van communicatie of opgeslagen bestanden. De student wordt in de gelegenheid gesteld uitleg te geven over de aangetroffen gegevens.
- Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.
- Nader onderzoek naar de beveiliging of integriteit van randapparatuur mag in afwijking hiervan door de IT-beheerder worden uitgevoerd op basis van concrete aanwijzingen, zonder aparte toestemming. De resultaten van dit onderzoek worden alleen gedeeld met de student met het doel de beveiliging of integriteit van de randapparatuur te verbeteren.

2.9.3 Bezwaar

De student ten aanzien van wie gericht onderzoek is of wordt uitgevoerd kan daartegen schriftelijk en gemotiveerd bezwaar aantekenen bij de algemeen directeur/rector van Curio binnen vier weken nadat de student is ingelicht over het onderzoek.

- Een ingediend bezwaar schort getroffen of te treffen maatregelen niet op;
- De algemeen directeur/rector 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 controlemaatregelen verkregen gegevens terstond vernietigd.
- Tevens worden maatregelen ingetrokken indien deze ten onrechte zijn genomen;

2.10 Consequenties van overtreding

2.10.1 Toelichting

Bij handelen in strijd met dit Reglement of algemeen geldende (wettelijke) regels, kan Curio afhankelijk van de aard en de ernst van de overtreding disciplinaire maatregelen treffen. Hieronder vallen een waarschuwing, berisping, een tijdelijke afsluiting of beperking van de faciliteiten (maximaal een jaar) en in extreme gevallen een beëindiging van de inschrijving als student.

2.10.2 Uitgangspunten

- Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet worden getroffen enkel op basis van een langs geautomatiseerde weg uitgevoerde verwerking van persoonsgegevens, zoals een constatering van een automatisch filter of blokkade.
- Voorts worden geen disciplinaire maatregelen getroffen zonder dat de student gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.
- In afwijking van het voorgaande is het mogelijk dat Curio bij (geautomatiseerde) constatering van overlast een tijdelijke blokkade van de betreffende faciliteit invoert.
- Deze blokkade zal maximaal een week worden gehandhaafd of korter als de oorzaak naar tevredenheid van de IT-beheerder is weggenomen. Indien na een week geen verbetering is geconstateerd door de IT-beheerder, kan deze besluiten tot een langere blokkade. Bij herhaling van de oorzaak kunnen alsnog disciplinaire maatregelen worden genomen.