

(cog)

Christelijke Onderwijs Groep
Vallei & Gelderland - Midden



Reglement verantwoord netwerkgebruik leerling/student



Versiebeheer:

Versie	Status	Datum	Auteur	Omschrijving
1.1	Draft	20-8-2020	Ludo Cuijpers	1 ^e Draft
1.2	Concept	18-5-2021	Henk Links / Ludo Cuijpers	Tekst doorgenomen, uitgelijnd naar situatie COG, layout gemaakt, versie beheer toegevoegd.
1.3	Voorstel	19-5-2021	Henk Links	Aangeboden aan Benjamin Bommel (jurist), Bert Pik (IT-manager), Peter Hoogeveen (HR-manager) ter kennisname en verificatie.
1.8	Voorstel	18-6-2021	Henk Links	Opmerkingen verwerkt
1.9	Voorstel	19-6-2021	Henk Links	Gereed voor vaststelling

Vastgesteld door COG:

Versie	Datum	Naam	Functie

Inleiding

De scholen vallend onder de Christelijke Onderwijsgroep Vallei & Gelderland-Midden (hierna: de Instelling) biedt aan de eigen leerlingen en studenten (en in sommige gevallen ook aan bezoekende leerlingen/studenten) de mogelijkheid om diverse ICT-faciliteiten, zoals internetverbindingen, apparatuur en applicaties, te gebruiken (hierna samen: de Faciliteiten). Zo hebben leerlingen/studenten binnen de gebouwen van de Instelling de mogelijkheid om internet te gebruiken ten behoeve van de opleiding. Tevens worden aan leerlingen/studenten voor persoonlijk gebruik een instellingsgebonden e-mailbox en digitale leeromgeving en overige faciliteiten beschikbaar gesteld, ten behoeve van de opleiding.

Aan het gebruik van de Faciliteiten zijn regels verbonden, in het kader van de informatieveiligheid, beschikbaarheid, rechten van de Instelling en eventuele derden en een goede gang van zaken in de gebouwen en op de terreinen van de Instelling. Deze regels zijn in dit reglement voor leerlingen/studenten, hierna te noemen: het Reglement, opgenomen. Deze regels zijn van toepassing op leerlingen/studenten van de Instelling en bezoekende leerlingen/studenten. Het streven daarbij is een goede balans aan te brengen tussen verantwoord en veilig ICT- en internetgebruik en de privacy van leerlingen/studenten.

Om te controleren of de Faciliteiten niet worden gebruikt op een manier die in strijd is met de regels of geldende wetgeving en om te zorgen dat het netwerk, de apparatuur en de applicaties te allen tijde veilig zijn en niet overbelast worden, kan de Instelling het gebruik van de Faciliteiten monitoren op de manieren zoals beschreven in dit Reglement.

Omdat het Reglement voorziet in een verwerking van persoonsgegevens en/of controle op gedrag of prestaties van leerlingen/studenten, heeft voor het VO het medezeggenschapsorgaan en voor het mbo de studentenraad instemmingsrecht. Deze hebben op [DATUM] ingestemd met de inhoud van dit Reglement. Dit reglement vervangt eerdere reglementen op het gebied van verantwoord netwerkgebruik.

1. Gebruik van de Faciliteiten

De Faciliteiten worden aan de leerling/student beschikbaar gesteld ten behoeve van de studie, onder meer voor het kunnen maken van opdrachten, verslagen en scripties, het bijhouden van de studievoortgang, het raadplegen van bronnen en het communiceren met docenten, medeleerlingen/medestudenten.

Het gebruik van eigen apparatuur en toepassingen op de Faciliteiten van de Instelling is toegestaan, zolang dit gebruik voldoet aan de regels van dit Reglement. Het veranderen van instellingen in apparatuur en toepassingen beschikbaar gesteld door de Instelling is alleen toegestaan met aparte toestemming van de IT-afdeling. Het aansluiten van eigen netwerkapparatuur waarmee de verbinding kan worden gedeeld met derden op netwerkaansluitingen is te allen tijde verboden.

Dit Reglement geldt ook als je als gast gebruik maakt van netwerkvoorzieningen van andere instellingen, waarbij toegang wordt verkregen op basis van de inloggegevens van de eigen Instelling (bijvoorbeeld Eduroam).

Bepaalde Faciliteiten zijn alleen toegankelijk met behulp van een gebruikersnaam en een wachtwoord. Deze zijn persoonsgebonden en mogen niet met anderen worden gedeeld. IT-beheer kan nadere eisen stellen aan de kwaliteit van wachtwoorden en andere beveiligingsaspecten. Bij een

vermoeden van misbruik van een wachtwoord of ander authenticatiemiddel kan IT-beheer per direct het betreffende account ontoegankelijk maken.

1.1. Beveiliging door de Instelling en de leerling/student

De Instelling neemt informatiebeveiliging serieus. Zij hanteert dan ook 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.

De Instelling streeft naar een zo goed mogelijke beveiliging. Daarom verwacht de Instelling ook van leerlingen/studenten een proactieve houding en serieuze stappen om de eigen computer en andere apparatuur (zoals smartphones of tablets) adequaat te beveiligen. De leerling/student zijn te allen tijde zelf verantwoordelijk voor het gebruik van de eigen apparatuur en de op deze apparatuur opgeslagen gegevens.

In het bijzonder dient de leerling/student, indien met eigen apparatuur gebruik wordt gemaakt van een netwerkaansluiting van de Instelling, in het kader van beveiliging:

- deze apparatuur te voorzien van een adequate virusscanner en firewall;
- onrechtmatige toegang tot systemen van de Instelling te voorkomen door gebruik van sterke moeilijk te raden wachtwoorden en/of pincodes te gebruiken;
- deze apparatuur up-to-date te houden wat betreft software-instellingen (beveiligingsupdates);
- versleuteling (encryptie) toe te passen.

1.2. Privégebruik en overlast

Hoewel de Faciliteiten bedoeld zijn voor gebruik ten behoeve van de studie, is privégebruik in beperkte mate toegestaan. Gebruik (privé of ten behoeve van studie) mag niet illegaal of storend voor de goede orde bij de Instelling zijn en mag geen overlast veroorzaken bij anderen, inbreuk maken op rechten van de Instelling of derden of de integriteit en de veiligheid van het netwerk aantasten.

Onder illegaal, storend en/of overlast veroorzakend gebruik wordt in ieder geval verstaan:

- het in openbare ruimtes raadplegen van internetdiensten met een pornografische, racistische, discriminerende, bedreigende, 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 blijk geven van of (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 Netflix) te gebruiken wanneer dit overmatig veel dataverkeer genereert, zodanig dat het de beschikbaarheid van de Faciliteiten kan aantasten;
- films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van enige illegale bron of wanneer de leerling/student 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.

Leerlingen/studenten die in hun woonruimte gebruik maken van een netwerkfaciliteit van de Instelling worden geen beperkingen opgelegd aan het gebruik, behalve als het noodzakelijk is om de integriteit en de veiligheid van het netwerk te kunnen bewaren, of om de gevolgen van vertragingen te beperken. Als de Instelling ingrijpt om de gevolgen van vertragingen te beperken, zullen gelijke soorten verkeer gelijk worden behandeld. De overige bepalingen in dit Reglement zijn onverkort van toepassing voor leerlingen/studenten die in hun woonruimte gebruik maken van een netwerkfaciliteit van de Instelling.

Het gebruik van de Faciliteiten ten behoeve van eigen commerciële activiteiten is uitsluitend toegestaan, wanneer de Instelling hiervoor schriftelijk toestemming heeft verleend.

1.3. Vertrouwelijkheid en de intellectuele eigendomsrechten

De leerling/student maakt geen inbreuk op de intellectuele eigendomsrechten van de Instelling en derden en respecteren de licentie afspraken zoals die van toepassing zijn binnen de Instelling.

De zeggenschap over de informatie van de Instelling berust bij Instelling. De leerling/student heeft geen zelfstandige zeggenschap over de informatie behalve als hem/haar dat expliciet is toegekend door de Instelling.

Het is de leerling/student niet toegestaan om grote hoeveelheden artikelen uit de bestanden van de digitale bibliotheek te downloaden of substantiële delen van de bestanden of databases in de digitale bibliotheek systematisch te kopiëren.

Indien de leerling/student in het kader van zijn studie of het uitvoeren van taken voor de Instelling toegang krijgt tot vertrouwelijke informatie of privacygevoelige informatie, dient de leerling/student die informatie strikt vertrouwelijk te behandelen.

De leerling/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 de Instelling noodzakelijk is zoals via e-mail, in niet instellingsgebonden cloud-toepassingen, op externe opslagmedia of eigen apparatuur (USB-gegevensdragers, tablets, etc.).

Indien de Instelling met betrekking tot het waarborgen van de vertrouwelijkheid en de intellectuele eigendomsrechten nadere voorschriften heeft opgesteld, dient de leerling/student deze stipt op te volgen.

2. Controle door de Instelling

De Instelling controleert de naleving van dit Reglement. De Instelling handelt bij de controle op het gebruik van de Faciliteiten binnen de geldende wet- en regelgeving.

De Instelling streeft in het kader van de controle en handhaving van dit Reglement naar maatregelen, die inzage in privacygevoelige informatie of persoonsgegevens van individuele leerlingen/studenten zo veel mogelijk beperken. De Instelling zal daarbij uitgaan van de juiste balans tussen verantwoord gebruik van de Faciliteiten en de bescherming van de privacy van leerlingen/studenten. Zij zal, waar

mogelijk, slechts geautomatiseerd controleren of filteren, zonder daarbij zichzelf of andere personen inzage te geven in gedrag van individuele personen.

2.1. Voorwaarden voor controle

Controle van gebruik van de Faciliteiten vindt slechts plaats in het kader van handhaving van de regels uit dit Reglement ten behoeve van de goede orde binnen de Instelling, de bewaking van de integriteit en de veiligheid van de Faciliteiten van de Instelling. Verboden gebruik van de Faciliteiten wordt zo veel mogelijk langs technische weg onmogelijk gemaakt.

Ten behoeve van deze controle worden geautomatiseerd gegevens verzameld (gelogd). Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens, die niet herleidbaar zijn tot identificeerbare personen. De gegevens, die uit een dergelijke controle voortkomen, zijn alleen toegankelijk voor de direct verantwoordelijke IT-beheerders 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 leerlingen/studenten, worden overgegaan tot blokkering van de toegang tot de beschikbaar gestelde faciliteiten. Indien mogelijk wordt de leerling/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 men zo snel mogelijk melding van de maatregel.

Bij vermoedens van overtreding van de regels kan gedurende een vastgestelde (korte) periode, gerichte 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. De procedure bij gericht onderzoek, wordt hieronder in hoofdstuk 2.3. beschreven.

De Instelling houdt zich bij het controleren op het niveau van verkeersgegevens of de inhoud onverkort aan de Algemene verordening gegevensbescherming (AVG) en andere relevante wet- en regelgeving. In het bijzonder beveiligt de Instelling de bij controle vastgelegde gegevens tegen ongeautoriseerde toegang en zijn personen met toegang daartoe contractueel verplicht tot geheimhouding.

Persoonsgegevens, die zijn vastgelegd in het kader van toezicht en controle, worden bewaard voor een zo kort mogelijke periode. Enkel indien er een redelijk vermoeden bestaat van onrechtmatig gebruik kan deze periode worden verlengd. Zodra een onderzoek is afgerond en niet leidt tot maatregelen tegenover een betrokkene, worden de gegevens verwijderd.

2.2. Uitvoering van de controle

Om controle uit te kunnen voeren op de naleving van dit Reglement, kan de Instelling enkele specifieke maatregelen treffen. Zo vindt de controle op het uitlekken van vertrouwelijke informatie, waartoe de leerling/student in het kader van zijn studie of het uitvoeren van taken voor de Instelling toegang heeft, plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek.

Daarnaast wordt de controle in het kader van kosten- en capaciteitsbeheersing beperkt tot het op basis van verkeersgegevens nagaan van de bronnen van kosten of capaciteitsvraag (zoals de adressen van internetradio en videosites). Als deze websites tot grote kosten of overlast leiden, worden zij geblokkeerd of afgeknepen, zonder daarbij de vertrouwelijkheid van de inhoud van de communicatie te schenden;

De beheerders van de IT-afdeling zijn gebonden aan geheimhouding als men in het kader van de controle op dit Reglement om technische redenen kennis moet nemen van persoonsgebonden informatie, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

Door de Instelling worden in het kader van de controle op dit Reglement de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij verwerkt worden, juist en nauwkeurig zijn.

Door de Instelling worden in het kader van de controle op dit Reglement passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

2.3. Procedure bij gericht onderzoek

Van gericht onderzoek is sprake wanneer verkeersgegevens of andere persoonsgegevens betreffende de leerling/student worden vastgelegd in het kader van een onderzoek naar aanleiding van een zwaarwegend vermoeden van een overtreding van dit Reglement door die leerling/student.

Gericht onderzoek vindt uitsluitend plaats na schriftelijke opdracht van de directeur van de desbetreffende school, welke toestemming de redenen zal noemen waarom deze wordt verleend. Het bestuur ontvangt een afschrift van deze opdracht en een vastlegging 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 de Instelling na aparte toestemming overgaan tot het kennismaken van de inhoud van communicatie of opgeslagen bestanden. Indien het onderzoek geen aanleiding geeft tot verdere maatregelen wordt de vastlegging vernietigd.

Gericht onderzoek naar de beveiliging of integriteit van randapparatuur mag in afwijking hiervan door IT-beheer worden uitgevoerd op basis van concrete aanwijzingen, zonder aparte toestemming. De resultaten van dit onderzoek worden alleen gedeeld met de leerling/student met het doel de beveiliging of integriteit van de randapparatuur te verbeteren. Bij herhaling zal de procedure uit het vorige lid worden gevolgd.

De leerling/student wordt zo spoedig mogelijk schriftelijk geïnformeerd door de directeur over de aanleiding, de uitvoering en het resultaat van het onderzoek. De leerling/student 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.

De IT-beheerders verschaffen zich slechts toegang tot accounts of computers van de leerling/student als de leerling/student daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan in dringende gevallen of bij een duidelijk vermoeden van schending van dit Reglement, zoals nader bepaald in dit artikel. De leerling/student zal in dat geval achteraf worden geïnformeerd.

3. Consequenties van overtreding van dit Reglement

Bij handelen in strijd met dit Reglement of de algemeen geldende wetgeving bij het gebruik van de Faciliteiten, kan het bestuur van de Instelling, 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 leerling/student.

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 leerling/student gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

In afwijking van het voorgaande is het mogelijk dat de Instelling 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 IT-beheer is weggenomen. Indien na een week geen verbetering is geconstateerd door IT-beheer, kan IT-beheer besluiten tot een langere blokkade. Bij herhaling van de oorzaak kunnen disciplinaire maatregelen worden genomen.

De Instelling is te allen tijde gerechtigd om aangifte te doen van geconstateerde strafbare feiten.

4. Rechten van de leerling/student met betrekking tot persoonsgegevens

De leerling/student kan zich tot het bestuur wenden met het verzoek om een volledig overzicht van zijn persoonsgegevens, zoals door de Instelling verwerkt in het kader van dit Reglement.

De leerling/student kan het bestuur verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen, indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend zijn, dan wel het verwerken ervan in strijd met een wettelijk voorschrift is.

De leerling/student kan verder bezwaar maken tegen de verwerking van zijn persoonsgegevens, indien sprake is van bijzondere persoonlijke omstandigheden. In dat geval zal de verwerking gestopt, dan wel worden beperkt, tenzij sprake is van dwingende gerechtvaardigde belangen, die zwaarder wegen dan de rechten en vrijheden van de leerling/student.

De leerling/student heeft in sommige gevallen het recht om het verwerken van zijn persoonsgegevens (al dan niet tijdelijk) te beperken. De leerling/student kan de verwerking van zijn persoonsgegevens beperken, indien de gegevens mogelijk onjuist zijn, de verwerking onrechtmatig is, de gegevens niet meer nodig zijn, dan wel de leerling/student bezwaar tegen de verwerking heeft ingediend.

De leerling/student kan het bestuur verzoeken zijn persoonsgegevens te verwijderen indien deze niet meer nodig zijn, hij eerder toestemming heeft gegeven voor het gebruik van zijn gegevens maar deze toestemming nu intrekt, hij bezwaar gemaakt heeft tegen de verwerking, de verwerking onrechtmatig is, dan wel de wettelijk bepaalde bewaartermijn verlopen is.

Indien dit technisch mogelijk is, heeft de leerling/student tevens het recht om de persoonsgegevens, die de Instelling in het kader van dit Reglement van hem verwerkt, te laten overdragen naar een derde partij.

De leerling/student heeft daarnaast het recht op een menselijke blik bij besluiten op basis van automatisch verwerkte gegevens.

Op bovengenoemde verzoeken wordt binnen vier weken gereageerd. Deze termijn kan echter om twee maanden worden verlengd om redenen die verband houden met de specifieke privacyrechten of de complexiteit van het verzoek. Van een dergelijke verlenging van de termijn zal het bestuur de leerling/student binnen vier weken op de hoogte stellen. Een weigering is met redenen omkleed. Een toegewezen verzoek zal zo spoedig mogelijk worden uitgevoerd.

5. Slotbepalingen

Dit Reglement kan door het bestuur worden herzien. Wijzigingen worden alleen bij het begin van een collegejaar doorgevoerd, behalve in dringende gevallen of wanneer de Instelling door omstandigheden van buitenaf gedwongen is tot een snellere invoering.

Wijzigingen worden alleen ingevoerd nadat de instellingsmedezeggenschapsraad om voorafgaand advies is gevraagd. Het bestuur zal feedback van leerlingen/studenten in overweging nemen alvorens de wijzigingen in te voeren.

In gevallen waarin dit Reglement niet voorziet, beslist het bestuur.