



COG

Netwerkdiensten

Inhoudsopgave

Inleiding.....	3
Doel.....	3
Toepassingsgebied.....	3
Hiërarchie.....	3
1. Veiligheid en Privacy.....	4
1.1 Wachtwoordbeveiliging.....	4
1.2 Gegevensbescherming.....	4
1.3 Sociale Media.....	4
2. Toegestaan en Ongeoorloofd Gebruik.....	4
2.1 Toegestaan gebruik.....	4
2.2 Ongeoorloofd gebruik.....	4
3. Beveiligingsmaatregelen.....	5
3.1 Antivirus en Updates.....	5
3.2 Netwerkmonitoring.....	5
4. Sancties.....	5
Goedkeuring en Herziening.....	5

Inleiding

Voor het leerproces en de dagelijkse werkzaamheden binnen COG is toegang tot het internet en het gebruik van digitale middelen essentieel voor het leerproces en de dagelijkse werkzaamheden. Om een veilige en goed werkbare omgeving te garanderen, is het belangrijk dat er verantwoord wordt omgegaan met deze netwerkdiensten. Dit beleidsstuk biedt richtlijnen en regels voor het gebruik hiervan binnen onze onderwijsorganisatie.

Doel

Het doel van dit beleidsstuk is om een kader te bieden voor verantwoord en ethisch gebruik van het internet en het netwerk, en om misbruik en ongeoorloofde activiteiten te voorkomen. Dit draagt bij aan een veilige en respectvolle leer- en werkomgeving voor iedereen.

Toepassingsgebied

Dit beleid geldt voor iedereen die gebruik maakt van de netwerkdiensten die door COG (en de bijbehorende onderwijsinstellingen) ter beschikking worden gesteld.

Naast studenten, leerlingen en medewerkers van COG geldt dit beleid ook voor externen (bijvoorbeeld gedetacheerden en stagiaires), zowel op de onderwijslocaties als op externe locaties waar onze netwerkdiensten worden gebruikt.

Hiërarchie

- Dit document is een ondersteunend beleidsdocument van het IBP beleid van COG;
- Voor het gebruik van de netwerkdiensten gelden ook de omgangsnormen zoals opgenomen in de Omgangscode;
- Indien er gebruik wordt gemaakt van door COG verstrekte IT-middelen om connectie te maken met de netwerkdiensten, dan gelden ook de bepalingen in de toepasselijke bruikleenovereenkomsten.

In gevallen waarin dit beleid niet voorziet, beslist het College van Bestuur.

1. Veiligheid en Privacy

1.1 Wachtwoordbeveiliging

Gebruikers zijn verantwoordelijk voor het beschermen van hun wachtwoorden en inloggegevens. Wachtwoorden moeten regelmatig worden gewijzigd en nooit worden gedeeld. De wachtwoorden moeten voldoen aan de gestelde beleidsvoorwaarden (zie [20240701_Wachtwoordbeleid_def_v1.0.pdf](#)).

1.2 Gegevensbescherming

Het verwerken van persoonlijke gegevens mag alleen als aan de Algemene Verordening Gegevensbescherming (AVG) wordt voldaan en gebruik wordt gemaakt van extra beveiligingsmaatregelen als het gaat om gevoelige informatie. Zie voor nadere voorwaarden en richtlijnen ook [COG-IBP - Introductiepagina \(sharepoint.com\)](#).

1.3 Sociale Media

Het gebruik van Sociale Media op persoonlijke titel is toegestaan, zolang er voldaan wordt aan de regels van respect en privacy, zodat het geen (imago)schade toebrengt aan personen en instellingen. Zie hiervoor ook de richtlijnen in de Omgangscode ([Omgangscode COG.pdf](#)). Daar waar via Sociale Media uit naam van COG wordt gecommuniceerd, moet er aparte toestemming zijn vanuit de instelling (lees: afdeling Marketing & Communicatie).

2. Toegestaan en Ongeoorloofd Gebruik

2.1 Toegestaan gebruik

De netwerkdiensten mogen alleen worden gebruikt voor legitieme onderwijs- en werkgerelateerde activiteiten. Persoonlijk gebruik is in beperkte mate toegestaan zolang het de onderwijs- en werkgerelateerde activiteiten niet verstoort en binnen deze Gedragscode past.

2.2 Ongeoorloofd gebruik

Het is verboden om illegale activiteiten uit te voeren, zoals het downloaden of verspreiden van illegale software, auteursrechtelijk beschermd materiaal zonder toestemming, of het deelnemen aan cybercriminaliteit.

3. Beveiligingsmaatregelen

3.1 Antivirus en Updates

Alle apparaten die verbinding maken met onze netwerkdiensten moeten up-to-date antivirussoftware hebben en regelmatig beveiligingsupdates uitvoeren.

3.2 Netwerkmonitoring

Onze netwerkdiensten wordt actief gemonitord om beveiligingsbedreigingen en ongeoorloofd gebruik op te sporen. Gebruikers worden geacht hieraan mee te werken en verdachte activiteiten direct te melden.

4. Sancties

Misbruik door leerlingen en studenten kan leiden tot tijdelijke of permanente ontzegging van toegang tot de netwerkdiensten. Bij misbruik door medewerkers behoudt COG zich het recht voor, afhankelijk van de aard en ernst van de overtreding, frequentie en de omstandigheden van het geval, rechtspositionele maatregelen te nemen en maatregelen zoals bedoeld in de cao-vo en cao-mbo.

Goedkeuring en Herziening

Dit beleidsstuk is goedgekeurd door het College van Bestuur op 1 april 2025. Het beleid wordt jaarlijks geëvalueerd en aangepast waar nodig om relevant en effectief te blijven.