
# Gedragscode verantwoord gebruik van ICT-faciliteiten

## voor medewerkers

Vereniging voor Christelijk Voortgezet Onderwijs te Rotterdam en omgeving

## Inhoudsopgave

# 1. Inleiding

De ICT-faciliteiten van de vereniging CVO Rotterdam en omgeving, spelen een zeer belangrijke rol in het dagelijks werk van de CVO-medewerkers. Onder ICT-faciliteiten worden in ieder geval verstaan:

- Hardware: computer, laptop, tablet, smartphone, printpas en servers/systemen.
- Software: alle applicaties voor het uitvoeren van de dagelijkse werkzaamheden, zoals e-mail, Microsoft 365 en Somtoday.
- CVO-accounts.

De afhankelijkheid van de ICT-faciliteiten is groot. Naar verwachting gaat de rol van ICT-faciliteiten, en de afhankelijkheid daarvan, in de toekomst nog verder toenemen. Daarnaast bevatten deze ICT-faciliteiten in toenemende mate belangrijke, vertrouwelijke en/of persoonsgegevens. Vertrouwelijke gegevens zijn privé, geheim en/of gevoelig. Persoonsgegevens zijn gegevens waarmee medewerkers direct of indirect geïdentificeerd kunnen worden, zoals adresgegevens, telefoonnummers, personeelsdossiers en foto’s.

Het is van belang dat alle medewerkers binnen CVO weten wat hun verantwoordelijkheden bij het gebruik van de ICT-faciliteiten zijn en wat ze kunnen doen om de organisatie en haar gegevens veilig te houden. In het cybersecuritybeleid van CVO worden de taken en verantwoordelijkheden van medewerkers beschreven. Deze medewerkersgedragscode is een belangrijk onderdeel van het cybersecuritybeleid en beschrijft de normen met betrekking tot het gebruik van ICT-faciliteiten, wat deze betekenen voor medewerkers in hun dagelijkse werk en wat er van hen verwacht wordt omtrent het omgaan met vertrouwelijke informatie.

De gedragscode is van toepassing op het gebruik van de ICT-faciliteiten van CVO en geldt voor alle CVO-medewerkers, met inbegrip van externe inhuurkrachten, uitzendkrachten, vrijwilligers én stagiaires (hierna: medewerkers). Het gebruik van deze ICT-faciliteiten is voor alle medewerkers noodzakelijk om de eigen werkzaamheden goed te kunnen verrichten. Aan het gebruik van ICT-faciliteiten zijn risico’s verbonden, zoals beschadiging van het netwerk door virussen, besmetting van systemen met schadelijke software, het openbaar worden (lekken) van bedrijfsgeheimen/-gegevens, de schending van privacyregels en het in gevaar brengen van de goede naam van CVO. Van medewerkers van CVO wordt verwacht dat zij verantwoord en integer omgaan met de aan hen beschikbaar gestelde ICT-faciliteiten en informatie om te voorkomen dat de eerder aangegeven risico's zich voordoen.

Het gebruik van de door CVO beschikbaar gestelde ICT-faciliteiten is persoonlijk en van de medewerker wordt verwacht dat hier verantwoord mee om wordt gegaan. Deze gedragscode beschrijft hoe medewerkers verantwoord om dienen te gaan met ICT-faciliteiten als onderdeel van het CVO-beleid op het gebied van cyberweerbaarheid.

# 2. Algemene normen

In deze gedragscode staat beschreven wat de algemene normen zijn rondom het gebruik van ICT-faciliteiten, wat dit voor CVO-medewerkers in de dagelijkse praktijk betekent en hoe verwacht wordt dat medewerkers omgaan met (vertrouwelijke) informatie.

## 2.1 Gebruik van ICT-faciliteiten

Voor het verrichten van de werkzaamheden worden ICT-faciliteiten ter beschikking gesteld voor zakelijk gebruik. Hiervoor gelden de volgende regels:

- Zorg dat (persoons)gegevens niet toegankelijk zijn voor onbevoegden.
- Weet welke gegevens mogen worden gebruikt (mag iedereen het zien?) en welke ICT-faciliteiten kunnen worden ingezet (is het veilig genoeg?) bij het verrichten van de eigen werkzaamheden.
- Beperkt privégebruik van ICT-faciliteiten is toegestaan indien dit in geen geval storend is en niet ten koste gaat van het uitvoeren van de werkzaamheden en het naar behoren functioneren van de medewerker.
- Standaard software wordt alleen door de afdeling ICT van de CVO Shared Service Organisatie (SSO) geïnstalleerd. Het installeren van niet-standaard software is nimmer toegestaan.
- Sla (persoons)gegevens alleen op de daarvoor aangewezen systemen op. Hieronder wordt de Cloud-omgeving van Microsoft 365 (SharePoint, OneDrive en Teams) verstaan. Opslaan van gegevens in publieke Cloud-omgevingen, zoals een persoonlijke Dropbox of Google Drive, is nimmer toegestaan.
- Meld storingen van beheerde werkplekken (computer of laptop) altijd bij de ICT Servicedesk van CVO SSO.
- Meld diefstal of verlies van ICT-faciliteiten, én eigen apparatuur waarop werkzaamheden voor CVO zijn verricht (‘bring your own device’) onmiddellijk na constatering bij de ICT Servicedesk van CVO SSO.

## 2.2 Clear desk / clear screen regels

Voorkom dat anderen (onbedoeld) toegang kunnen krijgen tot gegevens via ICT-faciliteiten waartoe zij geen rechten hebben. Ga zorgvuldig met gegevens om en laat gegevens niet (onbedoeld) onbeheerd. Aanvullend gelden voor de werkplek de volgende clear desk en clear screen regels:

- Vergrendel bij het tijdelijk verlaten van de werkplek altijd de computer of laptop (ook op je BYOD-apparaat) (Windows: ‘Windowstoets + L’).
- Zorg dat wanneer je je werkplek verlaat, alle (vertrouwelijke) documenten en ICT-faciliteiten op een veilige plaats zijn opgeborgen (zoals in een kast die op slot kan of in een kluisje). Je computer is afgesloten of uitgelogd. Zorg dat kasten met vertrouwelijke documenten en ICT-apparatuur aan het einde van de werkdag op slot zitten.
- Voorkom dat gevoelige en vertrouwelijke informatie zichtbaar is wanneer iemand anders op het beeldscherm (of via bijvoorbeeld een beamer) mee kan kijken.
- Documenten met gevoelige (persoons)gegevens mogen niet onbewaakt worden achtergelaten. Laat bijvoorbeeld vertrouwelijke documenten niet rondslingeren op je bureau of bij de printer.
- Gooi overbodig geworden documenten met persoonsgegevens erop altijd in de hiervoor speciaal bestemde container of papierversnipperaar.

LET OP: Als persoonsgegevens toegankelijk en/of inzichtelijk zijn voor personen die geen toegang behoren te hebben tot die gegevens, is dit een beveiligingsincident waaruit mogelijk een datalek kan voortkomen. Van alle medewerkers wordt verwacht dat zij (mogelijke) datalekken onmiddellijk na constatering melden via datalek@cvo.nl.

# 3. Gebruik CVO-apparatuur

CVO kan ter ondersteuning van de uitoefening van de functie en/of werkzaamheden (tijdelijk of voor langere tijd) bepaalde hardware (apparatuur) aan haar medewerkers in bruikleen geven. Onder CVO-apparatuur voor bruikleen wordt onder andere verstaan: laptop, tablet, smartphone, (web)camera en beeldscherm.
De aan de medewerkers uitgeleende apparatuur mag door de medewerker uitsluitend ter uitoefening van zijn/haar functie/werkzaamheden bij CVO en in overeenstemming met de bestemming worden gebruikt. De medewerker tekent voor het in ontvangst nemen van de apparatuur een bruikleenovereenkomst. Bij het ondertekenen van de bruikleenovereenkomst verklaart de medewerker de apparatuur in goede orde te hebben ontvangen en goed voor de apparatuur te zorgen.

Voor gebruik van CVO-apparatuur gelden de volgende regels:

- De medewerker zal goed voor de CVO-apparatuur zorgen; dit houdt in dat de medewerker zijn/haar gedrag afstemt op wat in redelijkheid verwacht kan worden op basis van gezond verstand, fatsoen, zorgvuldigheid, algemene kennis, hygiëne. specifieke instructies, enz.
- Beperkt privégebruik van CVO-apparatuur is toegestaan, indien dit in geen geval storend is en niet ten koste gaat van het uitvoeren van de werkzaamheden en het naar behoren functioneren van de medewerker.
- Het is niet toegestaan om de CVO-apparatuur te gebruiken voor nevenactiviteiten of commerciële doeleinden buiten CVO.
- Het is niet toegestaan om de apparatuur door derden te laten gebruiken.
- Bij het uitvoeren van werkzaamheden ten behoeve van CVO, mag geen gebruik worden gemaakt van computerprogrammatuur die niet door CVO ter beschikking is gesteld.
- Het is niet toegestaan om eventuele bij de apparatuur behorende of daarop aanwezig zijnde computerprogrammatuur, gegevensbestanden, of documentatie te kopiëren of te verveelvoudigen dan wel te versturen en/of derden daartoe toegang te geven.
- De CVO-apparatuur dient regelmatig op de CVO-netwerkvoorziening te worden aangesloten, zodat noodzakelijke updates automatisch kunnen worden geïnstalleerd. Bij voorkeur en daar waar mogelijk 1 keer per maand.
- Bij het beëindigen van de bruikleenovereenkomst dient de apparatuur in goede staat bij CVO te worden teruggegeven.
- CVO is nimmer verantwoordelijk noch verantwoordelijk te stellen voor het verlies van eventuele privégegevens die op een CVO-apparaat zijn opgeslagen.

De regels zijn ook van toepassing voor medewerker die elders dan de CVO-locaties (bv. thuis) op CVO-apparatuur (werklaptop) werkzaamheden uitvoeren.

# 4. Gebruik eigen apparatuur (BYOD)

Naast de ICT-faciliteiten die CVO voor haar medewerkers beschikbaar stelt, is het ook mogelijk om eigen apparatuur te gebruiken om werkzaamheden voor CVO te verrichten. Ook voor het gebruik van eigen apparatuur, ook wel ‘bring your own device’ (BYOD) genoemd, gelden regels. Deze regels hebben zowel betrekking op het gebruik als op de beveiligingsmaatregelen in geval met eigen apparatuur (waaronder laptops, pc’s, tablets en smartphones) werkzaamheden voor CVO worden uitgevoerd.
CVO is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de ICT-faciliteiten, ongeacht of het gaat om CVO-apparatuur of BYOD-apparatuur. Bij BYOD-apparaten moet CVO een vergelijkbaar beveiligingsniveau als voor eigen CVO-apparatuur kunnen garanderen. Daarom stelt CVO eisen aan deze BOYD-apparatuur. De afdeling ICT van de SSO moet kunnen verifiëren dat een BYOD-apparaat aan deze eisen voldoet.

De BYOD-apparatuur dient te voldoen aan de volgende eisen:

- Op het BYOD-apparaat moet een Mobile Device Management (MDM) applicatie geïnstalleerd kunnen worden die wordt beheerd door CVO en minimaal de volgende functionaliteiten biedt:
    - vereisten voor een wachtwoord;
    - vereisten voor gegevens encryptie, die in lijn zijn met het encryptiebeleid van CVO;
    - voorkomen van het opslaan van gegevens van CVO op persoonlijke opslaglocaties;
    - isoleren van persoonlijke gegevens van CVO-gegevens op het BYOD-apparaat;
    - beperken van de acties die de gebruiker kan ondernemen met gegevens van CVO, zoals kopiëren, knippen en plakken, screenshots, opslaan en weergeven;
    - op afstand blokkeren en wissen van CVO-gegevens op gestolen apparatuur;
    - blokkeren van toegang tot CVO-gegevens via verouderde en kwetsbare systemen;
    - detecteren van niet-ondersteunde besturingssystemen.
- Voor BYOD-apparaten evalueert CVO periodiek welk versienummer van het besturingssysteem minimaal moet worden gebruikt. BYOD-apparatuur moet altijd zijn voorzien van de meest recente software updates.
- Vergrendel het BYOD-apparaat bij het verlaten van de werkplek.
- BYOD-apparaten moeten voorzien zijn van adequate en up-to-date virusscanners.
- Op BYOD-apparaten mag geen illegale software of games worden gedownload.
- Op BYOD-apparaten mag geen software worden gebruikt die (persoons)gegevens verwerken, zonder een verwerkersovereenkomst.
- In het geval een BYOD-device door niet naleven van deze eisen het CVO-netwerk infecteert met een virus of malware, kan de medewerker hiervoor aansprakelijk worden gehouden.

# 5. Gebruik CVO-account en e-mail

CVO stelt een account en e-mailfaciliteit aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden.

## 5.1 Gebruik CVO-account

Voor het gebruik van het CVO-account gelden de volgende regels:

- Het CVO-account is een persoonlijk account. Deel daarom inloggegevens nooit met een ander, ook niet met collega's, familie- of gezinsleden of kennissen.
- Medewerkers verkrijgen toegang tot het CVO-account via multi-factor authenticatie (MFA). Dit betekent dat medewerkers naast een gebruikersnaam en wachtwoord de inlog moeten bevestigen door middel van een Authenticator-app.
- Installeer en activeer deze Authenticator-app op slechts één apparaat.
- Schrijf je inloggegevens nergens op en deel ze nooit via e-mails, berichtendiensten of sociale media.
- Wil je toch ergens je wachtwoord vastleggen, doe dit dan op een veilige manier. Hierbij kun je bijvoorbeeld gebruik maken van een passwordmanagement tool (bijvoorbeeld: Keepass of Bitwarden).

## 5.2 Gebruik e-mail

Voor het gebruik van e-mail gelden de volgende regels:

- Gebruik je werk e-mailadres alleen voor werkgerelateerde zaken.
- Het is niet toegestaan e-mail te gebruiken voor berichten met pornografische, racistische, discriminerende, beledigende, (seksueel) intimiderende of aanstootgevende inhoud of voor berichten die kunnen aanzetten tot haat, discriminatie en/of geweld.
- Het is uitsluitend toegestaan om de zakelijke mailbox met een persoonlijk device te synchroniseren als wordt voldaan aan de eisen voor BYOD-apparaten zoals beschreven in hoofdstuk 4.

# 6. Gebruik internet en sociale media

CVO stelt het gebruik van internet en de bijbehorende faciliteiten aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Zie hiervoor het reglement "gebruik internet en social media CVO"

# 7. Gebruik AI

CVO stelt dat AI een levend onderwerp is met veel mogelijkheden, maar ook met mogelijke risico's. Op een later moment zal hier beleid voor worden opgesteld.

# 8. Naleving

Het gebruik van ICT-faciliteiten wordt vastgelegd (gelogd). Deze registratie geschiedt om de continuïteit en bedrijfszekerheid van de technische infrastructuur te kunnen waarborgen, verstoring van bedrijfsprocessen en andere schade tegen te kunnen gaan en om toezicht te kunnen houden op de naleving van dit reglement.

In zijn algemeenheid geldt dat veel medewerkers gebruik maken van de diverse systemen binnen CVO om hun werk te kunnen doen. Het is mogelijk om op individueel niveau de betreffende activiteiten (al dan niet steekproefsgewijs) te monitoren. De activiteiten worden echter niet geanalyseerd als daar geen noodzaak voor is. Medewerkers worden hierop qua gedrag dus ook niet beoordeeld of aangesproken. Mocht het op enig moment noodzakelijk zijn om het computergebruik (of telefoon-/internetverkeer waaronder sociale media-uitingen) van een medewerker te controleren, dan gebeurt dit op basis van een gerechtvaardigd belang en slechts met toestemming van de algemene directie van de scholengroep, directie van de SSO of de raad van bestuur. Hierbij wordt rekening gehouden met het recht op vertrouwelijke communicatie van medewerkers.

De controle op het gebruik van ICT-faciliteiten (waaronder het gebruik van internet en sociale media) is een verwerking van persoonsgegevens in de zin van de privacywetgeving. CVO zal dan ook de controle en handhaving van deze gedragscode conform de privacywetgeving en het algemene arbeidsrechtelijk kader uitvoeren. We zorgen daarmee voor een goede balans tussen het verantwoord gebruik van ICT-faciliteiten en de bescherming van de privacy van medewerkers.
Een medewerker is alleen aansprakelijk voor schade, als de schade een gevolg is van opzet, bewuste roekeloosheid of nalatigheid. Bovendien moet sprake zijn van schade die binnen de uitvoering van het arbeidscontract valt. Schade veroorzaakt door activiteiten buiten het bereik van het arbeidscontract vallen binnen de risicosfeer van de medewerker.

## 8.1 Voorwaarden voor controle

- Controle van persoonsgegevens met betrekking tot gebruik van ICT-faciliteiten vindt slechts plaats in het kader van handhaving van deze gedragscode.
- Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen.
- Controle beperkt zich in beginsel tot verkeersgegevens[1] van de ICT-faciliteiten. Slechts bij zwaarwegende redenen vindt controle op de inhoud plaats na besluit van de Functionaris Gegevensbescherming (FG) samen met de Raad van Bestuur (RvB).
- Verboden e-mail- en internetgebruik wordt zo veel mogelijk door het aanbrengen van blokkades, softwarematig onmogelijk gemaakt.
- Indien een medewerker, of een groep medewerkers, wordt verdacht van het overtreden van regels in deze gedragscode, kan gedurende een vastgestelde (korte) periode een gerichte controle op het gebruik van de ICT-faciliteiten waarop deze gedragscode betrekking heeft plaatsvinden.
- Bij constatering van ongeoorloofd gebruik van ICT-faciliteiten wordt dit onmiddellijk met de betrokken medewerker besproken. CVO zal de medewerker op verzoek inzage verschaffen in de gegevens over het ongeoorloofd gebruik. De medewerker wordt gewezen op de consequenties wanneer niet wordt gestopt met het ongeoorloofd gebruik.
- Een ICT-medewerker kan meekijken op apparatuur van medewerkers door middel van ‘meekijksoftware’. De ICT-medewerker kijkt alleen mee zover dit nodig is om ICT-problemen te verhelpen.

Medewerkers die zich niet aan deze gedragscode houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken. Zij krijgen daarbij inzage in de over hen vastgelegde gegevens en hebben de gelegenheid

[1] Gegevens over gedrag van medewerkers met betrekking tot het gebruik van digitale ICT-faciliteiten, die niet de details van de berichten of bestanden zelf betreffen (bijvoorbeeld: tijd, hoeveelheid, omvang etc.).

te reageren op het geconstateerde. Medewerker en leidinggevende maken dan afspraken voor de toekomst en bepalen de mogelijke maatregelen bij overtreding daarvan.

## 8.2 Sancties en maatregelen

Bij het handelen in strijd met deze gedragscode of enige andere algemeen geldende norm gericht op het belang dat onderwerp is van deze Gedragscode, kan de Raad van Bestuur of namens hem de Algemene Directie van de scholengroep, afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen. Hieronder vallen onder andere een waarschuwing/berisping, financiële sanctie, overplaatsing, schorsing en/of beëindiging van de arbeidsovereenkomst. In geval van een vermoeden van een strafbaar feit, zal altijd aangifte worden gedaan bij de politie.

## 8.3 Vragen of klachten

Vragen over deze Gedragscode? Neem dan contact op met de ICT Servicedesk van CVO SSO.

Ben je het niet eens met een wegens niet naleving van deze Gedragscode opgelegde disciplinaire maatregel of sanctie? Dan kun je een beroep indienen bij de Commissie van Beroep Funderend Onderwijs. Zie de CVO Klachtenregeling en www.onderwijsgeschillen.nl voor meer informatie.