Gedragscode gebruik internet en devices OVO Zaanstad

OPENBAAR VOORTGEZET ONDERWIJS ZAANSTAD

Opsteller: Raymondo Boerkamp
Expertise: Informatiemanager
Besluitvorming:
GMR ter instemming op 13 mei 2024
Vastgesteld door College van Bestuur op 28 mei 2024
Revisie 2026

Doel van de gedragscode

Deze gedragscode omschrijft de regels voor het gebruik van internet, e-mail, intranet en sociale media (hierna tezamen “internet”) op de scholen van OVO Zaanstad. Daarnaast omschrijft de gedragscode regels voor het gebruiken van middelen die OVO Zaanstad aan medewerkers ter beschikking stelt (hierna tezamen “devices”) De volgende punten zijn overwogen bij het vaststellen van deze gedragscode:

1. Gebruik van het internet is voor velen binnen OVO Zaanstad nodig om hun werk goed te doen of hun opleiding te volgen, maar onjuist hiermee omgaan kost tijd en capaciteit van mensen en apparatuur en brengt diverse risico’s met zich mee.
2. Internet kent verschillende verschijningsvormen. Aan het gebruik van internet zijn risico's verbonden die nopen tot het stellen van gedrags- en gebruiksregels. Bij risico's valt te denken aan beschadiging van het netwerk door virussen, het uitlekken van vertrouwelijke informatie en het in diskrediet brengen van (de goede naam van) personen en de organisatie.
3. Ook aan het gebruik van devices en de applicaties die daarop geïnstalleerd zijn zijn risico’s verbonden. Denk aan verlies, diefstal of beschadiging. Dat geldt voor zowel het fysieke object als de data die op het fysieke object aanwezig zijn, of accounts die daarvoor gebruikt worden. Daarnaast worden gegevens van OVO Zaanstad ook op devices die in privébezit zijn gebruikt.
4. Ter vermijding van dergelijke risico's kan OVO Zaanstad voorschriften geven voor het verrichten van de arbeid en maatregelen nemen ter bevordering van de goede orde in de organisatie. Die voorschriften beperken zich niet tot devices die door OVO Zaanstad geleverd worden, maar kunnen ook betrekking hebben op het gebruik van privémiddelen zolang men zich daarop toegang verschaft tot gegevens die zich in informatiesytemen van OVO Zaanstad bevinden.
5. Tegen de achtergrond van de risico's van het gebruik van internet wordt van de gebruiker professioneel, integer en verantwoordelijk handelen verwacht. Zo:
    a. Deelt de gebruiker op internet of sociale media geen persoonsgegevens van personeel of leerlingen waartoe hij uit hoofde van zijn functie toegang heeft.
    b. Laat de gebruiker zich op social media niet negatief of anderszins ongepast uit over de school, over collega’s, over personeelsleden en/of over (mede-) leerlingen.
    c. Plaatst de gebruiker op social media niet zonder toestemming foto’s of andere afbeeldingen van de school en/of aan de school verbonden personen of leerlingen.
    d. Plaatst de gebruiker op social media geen content namens de stichting OVO Zaanstad, tenzij hij daarvoor toestemming heeft gekregen.
    e. Plaatst de gebruiker in zijn algemeenheid op social media geen content of gedraagt zich anderszins op een wijze die de school schade kan toebrengen.
6. Tegen de achtergrond van de risico's van het gebruik van devices wordt van de gebruiker verwacht dat zij hier als een verantwoordelijk gebruiker mee omspringt. Hier gelden de principes van fair use:
    a. Gebruiker heeft de devices in bruikleen, en dient daarom beschadiging, verlies of diefstal te voorkomen.
    b. Devices worden niet onbeheerd achtergelaten in openbare ruimten. Hieronder valt ook een auto indien deze niet geparkeerd is in een afgesloten garage die alleen toegankelijk is voor de gebruiker.

c. Persoonlijk gebruik van devices is toegestaan, maar binnen de kaders die verderop in de gedragscode worden gesteld.
d. Dataverbruik buiten WiFi-verbindingen dient te worden geminimaliseerd. Er wordt in principe niet verbonden met openbare WiFi-netwerken zoals bijvoorbeeld restaurants en hotels. Dit mag alleen als er sprake is van een noodgeval en er geen alternatieven zijn, zoals een persoonlijke hotspot via mobiele dataverbinding. Netwerken thuis zijn toegestaan.

7. In deze gedragscode wordt gestreefd naar een goede balans tussen controle op verantwoord gebruik van internet en devices en bescherming van de privacy van werknemers op de werkplek en leerlingen in de school.
8. De intensiteit van het gebruik van internet en de mate van gebruik van mobiele data wordt vastgelegd. Deze registratie geschiedt om de continuïteit van de technische infrastructuur te waarborgen, verstoring van bedrijfsprocessen en andere (financiële) schade tegen te gaan en om toezicht te houden op de naleving van de gedrags- en gebruiksregels door de gebruikers.
9. Inhoudelijke controle van internetgebruik kan, uitsluitend in opdracht van het College van Bestuur, plaatsvinden indien sprake is van een vermoeden van strijdig handelen met de gedrags- en gebruiksregels uit deze gedragscode door de gebruiker. Het niet naleven van deze regels kan leiden tot disciplinaire en arbeidsrechtelijke maatregelen.
10. Deze gedragscode betreft:
    a. De regels die de gebruiker dient na te leven bij het gebruiken van de door OVO Zaanstad voor zakelijk gebruik en/of onderwijszaken ter beschikking gestelde internetsystemen en devices.
    b. De omstandigheden waaronder OVO Zaanstad besluit tot het registreren, verzamelen en monitoren van tot personen herleidbare gegevens omtrent internetgebruik en het gebruik van devices.

1. Werkingssfeer

1.1 De gedragscode is bestemd voor medewerkers, leerlingen, ouders, inhuurpersoneel, stagiaires en gasten, hierna te noemen gebruikers. De gedragscode geldt voor alle gebruikers die binnen de gebouwen van OVO Zaanstad toegang tot internet hebben, maar ook voor hen die vanaf elders kunnen inloggen. De gedragscode heeft ook betrekking op alle apparaten die door OVO Zaanstad aan de gebruiker in bruikleen worden gegeven. Tevens geldt de gedragscode voor het gebruik van eigen apparatuur waarmee (draadloos) kan worden ingelogd op applicaties en informatiesystemen die door OVO Zaanstad aan de gebruiker ter beschikking worden gesteld.

2. Algemeen

2.1 OVO Zaanstad behoudt zich het recht voor de toegang tot bepaalde sites te beperken. Met name sites met een pornografische, racistische, discriminerende of een op entertainment gerichte inhoud kunnen worden geweerd.

2.2 OVO Zaanstad kan gebruikers het recht op het gebruik van (een deel van) internet ontzeggen wanneer toegang tot netwerken die door OVO Zaanstad worden beheerd, wordt misbruikt.

2.3 OVO Zaanstad kan medewerkers toegang tot bedrijfsdata via hun privéapparaten ontzeggen wanneer deze apparaten niet aan de beveiligingseisen voldoen. De actuele beveiligingseisen worden door ICT gepubliceerd.

3. Gebruik

3.1 Gebruikers mogen de internetsystemen en devices die OVO Zaanstad ter beschikking stelt, privé gebruiken onder de volgende voorwaarden:

a. Gokken, (online) gamen, downloaden van illegaal verkregen, auteursrechtelijk beschermde bestanden, en het bekijken van pornografisch, racistisch en beledigend materiaal is niet toegestaan.
b. Gebruik van sociale media is toegestaan, mits er geen berichten worden verstuurd die kunnen aanzetten tot haat, pesten en/of geweld.
c. Het gebruik van streamingdiensten is toegestaan, mits de inhoud van deze diensten niet illegaal verkregen is.
d. Applicaties en software mogen niet gedownload en geïnstalleerd worden op de devices van OVO Zaanstad. Dit is alleen mogelijk ná toestemming van leidinggevende en ná goedkeuring van de afdeling Onderwijsfaciliteiten. Laatstgenoemde afdeling is ook de enige die software en applicaties kan installeren voor de gebruiker.

3.2 De gebruiker is persoonlijk verantwoordelijk voor de inhoud die hij of zij publiceert op de sociale media. Uitgangspunt is hierbij dat de professionaliteit die wordt verlangt van medewerkers in het onderwijs, zoals beschreven in de gedragscode voor de sector en de CAO. De normen voor het gedrag op sociale media wijken bovendien niet af van de normen voor het real life gedrag binnen de school of organisatie. OVO Zaanstad vertrouwt erop dat medewerkers, leerlingen, ouders/verzorgers en andere betrokkenen verantwoord zullen omgaan met de sociale media.

3.3 Voor de communicatie op sociale media tussen medewerkers en leerlingen en/of ouders/verzorgers wordt een ander, professioneel account dan het privé account van de medewerker gebruikt. Wanneer er gebruik gemaakt wordt van chatapps zoals Whatsapp of Signal geldt dat de professional alleen deel mag nemen aan groepen waarvan deze zelf een beheerder is.

3.4 Ten aanzien van privégebruik van internet en sociale media op devices verstrekt door OVO Zaanstad geldt dat OVO Zaanstad geen verantwoordelijkheid of aansprakelijkheid accepteert wanneer de gebruiker via deze devices aanstootgevend, pornografisch of racistisch materiaal publiceert of zich anderszins schuldig maakt aan het plegen van strafbare feiten met behulp van devices van OVO Zaanstad.

3.5 De infrastructuur voor elektronische communicatie kent een eigen vorm van kwetsbaarheid en een eigen vorm van beveiliging. Dit vraagt om speciale aandacht op tenminste de volgende punten:

- User-identificatie (inlognaam) en wachtwoord zijn persoonsgebonden en vertrouwelijk en mogen niet worden gedeeld met anderen.
- Het is niet toegestaan om de e-mail die verstrekt wordt door OVO Zaanstad te gebruiken voor privé-doeleinden. Denk hier aan nieuwsbrieven, webwinkels of forums op internet.

- Onbedoelde inbreuken op de beveiliging van binnenuit of van buitenaf moeten onverwijld conform het protocol Informatiebeveiliging en Privacy aan de privacymedewerker op de school gemeld worden.

3.6 Data die in systemen van OVO Zaanstad opgeslagen is, blijft eigendom van OVO Zaanstad. Het is niet toegestaan om:

a. Data uit systemen van OVO Zaanstad te downloaden en op te slaan op privésystemen. Wanneer gegevens van OVO Zaanstad via een privédevice worden geraadpleegd, dan dienen de gegevens in het informatiesysteem te blijven staan. Exporteren naar Excel of PDF is daarmee uitgesloten, als ook het opslaan op externe opslagmedia.
b. Gegevens uit de informatiesystemen van OVO Zaanstad mogen niet op internet verspreid worden, ook niet geredacteerd of geherformuleerd.
c. Foto- en videomateriaal opgeslagen in systemen van OVO Zaanstad mag niet verspreid worden op internet, of opgeslagen op privédevices.
d. Gegevens uit informatiesystemen mogen niet gedeeld worden met derde (commerciële) partijen, niet zonder uitdrukkelijke toestemming van het College van Bestuur en na advies van de Functionaris Gegevensbescherming. Uitzondering hierop zijn gegevens die gedeeld worden met derden voor het uitvoeren van onze eigen publiekrechtelijke taak, of wanneer een derde partij voor het uitvoeren van die taak gegevens verlangt. De derde partij moet altijd kunnen verklaren op welke grond zij gegevens verlangt.
e. Uitzondering op bovenstaande is het delen van gegevens op basis van goed werkgeverschap, zoals het versturen van een attentie bij ziekte of verjaardag.

4. Controle

4.1 Om de veiligheid van het netwerk te waarborgen en toe te zien op een zorgvuldig gebruik overeenkomstig deze gedragscode worden voortdurend controles uitgevoerd door OVO Zaanstad. Hiernaast wordt toegezien op de technische integriteit en beschikbaarheid van de infrastructuur en diensten. Controle vindt in beginsel geanonimiseerd plaats. Controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeersgegevens (tijd, hoeveelheid, omvang, ed.).Overig toezicht op het gebruik zal bestaan uit het technisch controleren van het gebruik van internet en e-mail verkeer (bv. sites die bezocht worden, de omvang van e-mailboxen). Slechts indien er sprake is van ernstig vermoeden van strijdig handelen met de gedrags- en gebruiksregels door de gebruiker en na opdracht van het College van Bestuur worden gegevens niet-anoniem gecontroleerd. Betrokkene wordt hiervan op de hoogte gesteld.

4.2 Toegang tot gegevens van OVO Zaanstad vanaf privédevices wordt gecontroleerd. Dat houdt in dat gecontroleerd wordt met welk device de gebruiker verbinding probeert te maken met de systemen van OVO Zaanstad. Dit device wordt gecontroleerd op de aanwezigheid van mimimale criteria voor de beveiliging. OVO Zaanstad stelt eisen aan het niveau van geïnstalleerde beveiligingsupdates en vereist dat het apparaat beveiligd is met een pincode, beveiligingspatroon of biometrische beveiliging. OVO Zaanstad kan niet de inhoud van een privédevice controleren. De controles die plaatsvinden hebben uitsluitend het karakter van toegangscontrole. Devices die niet aan de minimale eisen voldoen zullen geen verbinding kunnen maken met informatiesystemen van OVO Zaanstad, zoals bijvoorbeeld e-mail en bestanden.

4.3 E-mailberichten van MR-leden, bedrijfsarts en vertrouwenspersonen zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle op de veiligheid van het

berichtenverkeer (bv. virussen), of de aanwezigheid van voldoende beveiligingsmaatregelen op privédevices.

4.4 Binnenkomend internet- en e-mailverkeer wordt zo goed mogelijk gecontroleerd op virussen. Mocht blijken dat een e-mailbericht een virus bevat, dan wordt het automatisch tegengehouden en worden de verzender en eventueel de ontvanger daarover ingelicht. Indien desondanks een e-mail wordt ontvangen die mogelijk een virus bevat, dan dient de ontvanger onverwijld contact op te nemen met de informatiemanager en/of de directie van de school. Deze zorgt in dat geval voor adequate actie.

4.5 Indien mocht blijken dat in strijd met deze gedragscode wordt gehandeld of indien daarvoor aanwijzingen zijn (zoals klachten, signalen van binnen of buiten OVO Zaanstad en systeemstoringen), dan kunnen gegevens van (de) betrokken gebruiker(s) worden uitgedraaid, bekeken en gebruikt. Controleren alsmede openen van e-mail, ook die voor privégebruik ontvangen op een mailadres van OVO Zaanstad, ten behoeve van het opsporen van onrechtmatig gedrag van de gebruiker is dus alleen toegestaan indien er sprake is van een ernstig vermoeden of een verdenking van ongeoorloofd handelen. Alleen het College van Bestuur kan opdracht geven tot persoonsgerichte/inhoudelijke controle. Controle van privédevices is niet mogelijk en niet toegestaan. De controles die OVO Zaanstad mag uitvoeren hebben uitsluitend betrekking op devices en toegang tot systemen die door OVO Zaanstad worden verstrekt en beheerd.

4.6 Persoonsgegevens over e-mail en internetgebruik worden niet langer bewaard dan wettelijk toegestaan. Van langere opslag is alleen sprake wanneer nader onderzoek en eventueel te treffen maatregelen jegens een gebruiker noodzakelijk zijn. Gegevens worden bewaard als er procedures lopen waarbij genomen maatregelen in rechte worden bestreden.

5. Sancties

5.1 Bij handelen in strijd met deze gedragscode, het belang van de stichting of de algemeen geldende normen en waarden voor het gebruik van internet en devices kunnen, afhankelijk van de aard en de ernst van de overtreding, maatregelen worden getroffen. Voor medewerkers kan dit worden aangemerkt als plichtsverzuim op grond waarvan disciplinaire maatregelen krachtens de CAO VO kunnen worden getroffen. Voor leerlingen en gasten zijn maatregelen denkbaar als tijdelijke of permanente ontzegging van de toegang tot het netwerk of tot internet. Daarnaast kunnen voor leerlingen ook maatregelen getroffen worden zoals schorsing op grond van overtreding van de huis- en orderegels als bedoeld in het schoolreglement.

5.2 Indien een uitlating op internet van leerlingen en/of ouders/verzorgers of medewerkers mogelijk een strafrechtelijke overtreding inhoudt, wordt in beginsel door de betreffende school of door OVO Zaanstad aangifte bij de politie gedaan.

6. Slot

6.1 In alle gevallen waarin deze gedragscode niet voorziet, beslist het College van Bestuur conform het arbeidsrechtelijke kader en de Algemene Verordening Gegevensbescherming (AVG).

6.2 Deze geactualiseerde gedragscode treedt in werking op 1 juli 2024.