



SAMENWERKINGSVERBAND VO ZAANSTREEK

Gedragcode gebruik internet, intranet-
e-mailgebruik en sociale media
Samenwerkingsverband VO Zaanstreek

Vastgesteld door directeur-bestuurder	13 oktober 2023
Besproken met Raad van Toezicht	12 oktober 2023
Instemming MR-p	03 oktober 2023

Inhoudsopgave

Doel van de gedragscode.....	2
1. Werkingssfeer	3
2. Algemeen	3
3. Gebruik.....	3
4. Controle.....	4
5. Sancties	5
6. Slot.....	5

Doel van de gedragscode

Deze gedragscode omschrijft de regels voor het gebruik van internet, e-mail, intranet en sociale media (hierna tezamen "internet").

De volgende punten zijn overwogen bij het vaststellen van deze gedragscode:

1. In deze gedragscode wordt gestreefd naar een goede balans tussen controle op verantwoord internetgebruik en bescherming van de privacy van werknemers op de werkplek en leerlingen in de school.
2. Gebruik van het internet is voor de medewerkers van SVZ nodig om hun werk goed te doen, maar onjuist hiermee omgaan kost tijd en capaciteit van mensen en apparatuur en brengt diverse risico's met zich mee.
3. 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.
4. Ter vermijding van dergelijke risico's geeft deze gedragscode voorschriften voor het verrichten van de arbeid en neemt maatregelen ter bevordering van de goede orde in de organisatie.
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.
 - b. Laat de gebruiker zich op social media niet negatief of anderszins ongepast uit over de organisatie, over collega's, over personeelsleden en/of over leerlingen.
 - c. Plaatst de gebruiker op social media niet zonder toestemming foto's of andere afbeeldingen van de organisatie of aan de organisatie verbonden personen of leerlingen.
 - d. Plaatst de gebruiker op social media geen content namens de SVZ, 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 organisatie schade kan toebrengen.
6. De intensiteit van het gebruik van internet 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.

Inhoudelijke controle van internetgebruik kan, uitsluitend in opdracht van de directeur-bestuurder, 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.
7. Deze gedragscode betreft:
 - a. De regels die de gebruiker dient na te leven bij het gebruiken van de door SVZ voor zakelijk gebruik en/of onderwijszaken ter beschikking gestelde internetsystemen.
 - b. De omstandigheden waaronder SVZ besluit tot het registreren, verzamelen en monitoren van tot personen herleidbare gegevens omtrent internetgebruik.

1. Werkingssfeer

1.1 De gedragscode geldt voor alle gebruikers die in opdracht van SVZ-toegang tot internet hebben, ook voor hen die vanaf elders kunnen inloggen. Tevens geldt de gedragscode voor het gebruik van eigen apparatuur waarmee (draadloos) kan worden ingelogd.

2. Algemeen

2.1 SVZ 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 SVZ kan gebruikers het recht op het gebruik van (een deel van) internet ontzeggen.

2.3 SVZ is voornemens over te gaan naar een systeem van beveiligd e-mailen. Het verdient de voorkeur om altijd versleuteld te mailen met partijen buiten SVZ.

3. Gebruik

3.1 Gebruikers mogen, m.u.v. het in punt 3.4 gestelde, uitsluitend zakelijk gebruik maken van het internetsysteem van de organisatie. Gebruik is dus verbonden met taken/bezigheden die voortvloeien uit de taken en werkzaamheden van de gebruiker. Daarbij dienen zij zich te houden aan de door SVZ opgestelde regels en procedures.

De gebruiker is persoonlijk verantwoordelijk voor de inhoud, die hij of zij publiceert op de sociale media. Uitgangspunt is hierbij dat de professionals zelf weten hoe ze verstandig omgaan met de sociale media. De normen voor het gedrag op sociale media wijken niet af van de normen voor het real life gedrag binnen de school of organisatie.

3.2 Het is gebruiker niet toegestaan:

- Spelletjes, muziekbestanden, foto's en filmpjes te downloaden of real time te bekijken, te winkelen, te gokken, deel te nemen aan kansspelen en/of chat-/babbelboxen te bezoeken, tenzij dit past in het kader van onderwijs(ondersteunende)activiteiten.
- Sites te bezoeken, te downloaden en te verspreiden die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten, tenzij dit past in het kader van onderwijs(ondersteunende)activiteiten.
- Berichten te versturen die kunnen aanzetten tot haat en/of pesten en geweld.

3.3 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 mogen niet aan anderen worden doorgegeven.
- Het downloaden en installeren van software en applicaties is niet toegestaan, tenzij vooraf toestemming is verleend door de leidinggevende. Deze toestemming wordt alleen verleend als wordt voldaan aan de geldende rechten van veel auteursrechtelijk beschermde bestanden (zoals copyright) en eventuele licenties worden betaald. Gedownloade en geïnstalleerde software en applicaties moeten voor gebruik op virussen zijn gescand.
- De leidinggevende is verantwoordelijk voor vertrouwelijke gegevens en bedrijfsgevoelige informatie die wordt verstuurd. Bij twijfel moet met hem/haar worden overlegd.

- Het is niet toegestaan deel te nemen aan niet-zakelijke nieuwsgroepen, abonnementen op e-zines, nieuwsbrieven en dergelijke met het e-mailadres van SVZ.
 - Onbedoelde inbreuken op de beveiliging van binnenuit of van buitenaf dienen onverwijld conform het protocol Informatiebeveiliging en Privacy aan de privacy-officer gemeld te worden.
- 3.4 Werknemers mogen het internet van de organisatie incidenteel en kortstondig voor privédoeleinden gebruiken, zowel intern als extern, mits dit niet storend is voor de dagelijkse werkzaamheden en mits hierbij wordt voldaan aan de verdere richtlijnen van de gedragscode en de privacyreglementen van SVZ.
- 3.5 Het is bovendien niet toegestaan om door middel van internet:
- berichten anoniem of onder een fictieve naam te versturen;
 - iemand elektronisch lastig te vallen;
 - met opzet virussen te verspreiden;
 - dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten en kettingmailberichten te verzenden of door te sturen. Indien de gebruiker ongevraagde informatie van deze aard aangeboden krijgt, dient deze dit te melden aan de direct leidinggevende. De direct leidinggevende meldt dit vervolgens aan de informatiemanager.
- 3.6 Het is ook anderszins niet toegestaan op internet of door middel van het e-mailsysteem in strijd met de wet of onethisch te handelen.

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. 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 de directeur-bestuurder worden gegevens niet-anoniem gecontroleerd. Betrokkene wordt hiervan op de hoogte gesteld.
- 4.2 E-mailberichten van OPR-leden, bedrijfsarts en vertrouwenspersonen zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle op de veiligheid van het berichtenverkeer (bv. virussen).
- 4.3 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 dat 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.
- 4.4 Indien mocht blijken dat in strijd met deze gedragscode wordt gehandeld of indien daarvoor aanwijzingen zijn (zoals klachten, signalen van binnen of buiten SVZ 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, 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 de directeur-bestuurder kan opdracht geven tot persoonsgerichte/inhoudelijke controle.

- 4.5 Persoonsgegevens over e-mail en internetgebruik worden niet langer bewaard dan in het kader van nader onderzoek en eventueel te treffen maatregelen jegens een gebruiker noodzakelijk is. 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 bedrijfsbelang of de algemeen geldende normen en waarden voor het gebruik van internet 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 gasten zijn maatregelen denkbaar als tijdelijke of permanente ontzegging van de toegang tot het netwerk of tot internet.

5.2 Indien de uitlating van medewerkers mogelijk een strafrechtelijke overtreding inhoudt, wordt in beginsel aangifte bij de politie gedaan.

6. Slot

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

6.2 Deze geactualiseerde gedragscode treedt in werking op 1 augustus 2023.