PROO LEIDEN LEIDERDORP

Stichting Openbaar Primair en Speciaal Onderwijs Leiden-Leiderdorp

Gedragscode Informatie Beveiliging en Privacy (IBP)

Document vanuit Kennisnet	
Tekstuele aanpassingen, document naar HR en Functionaris Gegevensbescherming	17 november 2020
Aanpassingen doorgevoerd, document naar klankbordgroep en directeur-bestuurder.	8 december 2020
Aanpassingen doorgevoerd.	9 maart 2021
Ter instemming voorgelegd aan de GMR	31 maart 2021
Vastgesteld door de directeur-bestuurder	
Evaluatie en herziening	medio 2022
Vastgesteld door GMR	12 mei 2021
Vastgesteld door bestuur	26 mei 2021
Document van kracht per	1 juli 2021

ONDERWIJS MET AANDACHT VOOR ELKAAR

Elisabethhof 17 • 2353 EW Leiderdorp • 071 524 76 70
mail@prooleiden.nl • www.prooleiden.nl

Deze gedragscode sluit aan bij het informatiebeveiliging en privacy beleid (IBP-beleid). De gedragscode geeft aan wat het IBP-beleid voor medewerkers in de praktijk betekent en legt vast wat er van de medewerkers verwacht wordt met betrekking tot het gebruik van de ter beschikking gestelde bedrijfsmiddelen en de inzet van eigen devices voor schoolwerkzaamheden.

Dit document is opgesteld aan de hand van de richtlijnen van Kennisnet en daarmee juridisch in lijn met de Privacywetgeving. De teamleider HR en twee klankbordgroepen (HR en communicatie) zijn bij het proces betrokken geweest, net als de FG die voor onze stichting is aangesteld.

Hoofdstuk 1 'Inleiding' beschrijft wat onder bedrijfsmiddelen verstaan wordt, de uitgangspunten van de gedragscode en de driedeling van gegevens (openbaar, intern en vertrouwelijk) die verwerkt worden.
Hoofdstuk 2 'Gedragscode' bevat de 'bouwstenen' waarmee de afspraken kunnen worden vastgelegd die relevant zijn voor de gewenste gedragscode van een school. Elke school kan met de bijbehorende paragrafen een gedragscode ***'op maat'*** maken.
Per onderwerp en/of per onderdeel (bullet) binnen een onderwerp kunnen keuzes en aanpassingen gemaakt worden.
HOOFDSTUK 3: **'CONTROLE GEBRUIK BEDRIJFSMIDDELEN' BESCHRIJFT DE VOORWAARDE VAN CONTROLE, DE UITVOERING ERVAN, DE EVENTUELE SANCTIES EN DE MOGELIJKHEID VAN BEZWAAR MAKEN.**
Hoofdstuk 4: 'GMR' laat de rol van de GMR zien.
Hoofdstuk 5: 'Slotbepaling' toont de datum van de eerstvolgende evaluatie en eventuele aanpassing van de gedragscode.

Inhoudsopgave

1 Inleiding

Het gebruik van internet, computernetwerk, en e-mail is voor alle medewerkers van de school noodzakelijk om de werkzaamheden te kunnen verrichten. Bij deze werkzaamheden wordt gebruik gemaakt van veel gegevens, waaronder persoonsgegevens. De (ict)faciliteiten en de verschillende gegevens worden in dit document **bedrijfsmiddelen** genoemd.
Onder bedrijfsmiddelen worden in ieder geval verstaan:

- Hardware: *pc, laptop, tablet, telefoon, hardware token (tag).*
- Software (of -systemen): *alle applicaties voor het uitvoeren van de werkzaamheden, zoals de school e-mailomgeving, Microsoft Office, administratiesystemen, leerlingvolgsystemen en (online)digitaal lesmateriaal maar ook apps op (mobiele) devices.*
- Informatie en (persoons)gegevens: *rapportages, leerling dossiers, gegevens in e-mails. Hierbij vraagt de verwerking van persoonsgegevens vanuit de privacywetgeving extra maatregelen.*
- Internetgebruik: *het bezoeken van het World Wide Web, het gebruik van e-mail en sociale media zoals Facebook, LinkedIn, Instagram en Twitter.*

Aan het gebruik van deze bedrijfsmiddelen zijn risico's verbonden, waardoor het noodzakelijk is om hierover afspraken te maken. Van medewerkers van PROOLeiden-Leiderdorp wordt verwacht dat zij verantwoord omgaan met de beschikbaar gestelde bedrijfsmiddelen. Dit wordt ook verwacht als medewerkers hun eigen middelen inzetten om werkzaamheden voor de school uit te voeren.

De afspraken in dit document gelden voor alle locaties van waaruit (school)werkzaamheden worden verricht en voor alle devices waarmee het werk wordt uitgevoerd. Ze gelden voor iedereen die werkzaam is bij PROOLeiden-Leiderdorp, ook voor uitzendkrachten en tijdelijke werknemers.

1.1 Uitgangspunten gedragscode

Deze gedragscode legt regels vast voor het gebruik van de bedrijfsmiddelen door medewerkers en over de controle op de naleving hiervan.
Het doel van deze gedragscode is om de normen en uitgangspunten vast te leggen ten aanzien van:

- systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik
- het tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten
- de bescherming van privacy gevoelige informatie waaronder persoonsgegevens van het schoolbestuur, haar medewerkers, leerlingen en hun ouders en daarmee het beschermen van de privacy en veiligheid van alle betrokkenen
- de bescherming van vertrouwelijke informatie van het schoolbestuur, haar medewerkers, leerlingen en hun ouders
- het voorkomen en tegengaan van misbruik van de bedrijfsmiddelen
- de bescherming van de intellectuele eigendomsrechten van het schoolbestuur en derden

- het voorkomen van negatieve publiciteit
- kosten- en capaciteitsbeheersing

De controle op het gebruik van bedrijfsmiddelen is een verwerking van persoonsgegevens in de zin van de privacywetgeving. Het PROOLeiden-Leiderdorp zal dan ook de controle en handhaving van deze regels conform de privacywetgeving en het algemene arbeidsrechtelijk kader uitvoeren. Hierbij is het uitgangspunt een goede balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers op de werkplek. Gegevens worden alleen verzameld en gebruikt voor deze doelen.
In het bijzonder zal het bestuur de bij controle vastgelegde gegevens beveiligen tegen ongeautoriseerde toegang. Het bestuur zal mensen met toegang daartoe contractueel verplichten tot afdoende geheimhouding.

Het schoolbestuur streeft in het kader van handhaving van dit document naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele medewerkers zo veel mogelijk beperken. Zij zal waar mogelijk slechts geautomatiseerd controleren of filteren zonder daarbij zichzelf of andere personen inzage te geven in het gedrag van individuele personen.

1.2 Eigen verantwoordelijkheid en privégebruik

Het gebruik van door PROOLeiden-Leiderdorp verstrekte bedrijfsmiddelen is persoonlijk en blijft de verantwoordelijkheid van de medewerker. Alle devices die voor schoolwerk worden gebruikt (inclusief eigen devices ‘Own Device’) worden niet uitgeleend of aan anderen ter beschikking gesteld zonder aanvullende (beveiligings)maatregelen. Het niet voldoen aan de regels voor informatiebeveiliging en privacy kan leiden tot disciplinaire maatregelen.

1.3 Verschillende soorten gegevens

PROOLeiden-Leiderdorp is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en privacy is het beschermen van gegevens.
PROOLeiden-Leiderdorp onderscheidt drie typen gegevens:

- **Openbare gegevens**; dit zijn gegevens die juist voor publicatie bedoeld zijn.
- **Interne gegevens**; dit zijn gegevens die alleen voor gebruik en verwerking binnen PROOLeiden-Leiderdorp bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
- **Vertrouwelijke gegevens**; dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen PROOLeiden-Leiderdorp toegankelijk zijn. Denk hierbij aan (bijzondere) persoonsgegevens, personeelsgegevens of aanbestedingsgegevens.

Persoonsgegevens verdienen bijzondere aandacht. Dit zijn gegevens die een persoon betreffen én waardoor een persoon geïdentificeerd of identificeerbaar is. Denk hierbij aan naamgegevens, e-mailadressen maar ook aan telefoonnummers van zowel collega’s als leerlingen en ouders van leerlingen.

De privacywetgeving verplicht elk individu om zorgvuldig met persoonsgegevens om te gaan. Een onderdeel van de wettelijke verplichting is dat PROOLeiden-

Leiderdorp schriftelijk afspraken maakt met leveranciers van (online)applicaties, waarbij persoonsgegevens worden verwerkt (denk hierbij aan inloggegevens, wachtwoorden en het opslaan van gemaakt werk). Persoonsgegevens moeten altijd met uiterste zorgvuldigheid verwerkt en gedeeld worden.

- Als persoonsgegevens toegankelijk en of inzichtelijk zijn voor personen, die geen toegang behoren te hebben tot deze gegevens is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Een dergelijk incident kan schadelijke gevolgen hebben voor de betrokkene(n) en PROOLeiden-Leiderdorp.

Om op een veilige, verantwoorde en werkbare manier met deze gegevens om te gaan maakt PROOLeiden-Leiderdorp afspraken over:

- de verwerking en verspreiding van vertrouwelijke- en persoonsgegevens. Er worden niet meer gegevens verwerkt dan noodzakelijk om het doel te bereiken
- de uitwisseling van gegevens, waarbij aan de ontvanger wordt aangegeven wat de ontvanger wel of niet mag doen met de gegevens
- opslag en verspreiding van gegevens, waarbij alléén gebruik gemaakt wordt van door PROOLeiden-Leiderdorp goedgekeurde bedrijfsmiddelen.

Van medewerkers van PROOLeiden-Leiderdorp en/of externe medewerkers, die uit hoofde van hun functie toegang hebben tot de digitale informatiesystemen en hiermee toegang hebben tot bv. personeelsdossiers, vertrouwelijke enquêtegegevens, zorgdossiers et cetera, wordt verwacht dat zij zorgvuldig omgaan met de functioneel aan hen beschikbaar gestelde informatie. Dat zij de privacywetgeving hanteren en op geen enkele wijze informatie, waarvan redelijkerwijze kan worden aangenomen dat deze vertrouwelijk of privacygevoelig is, zonder toestemming van betrokkene of leidinggevende te gebruiken en/of naar buiten te brengen.

2 Gedragscode

In deze gedragscode voor verantwoord gebruik van bedrijfsmiddelen geeft PROOLeiden-Leiderdorp aan wat de afspraken zijn met betrekking tot verschillende onderwerpen rondom het gebruik van bedrijfsmiddelen en wat dit voor de medewerkers in de dagelijkse praktijk betekent.

2.1 Algemene normen

Iedere medewerker voldoet aan de volgende algemene normen voor 'zorgvuldigheid' (niet uitputtend):

- Ga zorgvuldig om met persoonsgegevens, waarbij de basisregels (mede benoemd in de geheimhoudingsverklaring), voor het omgaan met persoonsgegevens als bekend worden geacht.
- Bewaar persoonsgegevens niet langer dan nodig is. Wanneer persoonsgegevens niet meer worden gebruikt, verwijder deze dan. Dit geldt zowel voor elektronische als papieren gegevens.
- Voorkom het lekken van interne en vertrouwelijke informatie.
- Zorg voor een goede fysieke en technische bescherming van bedrijfsmiddelen. (beveiligingsmaatregelen).
- Voorkom dat beveiligingsmaatregelen moedwillig worden omzeild
- Meld diefstal of verlies van bedrijfsmiddelen onmiddellijk na constatering door het sturen van een e-mail aan meldpuntdatalekken@prooleiden.nl of een telefonische melding bij de daarvoor aangewezen persoon (zie hiervoor de procedure meldplicht datalekken van PROOLeiden-Leiderdorp).
- Indien er vrijwilligers worden ingezet binnen de school die in aanraking zouden kunnen komen met persoonsgegevens, laat deze dan een geheimhoudingsovereenkomst ondertekenen. Wees terughoudend bij de inzet van vrijwilligers als het om gevoelige persoonsgegevens gaat.

Om bovenstaande te borgen dienen alle medewerkers binnen de scholen en vrijwilligers die werkzaam zijn op de scholen een geheimhoudingsverklaring te ondertekenen. Zie hiervoor de bijlagen.

2.2 Computergebruik

Voor het uitoefenen van de werkzaamheden stelt PROOLeiden-Leiderdorp aan de medewerker computer- en netwerkfaciliteiten (ict-bedrijfsmiddelen) ter beschikking. Het gebruik van deze ict-bedrijfsmiddelen is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:

- Zorg dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden.
- Weet welke gegevens er mogen worden gebruikt (mag iedereen het zien?) en welke ict-voorzieningen kunnen worden ingezet (is het veilig genoeg?) bij het verrichten van de verschillende schoolwerkzaamheden.
- Sla (persoons)gegevens alleen op de daarvoor aangewezen systemen op. (Opslaan van gegevens in public Cloud omgevingen, zoals een persoonlijke Dropbox, is niet toegestaan).
- Sla persoonsgegevens niet op de C-schijf van laptop of desktop op, omdat deze bij verlies of diefstal in verkeerde handen kan vallen. Sla

persoonsgegevens dus op jullie netwerkschijf op of in OneDrive (beveiligde cloudomgeving).
- Versleutel alle gegevens met betrekking tot PROOLeiden-Leiderdorp, indien deze gegevens, om welke reden dan ook, elders opgeslagen worden (bijvoorbeeld: geen onversleutelde persoonsgegevens op een USB-stick)
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.
- Sluit na gebruik de computer af of log uit.
- Meld storingen van beheerde werkplekken (computer of laptop) in overleg met de IT-coördinator van de school bij ITS.

2.3 Werkplek

Voorkom dat anderen (onbedoeld) toegang kunnen krijgen tot bedrijfsmiddelen waartoe zij geen rechten hebben en/of laat gegevens niet (onbedoeld) lekken. Als aanvullende regels op computergebruik gelden voor de werkplek de volgende clean desk en clear screen regels:

- Vergrendel bij het tijdelijk verlaten van de werkplek de pc (windowstoets+L).
- Verwijder interne en vertrouwelijke documenten van het bureau bij het voor langere tijd verlaten van de werkplek (denk hierbij voorbeeld aan het opbergen van de klassenmap als je een vergadering in gaat).
- Voorkom dat gevoelige en vertrouwelijke informatie zichtbaar is wanneer iemand anders op het beeldscherm (of via een beamer) mee kan kijken. Sluit het e-mailprogramma af en zorg voor een opgeruimd digitaal bureaublad.
- Laat geen afdrukken bij de printer liggen, zeker niet als er persoonsgegevens op staan (advies is te printen via een postbussysteem, waarbij de printer afdrukt nadat hierop is ingelogd).
- Haal overbodig geworden papieren documenten met persoonsgegevens erop altijd door de papierversnipperaar (een papierversnipperaar is op elke school verplicht aanwezig).
- Persoonsgegevens op papier dienen alleen voor bevoegden toegankelijk te zijn. Leerling- en personeelsdossiers dienen in een afgesloten kast of ruimte bewaard te worden.

LET OP: Als persoonsgegevens toegankelijk/inzichtelijk zijn voor personen, die geen toegang behoren te hebben tot die gegevens is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Weet dat beveiligingsincidenten en mogelijke datalekken gemeld moeten worden volgens de procedure meldplicht datalekken van PROOLeiden-Leiderdorp.

2.4 Gebruik eigen devices (BYOD - Bring Your Own Device)

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor PROOLeiden-Leiderdorp worden uitgevoerd. PROOLeiden-Leiderdorp is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen van de school.

Voor ‘Own Devices’ ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:

- Beveilig het device met een wachtwoord, of in het geval van een smartphone of tablet, met een pincode die langer is dan 4 tekens.
- Wees je bewust van de risico's van het gebruik van zakelijke (school)e-mail of andere school toepassingen op het device (bijv. gebruik door anderen binnen gezin, verlies of diefstal).
- Voor gebruik van schooltoepassingen op het device is vooraf toestemming van de schooldirecteur vereist
- Vergrendel het device bij het verlaten van de werkplek (windowstoets+L).
- Sla persoonsgegevens van PROOLeiden-Leiderdorp niet op het eigen device op; dit is niet toegestaan.
- Versleutel alle gegevens, anders dan persoonsgegevens, met betrekking tot PROOLeiden-Leiderdorp als deze, om welke reden dan ook, niet op het schoolnetwerk opgeslagen worden (denk hierbij aan het eigen device of usb-stick).
- In geval van thuiswerken geldt als uitgangspunt dat er gewerkt wordt via Remote Desktop of wordt gewerkt via de OneDrive of Google Drive van je schoolaccount.
- Scheid (versleutelde)gegevens, anders dan persoonsgegevens, van PROOLeiden-Leiderdorp en privégegevens van elkaar. Deze scheiding moet duidelijk herkenbaar zijn op het eigen device.
- Houd software up-to-date door het uitvoeren van periodieke updates (minimaal maandelijks).
- Neem adequate maatregelen tegen virussen of malware door het up-to-date houden van de virusscanner en door het periodiek (minimaal maandelijks) scannen van het device.

Op verzoek van PROOLeiden-Leiderdorp moet de medewerker zelf aantonen dat de bovenstaande maatregelen worden toegepast.

2.5 Software en digitaal lesmateriaal

Het gebruik van digitaal lesmateriaal is niet meer weg te denken bij PROOLeiden-Leiderdorp. Dit lesmateriaal staat steeds meer online waarbij steeds vaker persoonsgegevens worden uitgewisseld. De privacywetgeving eist dat elke organisatie vooraf aan het gebruik van dergelijk materiaal bekijkt wat de invloed ervan is op de privacy, dit kan specifieke maatregelen tot gevolg hebben.
De onderstaande regels gelden voor installatie en gebruik van software en (online)digitaal lesmateriaal:

- Installeren van software wordt bij PROOLeiden-Leiderdorp alleen toegestaan met de juiste licenties en na het nemen van eventuele aanvullende maatregelen.
- Bij het gebruik van online software, app's en digitaal lesmateriaal, wordt gekeken of er persoonsgegevens bij verwerkt worden.
- Een verwerkersovereenkomst wordt afgesloten met elke leverancier van (online)software, die in opdracht van PROOLeiden-Leiderdorp persoonsgegevens verwerkt. Regel dit vooraf aan het gebruik via het bestuurskantoor (verwerkersovereenkomst dient door bestuur ondertekend te worden).

- Aanvragen van digitaal lesmateriaal en/of andere software volgt bij PROOLeiden-Leiderdorp de afgesproken aanvraagprocedure.

2.6 Gebruik van e-mail

PROOLeiden-Leiderdorp stelt een e-mailsysteem en een bijbehorende mailbox aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik van e-mailfaciliteiten is verbonden aan deze werkzaamheden en gaan uit van de volgende afspraken:

- Gebruik het school e-mailadres *alléén* voor school gerelateerde zaken.
- Gebruik voor privé e-mail een eigen privé e-mailadres via een externe web maildienst. (bijvoorbeeld webmail van Gmail, Hotmail of een eigen provider).
- Ontvangen van privémail op het school e-mailadres is incidenteel toegestaan.
- Het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie.
- Persoonsgegevens mogen alleen versleuteld worden gemaild, waarbij de toegangscode op een ander wijze aan de ontvanger wordt verstrekt.
- Het is uiteraard 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 en geweld.
- Schoon de e-mailbox periodiek (bijv. maandelijks) op middels shift-delete (zodat deze ook niet in de verwijderde items blijft staan).
- Het e-mailadres is een bedrijfsmiddel welke nodig is om effectief te kunnen functioneren, conform de verplichtingen die voortvloeien uit de arbeidsovereenkomst en het kunnen voldoen aan wet- en regelgeving. Alleen in bijzondere situaties, denk hierbij aan uitdiensttreding, is verlenging tot toegang e-mail toegestaan, mits dit schriftelijk wordt bevestigd door een bevoegde persoon en waarbij een einddatum van de toegang is opgenomen.
- Het is niet toegestaan om tussentijds en/of na beëindiging van de arbeidsovereenkomst de inhoud van je mailbox, OneDrive en SharePoint te downloaden voor eigen gebruik.

2.7 Gebruik van internet

PROOLeiden-Leiderdorp stelt het gebruik van internet en de bijbehorende faciliteiten aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik hiervan is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:

- Incidenteel persoonlijk gebruik is toegestaan, mits dit
  - niet storend is voor de dagelijkse werkzaamheden
  - niet voor commerciële doeleinden is en
  - geen verboden gebruik oplevert.
- Het is niet toegestaan om
  - op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten
  - films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron
  - onder lestijd internettoegang te gebruiken voor privédoeleinden
  - deel te nemen aan kansspelen.

- Het is verboden op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende toon te communiceren via online fora, sociale netwerken en andere vergelijkbare communicatienetwerken over alle aan school verbonden betrokkenen en activiteiten. Dit geldt in het bijzonder ook voor internetgebruik buiten het schoolnetwerk met betrekking tot aan de school verbonden betrokkenen en activiteiten.

2.8 Veilig online

We brengen met z'n allen steeds meer tijd online door. Hierbij worden steeds meer mobiele devices gebruikt. Menselijk (online)handelen staat veelal aan de basis van een datalek.
PROOLeiden-Leiderdorp verwacht van medewerkers dat zij:

- het onderscheid kennen tussen veilige en onveilige netwerken (openbare wifinetwerken) en websites
- bij het verwerken van persoonsgegevens alléén gebruik maken van bekende én beveiligde draadloze netwerken
- weten wat malware is, het kunnen herkennen en weten hoe te handelen
- terughoudend zijn met het online achterlaten van gegevens met betrekking tot PROOLeiden-Leiderdorp
- controleren of er daadwerkelijk van een bekend én beveiligd netwerk gebruik gemaakt wordt bij het bezoek aan openbare ruimtes. (Een netwerk kan bekend zijn omdat het een PROOLeiden-Leiderdorp netwerk is of het eigen draadloze netwerk thuis is).

2.9 Sociale media

Sociale media is een verzamelnaam voor alle internettoepassingen die het mogelijk maken om informatie met elkaar te delen op een eenvoudige en vaak leuke manier. Het gaat hierbij niet alleen om informatie in de vorm van tekst (nieuws, artikelen). Ook geluid (podcasts, muziek) en beeld (fotografie, video) worden gedeeld via sociale media (Instagram, YouTube, Facebook, Twitter enz.). De essentie van sociale media is dat iemand er informatie deelt over zichzelf, over anderen of over een bepaald onderwerp. Voor gebruik van sociale media geldt als uitgangspunt dat het digitale gedrag op sociale media niet op een schadelijke manier afwijkt van het real life gedrag binnen de school. Medewerkers zijn altijd de vertegenwoordiger van PROOLeiden-Leiderdorp ook als zij online een privémening verkondigen.

Bij PROOLeiden-Leiderdorp gelden de volgende afspraken voor het gebruik van sociale media:

- Deel op verantwoorde wijze kennis via sociale media, rekening houdend met de goede naam van PROOLeiden-Leiderdorp en iedereen die hierbij betrokken is.
- Maak bij onderwijs gerelateerde onderwerpen duidelijk of publicatie op persoonlijke titel of namens PROOLeiden-Leiderdorp gedaan wordt.
- Publiceer geen vertrouwelijke informatie op sociale media.
- Publiceer geen beeldmateriaal van leerlingen zonder de uitdrukkelijke voorafgaande aantoonbare toestemming van ouders als de leerling jonger is dan 16 jaar, of van de leerling zelf als deze ouder is dan 16 jaar.

- Weet dat publicaties op sociale media altijd vindbaar (openbaar) en moeilijk vernietigbaar zijn. Medewerkers zijn persoonlijk verantwoordelijk voor wat zij publiceren.
- Neem contact op met je leidinggevende als er twijfel bestaat over een publicatie of over de raakvlakken met PROOLeiden-Leiderdorp.
- Het is medewerkers in beginsel niet toegestaan om met een privé account 'vrienden' te worden met leerlingen en ouders op sociale media (uitzondering zijn familiaire of vriendschappelijke relaties, waarbij advies is terughoudend te zijn).
- Inzetten van sociale media in het lesprogramma is gebonden aan de toestemming van ouders als leerlingen jonger zijn dan 16 jaar.

2.10 Gebruik beeld- en geluidsmateriaal

Het gebruiken van beeld- en geluidsmateriaal, het delen van foto's, video's en geluidsfragmenten van leerlingen onder verantwoordelijkheid van PROOLeiden-Leiderdorp mag alleen als daar vooraf toestemming voor gegeven is door de ouder/verzorger. Zonder deze toestemming mogen geen foto's, video's en geluidsfragmenten van leerlingen gebruikt worden.

- PROOLeiden-Leiderdorp verwijst hierbij naar de richtlijn die is opgesteld voor het gebruik en toestemming van beeldmateriaal.
- Voor de afspraken rondom het delen van beeld- en geluidsmateriaal via sociale media gelden tevens de richtlijnen die genoemd worden bij het gebruik van sociale media.

2.11 Wachtwoorden en pincodes

Het beveiligen van toegang tot het netwerk, diverse (online) applicaties en devices (pc, laptop, telefoon) begint met een goed wachtwoord. Een lang wachtwoord of een 'wachtzin' is beter dan een kort, complex wachtwoord. Voor het gebruik van wachtwoorden gelden onderstaande afspraken:

- Wachtwoorden moeten minimaal 8 tekens bevatten, met minstens drie van de volgende vier elementen: kleine letter, hoofdletter, cijfer of speciaal teken (!@#$%^&*().
- Pincodes (op telefoon of tablet) moeten langer zijn dan 4 tekens.
- Sla je wachtwoord niet op in je browser omdat daardoor de beveiliging wegvalt.
- Bij externe diensten wordt het wijzigen van het wachtwoord periodiek afgedwongen. Bij devices en diensten waarbij dit niet het geval is, is het raadzaam om dit ten minste eens per jaar te doen
- Gebruik niet voor elke systeem hetzelfde wachtwoord.
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.

2.12 Meldplicht Datalekken

Van alle medewerkers wordt verwacht dat zij beveiligingsincidenten en mogelijke datalekken melden volgens de procedure meldplicht datalekken van PROOLeiden-Leiderdorp.

3 Controle gebruik bedrijfsmiddelen

PROOLeiden-Leiderdorp handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving, te weten:

- De Grondwet,
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)
- Wet Medezeggenschap Onderwijs (WMO)
- Burgerlijk Wetboek (BW)
- Wetboek van Strafrecht
- Cao PO.

PROOLeiden-Leiderdorp zal bij controle rondom het gebruik van bedrijfsmiddelen op basis van deze gedragscode uitgaan van de juiste balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers.

3.1 Voorwaarden voor controle

- Controle van persoonsgegevens met betrekking tot gebruik van bedrijfsmiddelen vindt slechts plaats in het kader van handhaving van de doelen van deze gedragscode.
- Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen.
- Indien een medewerker of een groep medewerkers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode, in opdracht van PROOLeiden-Leiderdorp gerichte controle plaatsvinden.
- Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van PROOLeiden-Leiderdorp, controle op de inhoud plaats.
- Verboden e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt.
- Bij constatering van ongeoorloofd gebruik wordt dit onmiddellijk met de betrokken medewerker besproken. PROOLeiden-Leiderdorp zal de medewerker op verzoek inzage verschaffen in de gegevens over het eigen gebruik. De medewerker wordt gewezen op de consequenties wanneer niet wordt gestopt met het ongeoorloofd gebruik.
- E-mailberichten van leden van de (G)MR onderling, van vertrouwenspersonen, bedrijfsartsen en van eenieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden in principe niet gecontroleerd. Dit geldt niet voor veiligheid van berichten. Ook hier kan bij zwaarwegende redenen van afgeweken worden.

3.2 Uitvoering van de controle

- De controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van content-filtering.
- De controle op het uitlekken van interne en vertrouwelijke gegevens vindt plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek.
- De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeers- en opslaggegevens.

- De controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.
- De afdeling ict, de systeembeheerder(s) zijn aan geheimhouding gebonden als men 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 PROOLeiden-Leiderdorp worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
- Door PROOLeiden-Leiderdorp worden passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

3.3 Disciplinaire maatregelen

Bij het handelen in strijd met deze gedragscode of de algemeen geldende wettelijke regels, kan het bestuur van PROOLeiden-Leiderdorp, afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen. Hieronder vallen o.a. een waarschuwing/berisping, schadevergoeding, aangifte bij de politie, overplaatsing, schorsing en/of beëindiging van de arbeidsovereenkomst. 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 te reageren op het geconstateerde. Medewerker en leidinggevende maken dan afspraken voor de toekomst en bepalen de mogelijke maatregelen bij overtreding daarvan. Deze afspraken kunnen strenger zijn dan het in deze gedragscode bepaalde. Ook kan de toegang tot e-mail of internet worden beperkt of geheel worden afgesloten. Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens worden getroffen, zoals een constatering van een automatisch filter of blokkade. Er worden geen disciplinaire maatregelen getroffen zonder dat de medewerker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

3.4 Bezwaar en beroep

Als de medewerker het niet eens is met een (voorgenomen) disciplinaire maatregel, dan kan daar in een aantal gevallen bezwaar en/of beroep tegen worden ingesteld. Dit is geregeld in de van toepassing zijnde CAO (thans in artikel 12.1 Commissie van Beroep bijzonder onderwijs).

4 GMR

Dit document heeft betrekking op verwerking van persoonsgegevens en/of controle
van het gedrag of de prestaties van medewerkers. Het medezeggenschapsorgaan (de GMR) is om deze reden instemmingsplichtig. Dit orgaan heeft op 31 maart 2021 ingestemd met de inhoud van deze gedragscode.

De organisatie kan deze gedragscode met instemming van de GMR wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering ervan aan de medewerkers bekend gemaakt.

5 Slotbepaling

Deze regeling wordt jaarlijks geëvalueerd door PROOLeiden-Leiderdorp en de GMR.
De eerstkomende evaluatie vindt plaats medio 2022.