OPENBAAR ONDERWIJS
PRESENT

ICT gedragscode Stichting Openbaar Onderwijs Present

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, chromebook, tablet, telefoon, hardware token (tag).*
- Software (of -systemen): *alle applicaties voor het uitvoeren van de werkzaamheden, zoals de school e-mailomgeving, Office365, administratiesystemen 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 diensten zoals FTP.*

Aan het gebruik van deze bedrijfsmiddelen zijn risico's verbonden, waardoor het noodzakelijk is om hierover afspraken te maken. Van medewerkers van Openbaar Onderwijs Present (schoolbestuur) 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. Onder medewerkers worden niet alleen de mensen verstaan die een dienstverband hebben bij Openbaar Onderwijs Present, maar iedereen die op wat voor manier dan ook werkzaam is bij of voor Openbaar Onderwijs Present, dus ook uitzendkrachten, stagiaires 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 privacygevoelige informatie waaronder persoonsgegevens van het schoolbestuur, haar medewerkers, leerlingen en hun ouders/verzorgers 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/verzorgers
- 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. Openbaar Onderwijs Present zal dan ook de controle en handhaving van deze regels conform de privacywetgeving en het algemene arbeidsrechtelijk kader uitvoeren. Hierbij is het uitgangspunt om zowel een verantwoord gebruik van bedrijfsmiddelen als de bescherming van de privacy van medewerkers op de werkplek te garanderen.

Gegevens worden alleen verzameld en gebruikt voor deze doelen. In het bijzonder zal het schoolbestuur de bij controle vastgelegde gegevens beveiligen tegen ongeautoriseerde toegang. Het schoolbestuur 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. Daarbij garandeert het schoolbestuur dat bij geautomatiseerd controleren of filteren zij zichzelf en andere personen geen inzage geeft in het gedrag van individuele personen.

1.2 Eigen verantwoordelijkheid en privégebruik

Het gebruik van door Openbaar Onderwijs Present verstrekte bedrijfsmiddelen is persoonlijk en blijft de verantwoordelijkheid van de medewerker. Alle devices die voor werk worden gebruikt (inclusief eigen devices) worden niet uitgeleend of aan anderen ter beschikking gesteld zonder aanvullende (beveiligings)maatregelen. Alle devices die voor werk worden gebruikt dienen te zijn voorzien van een wachtwoord of pincode. Het niet voldoen aan de regels voor informatiebeveiliging en privacy kan leiden tot disciplinaire maatregelen.

1.3 Verschillende soorten gegevens

Openbaar Onderwijs Present is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en privacy is het beschermen van gegevens.
Openbaar Onderwijs Present 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 Openbaar Onderwijs Present bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
- **Vertrouwelijke gegevens**; dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen Openbaar Onderwijs Present 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, emailadressen maar ook telefoonnummers van zowel collega's als leerlingen en ouders/verzorgers van leerlingen.

De privacywetgeving verplicht elk individu om zorgvuldig met persoonsgegevens om te gaan. Een onderdeel van de wettelijke verplichting is dat Openbaar Onderwijs Present schriftelijk afspraken maakt met leveranciers van (online)applicaties, waarbij persoonsgegevens worden verwerkt (denk hierbij aan inloggegevens, wachtwoorden en het opslaan van gemaakt werk).
Openbaar Onderwijs Present heeft een Functionaris voor gegevensbescherming aangesteld. Deze communiceert intern de gedragsregels die horen bij het verwerken van persoonsgegevens. 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.[1] Een dergelijk incident kan schadelijke gevolgen hebben voor de betrokkene(n) en Openbaar Onderwijs Present.

[1] **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
Datalek; een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt
(opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle
beveiligingsincidenten zijn datalekken. Een klassiek voorbeeld van een datalek is een hack waarbij een database

Om op een veilige, verantwoorde en werkbare manier met deze gegevens om te gaan maakt Openbaar Onderwijs Present 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 Openbaar Onderwijs Present toegestane bedrijfsmiddelen. Onder toegestane bedrijfsmiddelen wordt verstaan; laptops uitgegeven door Openbaar Onderwijs Present en persoonlijke apparaten die voldoen aan de in dit document gestelde beveiligingsmaatregelen.

Van medewerkers van Openbaar Onderwijs Present en/of externe medewerkers, die uit hoofde van hun functie toegang hebben tot de digitale informatiesystemen en hiermee tot bv. personeelsdossiers, vertrouwelijke enquêtegegevens, zorgdossiers et cetera wordt verwacht dat zij zorgvuldig omgaan met de functioneel aan hen beschikbaar gestelde informatie. Dit betekent dat zij de privacywetgeving hanteren en op geen enkele wijze informatie, waarvan redelijkerwijs 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 Openbaar Onderwijs Present 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 minimaal aan de volgende algemene normen voor ‘zorgvuldigheid’:

- Ga zorgvuldig om met persoonsgegevens, waarbij de basisregels voor het omgaan met persoonsgegevens als bekend worden verondersteld.
- Voorkom het lekken van interne en vertrouwelijke informatie.
- Zorg voor een goede fysieke en technische bescherming van bedrijfsmiddelen. Laat bedrijfsmiddelen nooit onbeheerd achter (bijvoorbeeld in de auto) en beveilig bedrijfsmiddelen altijd met een wachtwoord of pincode.
- Voorkom dat beveiligingsmaatregelen moedwillig worden omzeild (bijvoorbeeld door jailbreaks).

- Meld diefstal of verlies van bedrijfsmiddelen onmiddellijk na constatering bij de (school)directie of via een telefonische melding bij de daarvoor aangewezen persoon.

2.2 Computergebruik

Voor het uitoefenen van de werkzaamheden stelt Openbaar Onderwijs Present 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.

---

met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop de adresgegevens van
groep 3b, is ook een datalek.

- 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 werkzaamheden.
- Sla (persoons)gegevens alleen op de daarvoor aangewezen systemen op en versleutel deze waar mogelijk.
- Deel wachtwoorden/pincodes nooit, ook niet incidenteel. Wachtwoorden/pincodes zijn persoonlijk.
- Sluit na gebruik de computer af of log uit.
- Laat geen andere personen werken op jouw account.
- Meld storingen van beheerde werkplekken (computer of laptop) bij de daartoe aangewezen persoon binnen jouw organisatie.
- Wanneer een eigen device wordt gebruikt (zoals een smartphone) voor zakelijke doeleinden, meld verlies of diefstal dan zo snel mogelijk bij jouw directeur en geef duidelijk aan welke accounts gekoppeld zijn aan het eigen device.

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 jouw device.
- Verwijder interne en vertrouwelijke documenten van het bureau bij het voor langere tijd verlaten van de werkplek (denk hieraan bij het bijwonen van een vergadering).
- Voorkom dat gevoelige en vertrouwelijke informatie zichtbaar is wanneer iemand anders op het beeldscherm (of via een beamer) mee kan kijken.
- Als iemand mee kan kijken, sluit dan het e-mail programma af en zorg voor een opgeruimd digitaal bureaublad.
- Het printen van documenten voorzien van persoonsgegevens dient te gebeuren middels uitgesteld printen dmv pincode, of de opdracht tot printen wordt gegeven als je naast de printer staat (indien er sprake is van een draagbaar device). Als dit niet mogelijk is, haal dan de afdrukken direct na het geven van de printopdracht op bij de printer.
- Haal overbodig geworden papieren documenten met persoonsgegevens erop altijd door de papierversnipperaar, ook wanneer je deze documenten op een andere locatie dan de werkplek gebruikt.

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 altijd gemeld moeten worden volgens het Protocol informatiebeveiligingsincidenten en datalekken van Openbaar Onderwijs Present (zie 2.12). Dit protocol is voor medewerkers van Openbaar Onderwijs Present in te zien op www.openbaaronderwijspresent.nl

2.4 Gebruik eigen devices

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor Openbaar Onderwijs Present worden uitgevoerd. Openbaar Onderwijs Present is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen van de school. Openbaar Onderwijs Present stelt deze aldus beveiligde bedrijfsmiddelen / devices beschikbaar voor de werknemer.
Indien de werknemer ervoor kiest om (ook) één of meer eigen devices te gebruiken waarmee werkzaamheden voor Openbaar Onderwijs Present worden uitgevoerd dan is het belangrijk te onderkennen dat het gebruik en de beveiliging van deze device(s) onder de eigen verantwoordelijkheid van de werknemer valt. Hij of zij wordt geacht om op een verstandige manier met zakelijke informatie om

te gaan. Als er schade ontstaat die veroorzaakt is door de medewerkers dan ligt het risico daarvan bij de werknemer als er sprake is van grove nalatigheid (bijvoorbeeld bij bewust lekken van informatie).
Belangrijke richtlijnen in dit verband zijn:

- Ga verstandig om met schoolgerelateerde informatie.
- Haal informatie niet naar je device toe maar sla het op in de cloud.

Neem daarnaast in elk geval de volgende beveiligingsmaatregelen:

- Beveilig het device met een wachtwoord of, in het geval van een smartphone of tablet, met een pincode die langer is dan 4 tekens (tenzij er maar 4 tekens mogelijk zijn).
- Vergrendel het device bij het verlaten van de werkplek.
- Het is niet toegestaan persoonsgegevens van Openbaar Onderwijs Present en gegevens over Openbaar Onderwijs Present op het eigen device op te slaan.
- Scheid (versleutelde)gegevens, anders dan persoonsgegevens, van Openbaar Onderwijs Present en privégegevens (bijvoorbeeld gmail) 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.
- Meld verlies of diefstal van eigen devices die gekoppeld zijn aan een zakelijk account altijd bij de directie.

Openbaar Onderwijs Present mag controles uitvoeren op bovenstaande maatregelen, na verkregen toestemming van de medewerker. Op verzoek van Openbaar Onderwijs Present moet de medewerker zelf aantonen dat de bovenstaande maatregelen worden toegepast, voor zover dit wettelijk is toegestaan.

2.5 Software en digitaal lesmateriaal

Het gebruik van digitaal lesmateriaal is niet meer weg te denken bij Openbaar Onderwijs Present. Dit lesmateriaal staat uitsluitend 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:

- Gebruik van online software wordt bij Openbaar Onderwijs Present 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 Openbaar Onderwijs Present persoonsgegevens verwerkt. Regel dit vooraf aan het gebruik.
- Volg bij het aanvragen van digitaal lesmateriaal en/of andere software de bij Openbaar Onderwijs Present afgesproken aanvraagprocedure. Hiervoor is een aanvraagformulier beschikbaar wat als uitgangspunt dient voor eventuele wettelijk verplichte aanvullende privacy- en/of beveiligingsmaatregelen.

2.6 Gebruik van e-mail

Openbaar Onderwijs Present 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 zakelijke e-mailadres uitsluitend voor werkgerelateerde zaken.
- Gebruik voor versturen en ontvangen van privé e-mail een eigen privé e-mailadres via een externe webmaildienst (bijvoorbeeld webmail van Gmail, Hotmail of een eigen provider).

- Het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie.
- 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 en geweld.
- Synchroniseert een medewerker de school e-mail met een eigen device (tablet, telefoon) dan kan Openbaar Onderwijs Present, bij verlies of diefstal van het device, gebruik maken van de mogelijkheid om het zakelijke account te blokkeren en als maatregel een nieuw wachtwoord regelen.

2.7 Gebruik van internet

Openbaar Onderwijs Present 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:

- Beperkt 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
  - 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.
  - 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.

Openbaar Onderwijs Present verwacht van medewerkers dat zij:

- het onderscheid kennen tussen veilige en onveilige netwerken (openbare wifi netwerken) 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 Openbaar Onderwijs Present
- 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 Openbaar Onderwijs Present netwerk is, eduroam of het eigen (beveiligde) 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 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 social 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 afwijkt van het offline gedrag binnen de school / organisatie. Medewerkers moeten zich realiseren dat zij, ook als zij online een privé

mening verkondigen, altijd kunnen worden gezien als vertegenwoordigers van Openbaar Onderwijs Present.
Bij Openbaar Onderwijs Present gelden de volgende afspraken voor het gebruik van sociale media:

- Onder werktijd gebruik je sociale media uitsluitend voor werkgerelateerde zaken.
- Deel op verantwoorde wijze kennis via sociale media rekening houdend met de goede naam van Openbaar Onderwijs Present en iedereen die hierbij betrokken is.
- Maak bij onderwijs gerelateerde onderwerpen duidelijk of publicatie op persoonlijke titel of namens Openbaar Onderwijs Present gedaan wordt.
- Publiceer geen vertrouwelijke informatie op sociale media.
- Publiceer of gebruik geen beeldmateriaal van leerlingen zonder de uitdrukkelijke voorafgaande aantoonbare toestemming van ouders/verzorgers.
- Weet dat publicaties op sociale media altijd vindbaar (openbaar) en moeilijk vernietigbaar zijn. Medewerkers zijn persoonlijk verantwoordelijk voor wat zij publiceren.
- Neem vooraf contact op met een leidinggevende als er twijfel bestaat over een publicatie of over de raakvlakken met Openbaar Onderwijs Present.
- Het is medewerkers niet toegestaan om met een privé account ‘vrienden’ te zijn met leerlingen op sociale media.

2.10 Gebruik beeld- en geluidsmateriaal

Het gebruiken van beeld- en geluidsmateriaal, het delen van foto's, video's en geluidsfragmenten van leerlingen door medewerkers vallend onder Openbaar Onderwijs Present mag alleen als daar vooraf toestemming voor gegeven is door ouders/verzorgers. Zonder deze toestemming mogen geen foto's, video's en geluidsfragmenten van leerlingen gebruikt worden.

- Openbaar Onderwijs Present 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 de richtlijnen die genoemd worden bij het gebruik van sociale media.
- Foto’s, video’s en geluidsfragmenten van collega’s mogen alleen gebruikt worden wanneer de betreffende collega hiervoor mondelinge en/of schriftelijke toestemming heeft gegeven.

2.11 Wachtwoorden en pincodes

Het beveiligen van toegang tot het netwerk, diverse (online) applicaties en devices (pc, chromebook, 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, tenzij er maar 4 tekens mogelijk zijn.
- Wachtwoorden moeten volgens de afspraken binnen Openbaar Onderwijs Present op aangegeven tijden vervangen worden.
- Gebruik niet voor elke systeem hetzelfde wachtwoord.
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.
- Zorg ervoor dat anderen jouw wachtwoorden niet kunnen vinden of achterhalen

2.12 Meldplicht beveiligingsincidenten en datalekken

Van alle medewerkers wordt verwacht dat zij beveiligingsincidenten en mogelijke datalekken melden volgens het Protocol informatiebeveiligingsincidenten en datalekken van Openbaar Onderwijs Present.

3 Controle gebruik bedrijfsmiddelen

Openbaar Onderwijs Present handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving, te weten:

- De Grondwet
- Algemene Verordening Gegevensbescherming
- Wet Medezeggenschap Scholen (WMS)
- Burgerlijk Wetboek (BW)
- Wetboek van Strafrecht
- Cao PO

Openbaar Onderwijs Present 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 Openbaar Onderwijs Present gerichte controle plaatsvinden.
- Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van Openbaar Onderwijs Present, 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 door de leidinggevende. Openbaar Onderwijs Present 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 GMR onderling, van vertrouwenspersonen, bedrijfsartsen en van een ieder 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.
- 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 systeembeheerder(s) is / 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 Openbaar Onderwijs Present worden de nodige maatregelen getroffen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.

- Door Openbaar Onderwijs Present 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 Openbaar Onderwijs Present, 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 de leidinggevende bepaalt de mogelijke maatregelen bij overtreding daarvan. Deze afspraken kunnen strenger zijn dan het in deze gedragscode bepaalde. Ook kan de toegang tot school of zakelijk e-mail of internet worden beperkt of geheel worden afgesloten. Indien er sprake is van een langs geautomatiseerde weg uitgevoerde actie (bijv. als gevolg van een automatisch filter, blokkade of automatisch ingestelde doorstuurservice) die onbedoeld leidt tot verwerking van persoonsgegevens wordt er geen disciplinaire maatregel opgelegd, en kan er wel een waarschuwing worden gegeven. Het voorval kan geanonimiseerd worden gebruikt om de bewustwording onder medewerkers te vergroten en om (desgewenst) processen aan te scherpen.

3.4 Bezwaar en beroep

Als de medewerker het niet eens is met de (voorgenomen) disciplinaire maatregel, dan kan daartegen op grond van de vigerende wet - en/of regelgeving bezwaar c.q. beroep worden ingesteld.

4 GMR

Dit document heeft betrekking op verwerking van persoonsgegevens en/of controle van het gedrag of de prestaties van medewerkers. De personeelsgeleding van de GMR heeft om deze reden instemmingsrecht. De personeelsgeleding van de GMR heeft op 10 oktober 2019 ingestemd met deze ICT gedragscode Openbaar Onderwijs Present.

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

5 Slotbepaling

Deze regeling kan worden aangehaald als ICT Gedragscode Openbaar Onderwijs Present, is op 16 oktober 2019 vastgesteld door de voorzitter van het College van Bestuur en treedt in werking per 1 november 2019.

Deze regeling wordt bekend gemaakt aan de medewerkers via de website van Present: www.openbaaronderwijspresent.nl

Deze regeling wordt tweejaarlijks geëvalueerd door Openbaar Onderwijs Present en de GMR. De eerstkomende evaluatie vindt plaats in mei 2021.