

Gedragcode InformatieBeveiliging en Privacy (IBP)



Samenwerkingsverband

Passend Onderwijs VO 2801

*Voorschoten Wassenaar Leiderdorp Zoeterwoude
Oegstgeest Leiden Kaag en Braassem*

Bron

Kennisnet

Bewerkt door:

Stichting Samenwerkingsverband Passend Onderwijs VO 2801

Versie	Status	Datum	Auteur	Omschrijving
1.1	1 ^e concept	15-3-2019	M. v. Diggele	1 ^e concept ter bespreking

Vastgesteld door:

Stichting Samenwerkingsverband Passend Onderwijs VO 2801

Versie	Datum	Naam	Functie
1.1	09-04-2019	Frits Hoekstra	Bestuursvoorzitter

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 zakelijke werkzaamheden.

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 het samenwerkingsverband. 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: 'MR' laat de rol van de MR zien.

Hoofdstuk 5: 'Slotbepaling' toont de datum van de eerstvolgende evaluatie en eventuele aanpassing van de gedragscode.

Inhoudsopgave

1	Inleiding	4
1.1	Uitgangspunten gedragscode.....	4
1.2	Eigen verantwoordelijkheid en privégebruik	5
1.3	Verschillende soorten gegevens.....	5
2	Gedragscode.....	7
2.1	Algemene normen.....	7
2.2	Computergebruik	7
2.3	Werkplek	7
2.4	Gebruik eigen devices (BYOD).....	8
2.5	Software en digitaal lesmateriaal.....	8
2.6	Gebruik van e-mail	9
2.7	Gebruik van internet	9
2.8	Veilig online	10
2.9	Sociale media.....	10
2.10	Gebruik beeld- en geluidsmateriaal	11
2.11	Wachtwoorden en pincodes	11
2.12	Meldplicht Datalekken	11
3	Controle gebruik bedrijfsmiddelen	12
3.1	Voorwaarden voor controle	12
3.2	Uitvoering van de controle.....	12
3.3	Disciplinaire maatregelen.....	13
3.4	Bezwaar en beroep.....	13
4	MR	Fout! Bladwijzer niet gedefinieerd.
5	Slotbepaling.....	13

1 Inleiding

Het gebruik van internet, computernetwerk, en e-mail is voor alle medewerkers van het samenwerkingsverband 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 zakelijke 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 Samenwerkingsverband Passend Onderwijs VO 2801 (hierna genoemd: het samenwerkingsverband) wordt verwacht dat zij verantwoord omgaan met de beschikbaar gestelde bedrijfsmiddelen. Dit wordt ook verwacht als medewerkers hun eigen middelen inzetten om werkzaamheden voor het samenwerkingsverband uit te voeren.

De afspraken in dit document gelden voor alle locaties van waaruit werkzaamheden worden verricht en voor alle devices waarmee het werk wordt uitgevoerd. Ze gelden voor iedereen die werkzaam is bij het samenwerkingsverband, 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 bestuur van het samenwerkingsverband, 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 bestuur, haar medewerkers, leerlingen en hun ouders
- het voorkomen en tegengaan van misbruik van de bedrijfsmiddelen
- de bescherming van de intellectuele eigendomsrechten van het bestuur 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 samenwerkingsverband 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 bestuur 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 het samenwerkingsverband verstrekte bedrijfsmiddelen is persoonlijk en blijft de verantwoordelijkheid van de medewerker. Alle devices die voor werk 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

het samenwerkingsverband is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en privacy is het beschermen van gegevens.

het samenwerkingsverband 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 het samenwerkingsverband bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
- **Vertrouwelijke gegevens;** dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen het samenwerkingsverband 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 van leerlingen.

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

Om op een veilige, verantwoorde en werkbare manier met deze gegevens om te gaan maakt het samenwerkingsverband 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 het samenwerkingsverband goedgekeurde bedrijfsmiddelen.

Van medewerkers van het samenwerkingsverband 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. 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 het samenwerkingsverband 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 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 incidentenmelding via Topdesk of een telefonische melding bij de daarvoor aangewezen persoon (zie hiervoor de Protocol Informatiebeveiligingsincidenten van het samenwerkingsverband).
- Indien er vrijwilligers worden ingezet binnen het samenwerkingsverband 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.

2.2 Computergebruik

Voor het uitoefenen van de werkzaamheden stelt het samenwerkingsverband 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 werkzaamheden.
- 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 de netwerkschijf op of in One Drive (beveiligde cloudomgeving).
- Versleutel alle gegevens met betrekking tot het samenwerkingsverband, 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) bij de ICT-coördinator

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-mail programma af en zorg voor een opgeruimd digitaal bureaublad.
- Laat geen afdrucken 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 locatie 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 het samenwerkingsverband.

2.4 Gebruik eigen devices (BYOD)

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

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 email of andere zakelijke toepassingen op het device (bijv. gebruik door anderen binnen gezin, verlies of diefstal)
- Voor gebruik van toepassingen van het samenwerkingsverband op het device is vooraf toestemming van de directeur vereist
- Vergrendel het device bij het verlaten van de werkplek (windowstoets+L).
- Sla persoonsgegevens van het samenwerkingsverband niet op het eigen device op; dit is niet toegestaan.
- Versleutel alle gegevens, anders dan persoonsgegevens, met betrekking tot het samenwerkingsverband als deze, om welke reden dan ook, niet op het netwerk 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 van je zakelijke account.

- Scheid (versleutelde)gegevens, anders dan persoonsgegevens, van het samenwerkingsverband 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.

het samenwerkingsverband mag controles uitvoeren op bovenstaande maatregelen. Op verzoek van het samenwerkingsverband 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 het samenwerkingsverband. 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 het samenwerkingsverband 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 het samenwerkingsverband persoonsgegevens verwerkt. Verwerkersovereenkomst dient door bestuur ondertekend te worden.
- Aanvragen van digitaal lesmateriaal en/of andere software volgt bij het samenwerkingsverband de afgesproken aanvraagprocedure.

2.6 Gebruik van e-mail

het samenwerkingsverband 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 persoonlijke e-mail adres van het samenwerkingsverband alleén voor zaken die aan het samenwerkingsverband gerelateerd zijn.
- Gebruik voor privé e-mail een eigen privé e-mailadres via een externe webmaildienst. (bijvoorbeeld webmail van Gmail, Hotmail of een eigen provider).
- Ontvangen van privémail op het zakelijke e-mailadres is slechts incidenteel toegestaan.
- Het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie.
- Persoonsgegevens mogen alleen versleuteld worden gemaïld, 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 mailbox periodiek (bijv. maandelijks) op middels shift-delete (zodat deze ook niet in de verwijderde items blijft staan)

2.7 Gebruik van internet

het samenwerkingsverband 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 leestijd 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 het samenwerkingsverband verbonden betrokkenen en activiteiten. Dit geldt in het bijzonder ook voor internetgebruik buiten het netwerk van het samenwerkingsverband met betrekking tot aan het samenwerkingsverband 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.

het samenwerkingsverband 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 het samenwerkingsverband
- 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 het samenwerkingsverband 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 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 real life gedrag binnen het samenwerkingsverband. Medewerkers zijn altijd de vertegenwoordiger van het samenwerkingsverband ook als zij online een privémening

verkondigen. Bij het samenwerkingsverband 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 het samenwerkingsverband en iedereen die hierbij betrokken is.
- Maak bij onderwijs gerelateerde onderwerpen duidelijk of publicatie op persoonlijke titel of namens het samenwerkingsverband 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 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 het samenwerkingsverband.
- Het is medewerkers in beginsel niet toegestaan om met een privé account 'vrienden' te worden met leerlingen en ouders op sociale media (uitzondering zijn familiale 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 het samenwerkingsverband 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.

- het samenwerkingsverband 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
- Wachtwoorden moeten regelmatig vervangen worden.
- 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 het samenwerkingsverband.

3 Controle gebruik bedrijfsmiddelen

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

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

het samenwerkingsverband 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 het samenwerkingsverband gerichte controle plaatsvinden.
- Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van het samenwerkingsverband, 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. het samenwerkingsverband 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 MR 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 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 het samenwerkingsverband worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
- Door het samenwerkingsverband 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 het samenwerkingsverband, 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.

4 MR

Dit document heeft betrekking op verwerking van persoonsgegevens en/of controle van het gedrag of de prestaties van medewerkers. Het medezeggenschapsorgaan (de MR) is om deze reden instemmingsplichtig. Dit orgaan heeft op 28 maart 2019 ingestemd met de inhoud van deze gedragscode.

De organisatie kan deze gedragscode met instemming van de MR 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 het samenwerkingsverband en de MR. De eerstkomende evaluatie vindt plaats in maart 2020.