****

**GEDRAGSCODE**

**Samenwerkingsverband Brabantse Wal PO**

**Vastgesteld door Samenwerkingsverband Brabantse Wal PO**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Naam** | **Functie** |
| 1.0 | 10.02.2021  10.02.2021 | Mevr. H. Persoon  Mevr. P. Pellis | Directeur-bestuurder  Voorzitter OPR |
| 2.0 | 23.01.2023 | Mevr. H. Persoon | Directeur-bestuurder |
|  | 23.01.2023 |  | Voorzitter OPR |

|  |
| --- |
| **Inleiding**  Sinds 25 mei 2018 is de AVG van kracht, de Algemene Verordening Gegevensbescherming. Deze Europese privacywet waarborgt de zorgvuldige omgang met persoonsgegevens.  Dit zijn gegevens die een persoon betreffen én waardoor een persoon identificeerbaar is. Denk hierbij aan naamgegevens, emailadressen en telefoonnummers van leerlingen en van ouders van leerlingen, maar ook van de medewerkers van Samenwerkingsverband passend onderwijs Brabantse Wal PO (‘het samenwerkingsverband’).  Vanzelfsprekend vinden we het belangrijk dat er zorgvuldig wordt omgegaan met de persoonlijke gegevens en de (ICT-)faciliteiten die aan onze zorg zijn toevertrouwd. Vanuit de AVG zijn hier duidelijke kaders voor geschetst en zijn er eisen gesteld waaraan het samenwerkingsverband moet voldoen.  Maar nog belangrijker dan alles ‘op papier’ te regelen, is de eigen bewustwording van jou als medewerker hoe je omgaat met persoonsgegevens.  In deze gedragscode is beknopt en kernachtig weergegeven welke aspecten bijzondere aandacht vragen bij het omgaan met de gegevens van leerlingen, ouders, scholen.  Ook zijn in deze gedragscode afspraken opgenomen welke we hanteren als het gaat om gebruik van onze werkplek en de toegang hiertoe.  Ik vraag je dan ook deze gedragscode goed te lezen en hier op een juiste wijze invulling aan te geven.    Hellen Persoon  Directeur-bestuurder  SWV Brabantse Wal PO |

|  |  |
| --- | --- |
| U:\tekening paraplu.png | **Eigen verantwoordelijkheid**  Het gebruik van de door het samenwerkingsverband beschikbaar gestelde bedrijfsmiddelen is persoonlijk en blijft de verantwoordelijkheid van de medewerker. Alle apparatuur/devices die door de werkgever ter beschikking werden gesteld en voor het werk worden gebruikt, worden niet uitgeleend of aan anderen ter beschikking gesteld. Wanneer bij werknemer de intentie bestaat om eigen apparatuur/devices, die eveneens voor het werk worden gebruikt en waarop mogelijk persoonsgegevens staan dan wel in te zien zijn, aan een derde uit te lenen, dan dient de medewerker vooraf met de werkgever te overleggen over eventueel benodigde (beveiligings)maatregelen.  Het samenwerkingsverband verwacht van zijn 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, dit kunnen herkennen en weten hoe te handelen. * Terughoudend zijn met het online achterlaten van gegevens. * Controleren of er daadwerkelijk van een bekend én beveiligd netwerk gebruik gemaakt wordt bij het bezoek aan openbare ruimtes. |

|  |  |
| --- | --- |
|  | **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 geacht. * 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 (bijvoorbeeld door jailbreaks). * Meld diefstal of verlies van bedrijfsmiddelen onmiddellijk na constatering hiervan door telefonisch de directeur-bestuurder en/of de beleidsadviseur(s) kwaliteitszorg te informeren of, bij geen gehoor, een e-mail te sturen aan [privacy@swvbrabantsewal.nl](mailto:privacy@swvbrabantsewal.nl) (zie ook het protocol datalekken). |
|  |  |

|  |  |
| --- | --- |
| U:\tekening slotje.png | **Wachtwoorden zijn persoonlijk en geheim**  In verband met beveiliging én data-integriteit, zijn wachtwoorden strikt persoonlijk.   * Zorg dat je de enige bent die jouw wachtwoorden kent. Deel wachtwoorden nooit, ook niet incidenteel. * Wijzig je wachtwoord wanneer een ander het zou kunnen weten. * Wachtwoorden moeten volgens de (n.t.b.) afspraken binnen het samenwerkingsverband op aangegeven tijden vervangen worden. * Beveilig het apparaat met een wachtwoord, of in het geval van een smartphone of tablet, met een pincode die bij voorkeur langer is dan 4 tekens. * Gebruik niet voor elke systeem hetzelfde wachtwoord. * Wachtwoorden moeten minimaal 9 tekens bevatten, met minstens drie van de volgende vier elementen: kleine letter, hoofdletter, cijfer of speciaal teken (!@#$%^&\*() |
|  |  |

|  |  |
| --- | --- |
|  |  |
|  | **Toegang kantoorgebouw Rijtuigweg (met tag/sleutel)**  De vaste medewerkers hebben een tag en sleutel van het kantoorgebouw. De tag staat op naam en registreert wie in het gebouw aanwezig is (t.b.v. BHV bij calamiteiten).   * Met de tag- open je de toegangsdeur en meld je je automatisch aan in het gebouw. * Afmelden wanneer je het gebouw verlaat, gaat via de tag-console op de benedenverdieping. * Sleutel is van toegangsdeur naar eerste verdieping, laatste op de verdieping draait de deur op slot. * Toegang vanaf 06.00 uur ’s ochtends tot uiterlijk 22.30 uur ’s avonds. * Verlies van sleutel melden bij directeur-bestuurder of beleidsmedewerker. * Verlies van tag dient direct gemeld te worden aan Fluor   [Bergenopzoom.reception@fluor.com](mailto:Bergenopzoom.reception@fluor.com) en [laura.knopper@fluor.com](mailto:laura.knopper@fluor.com)  (office service specialist). Zij kunnen de tag blokkeren en eventueel vervangen.  Het vervangen van tag/sleutel en (waar nodig) sloten brengt kosten met zich mee en kunnen in rekening worden gebracht bij de werknemer. |
|  |  |
|  |  |
| U:\tekening bureau.jpg | **Gebruik werkplek/kantoorruimte en meld storingen**   * Sluit na gebruik de computer of laptop af of log uit. * Vergrendel je computer of laptop wanneer je de werkplek tussentijds verlaat. * Meld storingen van beheerde werkplekken (computer of laptop) bij de ICT-leverancier. * Verwijder interne en vertrouwelijke documenten van het bureau wanneer je langere tijd je werkplek verlaat, bijvoorbeeld voor een vergadering. * 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. * Doe kasten met privacygevoelige gegevens op slot bij het verlaten van je werkplek. * Zorg dat ramen en deuren gesloten zijn als je als laatste vertrekt. * Laat bezoekers zich melden bij de receptie en begeleid hen wanneer ze vertrekken. |

|  |  |
| --- | --- |
| U:\tekening dossier.jpg | **Papieren documenten**   * Zorg ervoor dat je zo min mogelijk papieren versies van persoonsgegevens hebt. * Print met een wachtwoord, zodat er geen afdrukken bij de printer kunnen liggen. * Laat geen afdrukken bij de printer liggen, zeker niet als er persoonsgegevens op staan. * Haal overbodig geworden papieren documenten met persoonsgegevens altijd door de papierversnipperaar. Deponeer dit soort documenten niet bij het oud papier. * Ook 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. Meld een datalek conform het protocol datalekken. |

|  |  |
| --- | --- |
| U:\tekening usb.jpg | **Persoonsgegevens op goedgekeurde plaatsen**  Gegevens over leerlingen moeten zorgvuldig beschermd worden en mogen alleen op afgesproken plaatsen vastgelegd worden.   * Sla persoonsgegevens van het samenwerkingsverband niet op het eigen thuisapparaat op; dit is niet toegestaan. * Sla persoonsgegevens alleen op de daarvoor aangewezen plaatsen op. Opslaan van gegevens in public cloud omgevingen, zoals een persoonlijke dropbox, is niet toegestaan. * Versleutel alle gegevens met betrekking tot het samenwerkingsverband indien deze gegevens, om welke reden dan ook, elders opgeslagen worden.   **USB-sticks zijn uitdrukkelijk verboden voor opslag van persoonsgegevens!** |
|  | **Persoonsgegevens beveiligd delen**   * Persoonsgegevens mogen alleen het samenwerkingsverband verlaten wanneer daar een wettelijk geldige reden of expliciete toestemming (handtekening) van de betrokkene voor is. * E-mail is niet geschikt voor het beveiligd versturen van vertrouwelijke informatie. Gebruik hiervoor L-DOS. * Wanneer je documenten per e-mail verstuurt, zorg je dat het bestand beveiligd is met een wachtwoord. En gebruik voor het versturen van (vertrouwelijke) gegevens aan collega’s binnen het samenwerkingsverband altijd het emailadres van het samenwerkingsverband. * Bewaar geen persoonsgegevens in je mailbox. |

|  |  |
| --- | --- |
|  | **Wees extra zorgvuldig met bijzondere persoonsgegevens**  Gezondheid en levensbeschouwing (religie) zijn voorbeelden van bijzondere persoonsgegevens. Deze gegevens zijn extra beschermd.  Het Burgerservicenummer (BSN) mag alleen in zéér specifieke situaties gebruikt worden. Hier moet een wettelijke grondslag voor zijn. |

|  |  |
| --- | --- |
| U:\tekening transparant.jpg | **Wees transparant**  Ouders hebben het recht om te weten welke gegevens het samenwerkingsverband over het kind heeft opgeslagen. De AVG biedt ouders ook de mogelijkheid om een kopie van het dossier op te vragen*.*   * Formuleer uitsluitend feitelijke informatie in de daarvoor aangewezen systemen. * Noteer niet meer dan noodzakelijk is voor de begeleiding van de leerling. * Wees helder naar betrokkenen over welke gegevens worden opgeslagen. |

|  |  |
| --- | --- |
|  | **Thuisdevices / apparatuur**  Op privéapparatuur mogen vanzelfsprekend geen leerlingengegevens staan. voor eigen devices/apparaten ligt de verantwoordelijkheid POor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:   * Sla persoonsgegevens van het samenwerkingsverband niet op het eigen apparaat op. * Laat wachtwoorden niet automatisch onthouden. * 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. * Beveilig het apparaat met een wachtwoord, of in het geval van een smartphone of tablet, met een pincode die langer is dan 4 tekens. * Vergrendel het apparaat bij het verlaten van de werkplek. * Sla persoonsgegevens in beheer van het samenwerkingsverband niet op het eigen apparaat op; dit is niet toegestaan. Verwijder documenten die persoonsgegevens bevatten en die automatisch opgeslagen worden (bijvoorbeeld bij het openen van een bestand in een e-mail). * Scheid (versleutelde) gegevens, anders dan persoonsgegevens, van het samenwerkingsverband en privégegevens van elkaar. Deze scheiding moet duidelijk herkenbaar zijn op het eigen apparaat. |

|  |  |  |
| --- | --- | --- |
|  | ***Email/internetgebruik***  Het samenwerkingsverband stelt een e-mailsysteem, internet 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 gaat uit van de volgende afspraken:   * Gebruik het Brabantse Wal-adres *alléén vo*or werkgerelateerde zaken. * Gebruik voor privé e-mail een eigen privé e-mailadres via een externe web maildienst. * Stel de e-mailapp op de mobiele telefoon en computer/laptop zo in dat er geen leesbare pop-ups verschijnen. * Reageer nooit op mails waarin gevraagd wordt om wachtwoorden of persoonlijke gegevens. Meld een phishingmail altijd via privacy@swvbrabantsewal.nl en de Functionaris voor Gegevensbescherming. * Het ontvangen van privémail op het werkmailadres is incidenteel toegestaan, mits dit de dagelijkse werkzaamheden niet stoort en niet voor commerciële of verboden doeleinden is. * Het is vanzelfsprekend 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. * Het is eveneens niet toegestaan om op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten; om films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron; en om deel te nemen aan kansspelen. * Synchroniseert een medewerker van het samenwerkingsverband de e-mailvoorziening met een eigen apparaat (tablet, laptop, pc, telefoon) dan kan Samenwerkingsverband Brabantse Wal PO bij verlies of diefstal van het apparaat gebruik maken van de mogelijkheid **om de e-mail op afstand te wissen, ook als daarmee alle (privé)gegevens van het apparaat gewist worden**. De inschatting van de noodzaak hiertoe is ter beoordeling van de directeur-bestuurder van het samenwerkingsverband. Indien het de directeur-bestuurder zelf is die een gesynchroniseerd apparaat verliest of als diens gesynchroniseerde apparaat gestolen wordt, dan informeert de directeur-bestuurder dan wel de beleidsmedewerker kwaliteitszorg de intern toezichthouder hieromtrent en is het aan de inschatting van laatstgenoemde **om de e-mail op afstand te wissen, ook als daarmee alle (privé)gegevens van het apparaat gewist worden.** * Bij afwezigheid van de medewerker kan de directeur-bestuurder besluiten de mailbox van die betreffende medewerker te laten openen om lopende zaken, wanneer dit door de directeur-bestuurder noodzakelijk wordt geacht en als zodanig gemotiveerd, voortgang te kunnen bieden. Wanneer het de directeur-bestuurder zelf is die afwezig is, waardoor knelpunten in de voortgang van de werkzaamheden van het samenwerkingsverband te voorzien zijn of ontstaan, informeert de beleidsmedewerker kwaliteitszorg de intern toezichthouder hieromtrent en is het aan de inschatting van laatstgenoemde om te besluiten over noodzaak (en zodanig gemotiveerd) tot opening van de mailbox van de afwezige directeur-bestuurder. * Bij het vermoeden van misbruik van een van bovenstaande punten, kan de directeur-bestuurder ook besluiten de mailbox te openen. Hier ligt dan een gemotiveerd besluit aan ten grondslag. | |
|  | |  |

|  |  |
| --- | --- |
|  | ***Ruim op!***  Als organisatie mag je persoonsgegevens niet langer bewaren dan noodzakelijk (en alleen op goedgekeurde plaatsen).  **Bewaartermijn Leerlinggegevens**  Leerlinggegevens die noodzakelijk zijn voor:   * de beoordeling van de toelaatbaarheid en/of * advisering over de ondersteuningsbehoefte en/of * de toewijzing van ondersteuningsmiddelen   mogen 3 jaar bewaard worden na afloop van de beoordeling van de toelaatbaarheid, na advisering over de ondersteuningsbehoefte  of na de toewijzing van ondersteuningsmiddelen.  Voor de registratie van thuiszitters hanteert het samenwerkingsverband een maximale bewaartermijn van een jaar na het verlaten van het primair onderwijs  (ter overbrugging naar het voortgezet onderwijs) en een jaar na het verlaten van het voortgezet onderwijs (ter overbrugging naar een eventuele vervolgopleiding). |

|  |  |
| --- | --- |
| U:\tekening telefoon.jpg | ***Telefoons en tablets***   * Ontvang je de e-mail van het samenwerkingsverband op je (eigen) telefoon of tablet? Zorg dan dat dit apparaat voorzien is van een pincode of beveiligingspatroon. Zie ook de aanwijzingen onder ‘Wachtwoorden zijn persoonlijk en geheim’. * (Privé)telefoon verloren of gestolen? Ook dat is een datalek (melden conform protocol datalekken). * Heb je een bestand van de organisatie (automatisch) gedownload op je eigen tablet of telefoon? Verwijder dit dan direct na gebruik. * Ga je op vakantie naar een land buiten de Europese Unie? Verwijder dan alles van de organisatie op je telefoon. Ook automatisch opgeslagen wachtwoorden kun je beter verwijderen. Het niet verwijderen van gegevens voor je naar bijvoorbeeld de Verenigde Staten vliegt is ook een potentieel datalek. Ook als je op vakantie gaat, blijft de organisatie verantwoordelijk voor de gegevens van de organisatie die mogelijk op jouw telefoon of tablet staan. |

|  |  |
| --- | --- |
| U:\tekening social media.png | **Social media**  Bij het samenwerkingsverband gelden de volgende afspraken voor het gebruik van social media:   * Deel op verantwoorde wijze kennis via social media, rekening houdend met de goede naam van Samenwerkingsverband Brabantse Wal PO en iedereen die hierbij betrokken is. * Maak bij onderwijs- en zorggerelateerde onderwerpen duidelijk of publicatie op persoonlijke titel of namens het samenwerkingsverband gedaan wordt. * Publiceer geen vertrouwelijke informatie op social media. * Weet dat publicaties op social media altijd vindbaar (openbaar) en moeilijk vernietigbaar zijn. Medewerkers zijn persoonlijk verantwoordelijk voor wat zij publiceren. * Neem contact op met een leidinggevende als er twijfel bestaat over een publicatie of over de raakvlakken met het samenwerkingsverband. * 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. |

|  |  |
| --- | --- |
| U:\tekening fotocamera.png | **Foto’s en video’s**  *Foto’s mogen uitsluitend gebruikt worden na schriftelijke toestemming van ouders c.q. wettelijk vertegenwoordigers.*   * Wanneer je foto’s met je (privé)telefoon maakt, blijven de foto’s op jouw toestel achter. Werkgerelateerde foto’s verwijder je na gebruik voor het vastgestelde doel. * Je mag van kinderen alleen beeld- en geluidsopnamen maken als je hiervoor toestemming hebt van de ouders/wettelijk vertegenwoordiger en – indien van toepassing - de verantwoordelijke groepsleerkracht en/of de directie. |

|  |  |
| --- | --- |
|  | **Datalekken**  *Wanneer gegevens onbedoeld in verkeerde handen terecht gekomen (kunnen) zijn, moet dit gemeld worden. Het bewust niet melden van een (potentieel) datalek is strafbaar en kan grote gevolgen voor de organisatie hebben.*  Een datalek meld je volgens het protocol datalekken.  Voorbeelden van een datalek zijn:  computer gehackt, telefoon verloren, naar verkeerde persoon gemaild, papieren dossier ergens laten liggen, printje van een gesprek laten slingeren. |

|  |  |
| --- | --- |
| FG | **Functionaris voor Gegevensbescherming**  *Omdat een samenwerkingsverband veel persoonsgegevens van jonge (kwetsbare) kinderen en jeugdigen verwerkt, moet de organisatie een externe Functionaris Gegevensbescherming hebben, die helpt om de privacyregels goed toe te passen.*   * Contactgegevens externe Functionaris voor Gegevensbescherming: Angela Groen-Vendrig (CED-Groep), 010-4071993 of [a.groen@cedgroep.nl](mailto:a.groen@cedgroep.nl). * Contactgegevens ICT-leverancier Central Point: 088-4300699. |

|  |  |
| --- | --- |
| [Afbeeldingsresultaat voor vergrootglas tekening](https://www.google.nl/url?sa=i&rct=j&q=&esrc=s&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjC1q3tk5XgAhXQfFAKHYD2B2IQjRx6BAgBEAU&url=https://www.bewustzijnsproject.nl/voorbeelden/bedrijfsarts-beter-vindbaar-voor-de-huisarts-via-patientoverleg-zorgdomein/vergrootglas/&psig=AOvVaw3-m9TiziT01Yh446Bkfl67&ust=1548925648422244) | **Controle op naleving**  Wanneer je samen afspraken maakt, zoals beschreven in deze gedragscode, kan periodiek of naar aanleiding van incidenten onderzocht worden of de afspraken nagekomen worden. Als blijkt dat dit niet gebeurt, kunnen hier consequenties aan verbonden worden. Het hierna volgende lijkt wellicht erg streng, maar we vinden het van belang dat juist vooraf duidelijk is wat dan de gang van zaken is.  Laten we er samen voor zorgen dat we dit nooit in werking hoeven te brengen. |
|  |  |
|  |  |
| Samenwerkingsverband Brabantse Wal PO handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving: de Grondwet, de Algemene Verordening Gegevensbescherming (AVG), de Wet Medezeggenschap Onderwijs (WMO), het Burgerlijk Wetboek (BW), het Wetboek van Strafrecht en de Cao PO/PO.  **Voorwaarden voor controle**  Vanzelfsprekend wordt er niet zonder een goede aanleiding een controle uitgezet, deze vindt plaats in het kader van nakoming van de doelen uit deze gedragscode. De controle vindt in eerste instantie plaats op getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen. Als één of meerdere medewerkers verdacht worden van het overtreden van regels, kan het samenwerkingsverband gedurende een vastgestelde (korte) periode een gerichte controle laten uitvoeren. Wanneer ongeoorloofd gebruik wordt geconstateerd, wordt dit direct 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.  **Uitvoering van controle**  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 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) 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 Samenwerkingsverband Brabantse Wal PO worden de nodige maatregelen getroffen zodat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn. En er worden door het samenwerkingsverband passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.  **Disciplinaire maatregelen**  Bij het handelen in strijd met deze gedragscode of de algemeen geldende wettelijke regels, kan de directeur-bestuurder van het samenwerkingsverband, afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen, zoals het geven van een waarschuwing of berisping of bij meer ernstige gevallen een schadevergoeding, aangifte bij de politie, schorsing en/of beëindiging van de arbeidsovereenkomst.  Medewerkers die zich niet aan deze gedragscode houden, worden zo spoedig mogelijk op hun gedrag aangesproken. Zij krijgen daarbij inzage in de over hen vastgelegde gegevens en hebben de gelegenheid te reageren op het geconstateerde. Er worden dan afspraken gemaakt voor de toekomst en de consequenties bij overtreding daarvan. Deze afspraken kunnen strenger zijn dan wat in deze gedragscode is beschreven.  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.  **Bezwaar en Beroep**  Als de medewerker het niet eens is met de (voorgenomen) disciplinaire maatregel, dan kan daar in een aantal gevallen bezwaar en/of beroep tegen worden ingesteld. | |

|  |  |
| --- | --- |
| OPR  Dit document heeft betrekking op de verwerking van persoonsgegevens en/of controle van het gedrag of de prestaties van medewerkers. De ondersteuningsplanraad (‘de OPR’) heeft om deze reden instemmingsrecht. Dit orgaan heeft ingestemd met de inhoud van deze gedragscode. |  |

|  |  |
| --- | --- |
| **Slotbepaling**  Deze regeling wordt elke twee jaar geëvalueerd door Samenwerkingsverband Brabantse Wal PO en de OPR. De eerstkomende evaluatie vindt plaats gelijktijdig met de evaluatie van het Informatiebeveiliging en Privacy Beleid (‘het IBP-beleid’). |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Gedragscode voor gezien en akkoord getekend door werknemer**   |  |  | | --- | --- | | **Naam** |  | | **Functie** |  | | **Datum ondertekening** |  | | **Handtekening** |  | |  |
|  |  |