



**STICHTING PRIMAIR
ONDERWIJS ZUNDERT**

GEDRAGSCODE IBP EN DIGITALE MEDIA

Inhoudsopgave

	blz
1. Inleiding	3
2. Privacy in de wet	3
2.1 Werken met persoonsgegevens: 5 vuistregels	3
3. Afspraken rond IBP en gebruik digitale media	4
3.1 Algemene uitgangspunten	4
3.2 Afspraken/gedragscode gebruik digitale media	4
3.2.1 Gebruik apparaten en netwerkvoorzieningen	4
3.2.2 Bring Your Own Device (BYOD): gebruik van eigen apparaten	4
3.2.3 Gebruik van e-mail	5
3.2.4 Gebruik internet en sociale media	5
3.2.5 Monitoring en controle	6
3.3 Afspraken gegevensuitwisseling met andere instanties en scholen	6
3.4 Afspraken gebruik apparaat en dataopslag	6
3.5 Wachtwoordbeleid	7
3.6 Afspraken bij een datalek	8
3.7 Afspraken gebruik software en bewerkersovereenkomsten	8
3.8 Rechten van de betrokkenen	8
4. Slotbepaling	8

1. Inleiding

Deze handreiking is de praktische invulling van het door Stichting Primair Onderwijs Zundert (SPOZ) geformuleerde beleid op het gebied van informatiebeveiliging en privacy (IPB). We willen onze medewerkers hier handvatten bieden om verantwoord en veilig gebruik te maken van de digitale middelen binnen ons onderwijs, waarbij de privacy van alle bij school en organisatie betrokken personen optimaal is geborgd conform privacy wet- en regelgeving.

In onze huidige sterk digitaliserende maatschappij groeit het aantal beschikbare digitale middelen dagelijks. Ook binnen ons onderwijs worden er steeds meer van deze digitale middelen ter verrijking of aanvulling gebruikt. Met dit toenemend gebruik wordt aandacht voor en afspraken over verantwoordelijk gebruik van deze middelen en daarbij het waarborgen van de privacy van onze leerlingen en medewerkers steeds belangrijker.

2. Privacy in de wet

Sinds 1983 is privacybescherming opgenomen in de Nederlandse Grondwet. De regelgeving rond privacy was uitgewerkt in de Wet Bescherming Persoonsgegevens (WBP) en vanaf 2018 in de Algemene Verordening Gegevensbescherming (AVG). De wet beschermt de privacy door regels te stellen voor de omgang met persoonsgegevens in Nederland (WBP) en Europa (AVG). Het uitgangspunt van de wet is dat privacy altijd wordt gerespecteerd. Leerling gegevens zijn ook persoonsgegevens. De wet is hierop dus van toepassing. Binnen de organisatie is het bevoegd gezag eindverantwoordelijk voor de bescherming van privacy van medewerkers, leerlingen en ouders. Alle betrokkenen zijn verplicht om volgens de wet te handelen en daarbij zorgvuldig te werk te gaan. De wet biedt scholen en organisaties voldoende ruimte om binnen de kaders persoonsgegevens te gebruiken.

2.1 Werken met persoonsgegevens: 5 vuistregels

Om persoonsgegevens te mogen verwerken kent de wet bescherming persoonsgegevens een aantal uitgangspunten. Deze voorwaarden gelden voor elke school/organisatie en zijn samengevat tot 5 vuistregels:

1. *Doel en doelbinding:* persoonsgegevens worden alleen gebruikt voor uitdrukkelijk voorafgaand aan de verwerking omschreven en gerechtvaardigde doeleinden. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. *Grondslag:* verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. *Dataminimalisatie:* persoonsgegevens die de school verwerkt, moeten redelijkerwijs nodig zijn om het doel te bereiken. De gegevens moeten in verhouding staan tot het doel. Dit betekent ook dat data niet langer worden bewaard dan noodzakelijk.
4. *Transparantie:* De betrokkene (medewerker, leerling en/of zijn ouders) is vooraf in begrijpelijke taal geïnformeerd over wat er precies aan informatie wordt verwerkt en wat het doel daarvan is. Verder hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. *Data-integriteit:* Maatregelen om te waarborgen dat te verwerken persoonsgegevens juist en actueel zijn.

3. Afspraken rond IBP en gebruik digitale media

3.1 Algemene uitgangspunten

- a. Medewerkers en leerlingen van SPOZ kunnen in ruime mate gebruik maken van diverse beschikbare digitale middelen.
- b. Medewerkers maken voor hun werk gebruik van een door de organisatie beheerde laptop/pc. Als werk- en opslagomgeving gebruiken medewerkers twee Cloud omgevingen:
 - Office 365 als digitale werkomgeving;
 - Daarnaast hebben leerkrachten (en leerlingen) toegang tot Aerobe (Google G suite for Education) als digitale leeromgeving voor educatief gebruik.
- c. Alle andere applicaties kunnen gestart worden vanuit een van deze twee basisomgevingen.
- d. Door heldere afspraken en gedragsregels (vastgelegd in verschillende documenten) beschermen we de privacy van medewerkers en leerlingen.
- e. Bij keuze, aanschaf en uitbreiding van apparatuur en het vaststellen van procedures is beveiliging en privacybescherming een vast aandachtspunt (privacy by design).
- f. De leidinggevende is verantwoordelijk voor toezicht, toepassing en controle op naleving van informatiebeveiliging en privacy beleid. Meestal is dit de schooldirecteur.

3.2 Afspraken/gedragscode gebruik digitale media

3.2.1 Gebruik apparaten en netwerkvoorzieningen

- a. Medewerkers, leerlingen en andere gebruikers mogen door SPOZ beschikbaar gestelde digitale middelen ook voor persoonlijke doeleinden gebruiken mits dit de dagelijkse werkzaamheden en het (computer)netwerk niet verstoort.
- b. Medewerkers, leerlingen en andere gebruikers die via door SPOZ beschikbaar gestelde digitale middelen, zoals de internet/wifi verbinding, gebruik maken van internet en sociale media gaan hier op een integere, correcte wijze mee om.
- c. Ook bij het gebruik van beschikbaar gestelde apparatuur verwachten we van alle gebruikers dat zij netjes en zorgvuldig met deze middelen omgaan.

3.2.2 Bring Your Own Device (BYOD): gebruik van eigen apparaten

Scholen bepalen zelf of ze al dan niet het gebruik van eigen ICT-apparaten (laptop/tablet/telefoon) toestaan. Ook hier geldt dat gebruik van (eigen) apparatuur nooit verstorend mag werken op de dagelijkse schoolwerkzaamheden en het schoolnetwerk. Deze apparaten worden niet ondersteund door de ICT-service van SPOZ. Als scholen er voor kiezen deze middelen (privé-eigendom) ook in te zetten bij hun onderwijs, kan dit alleen op vrijwillige basis waarbij de gebruiker altijd verantwoordelijk blijft voor zijn of haar device. Hierbij geldt het volgende:

- a. Met ouders/verzorgers worden afspraken gemaakt over de aansprakelijkheid bij verlies/diefstal en defecten bij gebruik op school. Hierbij is uitgangspunt dat de school toestemming geeft om het device te gebruiken, maar niet verantwoordelijk en aansprakelijk is voor het device.
- b. De school kan leerlingen /medewerkers nooit verplichten om eigen apparaten op de school te gebruiken.
- c. Als op de school eigen apparaten zijn toegestaan bepaalt de leerkracht op welke momenten en waarvoor deze apparaten mogen worden gebruikt.
- d. De apparaten kunnen voor een WiFi-verbinding alleen gebruik maken van het gastnetwerk.
- e. Omdat eigen apparaten geen onderdeel uitmaken van de beheerde schoolomgevingen moet rekening gehouden worden met een doorgaans lager beveiligingsniveau en minder functionaliteit dan op de schoolapparatuur.

- f. Voor gebruik van eigen apparaten in de onderwijs/schoolomgeving gelden verder uiteraard dezelfde gebruiks- en gedragsregels als wanneer er vanaf schoolapparaten wordt gewerkt.

3.2.3 Gebruik van e-mail

- a. Werknemers mogen hun SPOZ mailbox gebruiken voor alle mail die werk gerelateerd is.
- b. We verwachten van onze medewerkers dat ze werk gerelateerde mail alleen via dit mailadres versturen en niet via privé mailboxen.
- c. Hoog privacygevoelige informatie wordt op een zo veilig mogelijke manier uitgewisseld, met inachtneming van de vijf vuistregels. Als via de mail bijlages (met hoog privacygevoelige inhoud) verstuurd worden, worden deze bij voorkeur beveiligd verstuurd. Beveiligingscode/sleutel kan los naar de ontvanger gestuurd worden zodat alleen hij of zij de inhoud zichtbaar kan maken.
- d. De mailbox is niet bedoeld als archief voor bijvoorbeeld via de mail ontvangen bijlages. Sla deze altijd op op de daarvoor bedoelde opslagomgevingen.
- e. Bij mail verstuurd naar grotere groepen personen gebruiken we de BCC-mailfunctie. Voor interne groepen gebruiken we daarbij bij voorkeur de in Office 365 aanwezige distributielijsten.
- f. De optie 'allen beantwoorden' gebruiken we alleen indien de noodzaak daarvoor aanwezig is.
- g. Niemand mag, zonder gegronde redenen en toestemming van de eigenaar de inhoud van een persoonlijke mailbox lezen. Wel kan indien er gegronde redenen zijn en alleen met toestemming van de bestuurder een mailbox van een gebruiker geopend worden door daarvoor aangewezen en geautoriseerde medewerkers.

3.2.4 Gebruik internet en sociale media

- a. Bij digitale communicatie (bijvoorbeeld via sociale media) maken medewerkers duidelijk of zij op persoonlijke titel of namens de school publiceren. Betreft het een publicatie over SPOZ in een niet werk gerelateerde omgeving dan moet hiervoor expliciet toestemming worden gevraagd aan de bestuurder.
- b. Bij gebruik van sociale media zijn medewerkers van SPOZ zich bewust van het feit dat zij vertegenwoordiger zijn van hun school/SPOZ.
- c. Verder gaan we bewust om met wat we delen op sociale media: Is het wel of niet verstandig te publiceren, wat zijn de eventuele consequenties en is het betreffende sociale platform/middel wel het meest geschikt voor de te delen inhoud.
- d. Medewerkers gaan over school/organisatie gerelateerde onderwerpen niet in discussie op sociale media.
- e. Medewerkers van de school publiceren of delen geen vertrouwelijke informatie (waaronder persoonsgegevens van bij de organisatie betrokken personen zoals medewerkers, leerlingen en ouders en extern betrokkenen) op sociale media.
- f. Onze medewerkers zijn persoonlijk verantwoordelijk voor wat zij publiceren.
- g. Foto's en filmpjes waarop leerlingen herkenbaar staan, mogen uitsluitend gepubliceerd worden als de ouders/verzorgers van de desbetreffende leerlingen hiermee akkoord zijn. Scholen vragen jaarlijks voor verschillende door de school gebruikte media hiervoor toestemming aan de ouders/verzorgers. Dit geldt ook voor het verspreiden van privacygevoelige gegevens zoals die staan op adres- en bellijsten. Zie ook de brochure van Kennisnet: 'Privacy in tien stappen'.
- h. Onze scholen houden zich bij alle digitale en andere publicaties aan de geldende wettelijk kaders.
- i. Om onze leerlingen qua content in een zo veilig mogelijke omgeving te laten werken maakt elke school afspraken m.b.t. toezicht bij en gebruik van internet en sociale media. Deze worden vastgelegd in een protocol mediawijsheid. Daarnaast werken leerlingen op onze scholen vanuit Aerobe / Google for Education, waar standaard strengere filters aanstaan zoals bijvoorbeeld Google Safe Search.
- j. De school zorgt ook digitaal voor een veilig klimaat en communiceert met medewerkers, leerlingen en ouders hoe zij dit doet.

3.2.5 Monitoring en controle

- a. Controle op het internet- en mailgebruik vindt slechts ten behoeve van onderstaande doelen plaats:
 - Het tegengaan van virussen en andere schadelijke programma's;
 - Het oplossen van netwerkproblemen (capaciteit en blokkades etc);
 - Het tegengaan van 'verboden of foutief gebruik'.
- b. Controle vindt incidenteel of steekproefsgewijs plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Indien er aanwijzingen of vermoedens zijn dat de regels worden overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden.
- c. Controle beperkt zich in principe tot verkeersgegevens van het gebruik van e-mail en internet. Alleen bij zwaarwegende redenen kan er controle op de inhoud gedaan worden. Dit laatste kan bij medewerkers alleen met toestemming van de bestuurder.
- d. De leidinggevende spreekt medewerkers en leerlingen, op hun gedrag aan als zij zich niet houden aan de gemaakte afspraken.

3.3 Afspraken gegevensuitwisseling met andere instanties en scholen

- a. Uitwisseling tussen scholen onderling van onderwijskundige rapporten en overdrachtdossiers gebeurt vanuit ESIS via 'Onderwijs Overstap Service' (OSO). Dit is een digitaal, beveiligd overstapprotocol.
- b. Ook de verzuimregistratiemeldingen naar de leerplichtambtenaar en uitwisseling met DUO en Bron wordt gedaan vanuit ESIS via een digitaal en beveiligd protocol.
- c. De digitale overdracht naar andere instanties zoals bijvoorbeeld zorgaanbieders en de inspectie voor het Onderwijs, verloopt met in achtname van de privacyregels en daarbij horende procedures. Uitgangspunt zijn ook daar de 5 vuistregels genoemd eerder in dit handboek.

3.4 Afspraken gebruik apparaat en dataopslag

Om ervoor te zorgen dat de privacygevoelige informatie zowel binnen als buiten de school beschermd is, hanteren we de volgende afspraken:

- a. Medewerkers laten apparaten waarop toegang gekregen kan worden tot privacygevoelige gegevens niet onbeheerd en onbeveiligd achter. Zij kunnen dit doen door af te sluiten, uit te loggen of te vergrendelen. Wij gaan ervan uit dat dit ook toegepast wordt op externe (eigen) apparaten zoals bijvoorbeeld eigen tablets, mobiele telefoons of thuiscomputers.
- b. Externen hebben als basisregel geen toegang tot de leerling-administratie en het leerlingvolgsysteem of enig ander systeem waar (hoog)privacygevoelige informatie benaderbaar is.
- c. Medewerkers zijn verplicht om zorgvuldig met hun wachtwoorden om te gaan. Dit geldt in het bijzonder voor de (netwerk)inloggegevens en softwarepakketten waarin zich persoonsgegevens bevinden.
- d. Digitaal versturen van privacygevoelige gegevens dient, daar waar mogelijk, versleuteld of beveiligd te gebeuren.
- e. SPOZ gebruikt voor dataopslag als centrale plaats een eigen omgeving: Office 365 (data school en stichting). Privacygevoelige data alleen in de daarvoor bedoelde mappen.
Deze omgeving is door middel van een login en rechten systeem beveiligd. Gebruikers slaan privacygevoelige data altijd op op de daarvoor aangewezen opslag omgeving van de school of stichting. Hoog privacygevoelige informatie komt primair in ESIS en/of in de speciaal ingerichte bibliotheken op Sharepoint (b.v. leraar, IB- en directiebibliotheek).
- f. Het is niet toegestaan om hoog privacygevoelige data op te slaan buiten de daarvoor bedoelde school(Cloud)omgeving. Dus ook niet op de lokale harde schijf van de computer of onbeveiligde opslagmiddelen zoals een externe harde schijf, geheugenkaart of USB-stick. Mochten er toch externe opslagmiddelen gebruikt worden bijvoorbeeld door

synchronisatiemappen of voor een harde back-up, dan kan/mag dit alleen als er gebruik gemaakt wordt van beveiliging (zoals wachtwoordbeveiliging).

- g. Medewerkers moeten regelmatig controleren of er geen (privacygevoelige) data lokaal op de pc staan, bijvoorbeeld in de downloadmap. Telkens als er namelijk in de Cloud omgeving op de knop download geklikt wordt, wordt het betreffende bestand op de pc gezet, meestal in de downloadmap. Maak de downloadmap leeg wanneer nodig.

3.5 Wachtwoordbeleid

- a. SPOZ gaat ervan uit dat medewerkers zorgvuldig met hun wachtwoorden om gaan. Dat betekent o.a. dat wachtwoorden naar omgevingen waar zich privacygevoelige data bevinden nooit gedeeld worden met andere personen. Het zichtbaar ophangen van persoonlijke wachtwoorden is dus ook niet toegestaan.
- b. In de systemen waar SPOZ zelf het wachtwoordbeleid kan bepalen en waar privacygevoelige data worden opgeslagen (zoals Office 365 en de Aerobe omgeving) wordt periodiek (minimaal jaarlijks) afgedwongen dat medewerkers een nieuw (qua complexiteit 'sterk') wachtwoord kiezen. Ook worden accounts in die omgevingen automatisch uitgelogd als deze langere tijd ongebruikt ingelogd zijn op een apparaat. Ook in andere systemen raden we gebruikers aan regelmatig hun wachtwoord te vernieuwen.
- c. SPOZ gaat m.b.t. wachtwoordeisen en gebruik in de systemen uit van enkele basisregels:
 - Medewerkers mogen hun wachtwoord nooit delen, dat is persoonlijk. Op onze scholen zitten ook veel gegevens van anderen (in het bijzonder de leerlingen) achter iemands wachtwoord. Het gaat dus niet alleen om de eigen persoonsgegevens maar ook om vele andere. Wachtwoorden dus niet aan andere personen geven of op briefjes of lijsten schrijven die vrij toegankelijk voor anderen bereikbaar zijn.
 - Het wachtwoord mag niet makkelijk te raden zijn.
 - Het wachtwoord niet hergebruiken. In ieder geval andere wachtwoorden voor werk en privé omgevingen. Door de grote hoeveelheid wachtwoorden die iedereen heeft, is dit lastig. Medewerkers dienen dan in ieder geval te zorgen voor goede unieke wachtwoorden voor de omgevingen waar de echt privacygevoelige gegevens staan. Privé kan gedacht worden aan de inlogwachtwoorden van digiD, de bank, de zorgverzekering etc. Voor het werk gaat het dan om systemen als ESIS, Office 365, Afas etc.
 - Medewerkers dienen bewust te kiezen of zij wachtwoorden wel of niet opslaan in de browser:
 - Staan er geen persoonsgegevens in de betreffende omgeving dan is het altijd een vrije keuze om het wachtwoord in de browser te laten onthouden;
 - Sla bij gebruik van een onbeveiligde of slecht beveiligde (thuis)pc waar zonder wachtwoord op gewerkt wordt, geen wachtwoorden van (werk gerelateerde) programma's (waarin zich privacygevoelige (persoons)gegevens bevinden) op;
 - Indien gewerkt wordt op een goed met wachtwoord beveiligd apparaat vanuit Office 365 of Aerobe, dan mogen wachtwoorden door de browser opgeslagen worden: de omgeving is dan beschermd omdat met een wachtwoord ingelogd moet worden. Er dient dan nog zorgvuldiger omgegaan te worden met hoofdwachtwoorden.
 - Laat wachtwoorden van de pakketten waar zich veel en hoog privacygevoelige data bevinden, zoals ESIS of AFAS, niet opslaan in de browser.

3.6 Afspraken bij een datalek

Een datalek is een beveiligingsincident, waarbij (persoons)gegevens verloren raken of onrechtmatig worden ingezien of bewerkt (opgeslagen, aangepast, verzonden enzovoorts). Hierbij geldt het volgende:

- a. Als er door bijvoorbeeld verlies of diefstal van of inbraak in apparatuur (ook bijvoorbeeld USB- stick of externe harde schijf) of Cloud omgeving mogelijk sprake is van verlies, onrechtmatig gebruik van of inzage is in privacygevoelige data, spreken we van een (mogelijk) datalek. Bij kennis hiervan is de medewerker verplicht dit aan zijn leidinggevende te melden zodat de organisatie de juiste acties kan inzetten.
- b. Procedure voor het melden van een (mogelijk) datalek:
 - Melden bij degene die verantwoordelijk is voor IBP (meestal is dat de directeur),
 - Als dat mogelijk is direct maatregelen nemen om de gevolgen te beperken. Bijvoorbeeld: pc afsluiten/vergrendelen, lokaal afsluiten, USB-stick veiligstellen, materiaal op de printer veiligstellen etc.
- c. Bij SPOZ is de procedure dat de directeur/leidinggevende de melding moet doen bij de functionaris gegevensbescherming (FG) die vervolgens samen met de bestuurder bepaalt of er sprake is van een datalek. Zo ja, dan doet de FG een melding bij de Autoriteit Persoonsgegevens. De schooldirecteur is verantwoordelijk voor de te nemen maatregelen op school (en voor het aanleveren van alle gegevens).
- d. Een school(bestuur) is verplicht binnen 72 uur een datalek te melden bij de Autoriteit Persoonsgegevens.
- e. Bij/na melding van een mogelijk datalek volgen we de procedures zoals die zijn vastgelegd in het protocol datalekken SPOZ.

3.7 Afspraken gebruik software en bewerkersovereenkomsten

Al onze systemen en opslag bevinden zich in Cloud omgevingen. Dat betekent concreet dat de informatie van onze medewerkers en leerlingen zich in de digitale omgevingen van diverse externe partijen bevindt. De basisregel hierbij is dat alle gegevens in deze systemen eigendom zijn van de school/organisatie.

Voor alle softwaresystemen en apps die we gebruiken (dus ook educatieve software en apps) geldt dat zodra er privacygevoelige data worden ingevoerd een bewerkersovereenkomst met de leverancier van de software afgesloten moet zijn/worden.

Bij SPOZ dragen we er zorg voor dat die ondertekende bewerkersovereenkomsten aanwezig zijn van de partijen waar wij gegevens opslaan en waarmee we gegevens uitwisselen.

Uitgangspunten bij gebruik van systemen en gebruik/invoer van persoonsgegevens zijn:

- We voeren alleen persoonsgegevens in in systemen/programma's als dit voor het desbetreffende doel noodzakelijk is. Dus als het zonder kan, dan geen persoonsgegevens invoeren/gebruiken.
- Als er in plaats van persoonsgegevens ook geanonimiseerde gegevens kunnen worden gebruikt heeft dat de voorkeur. Moet er persé iets ingevoerd worden dan liefst geanonimiseerd.
- Als het noodzakelijk is dat er in systemen/programma's privacygevoelige data (persoonsgegevens) worden opgeslagen, moet er altijd een bewerkingsovereenkomst met de externe partij zijn of zo spoedig mogelijk komen.
- Als scholen of medewerkers systemen in gebruik nemen waar privacygevoelige data ingevoerd moeten worden (persoonsgegevens) checken zij of hiervoor al een bewerkersovereenkomst bij SPOZ aanwezig is. Zo niet, dan kan in overleg met de bestuurder door de betreffende directeur bij de betreffende leverancier of organisatie een bewerkingsovereenkomst bovenschols opgevraagd en afgesloten worden. Dit geldt dus ook voor alle (gratis) beschikbare educatieve software en apps.
- Alle bewerkersovereenkomsten worden bovenschols beoordeeld en getekend door de bestuurder. Scholen tekenen zelf geen overeenkomsten maar sturen deze bij ontvangst door naar het bestuurskantoor.

- Als er met een aanbieder geen bewerkersovereenkomst gesloten kan worden, mogen er geen privacygevoelige gegevens in het betreffende systeem worden ingevoerd. Als het systeem dit afdwingt of eist kan het alleen gebruikt worden met geanonimiseerde gegevens of als er na nader onderzoek (bovenschools) is vastgesteld dat betreffende partij aan de voorwaarden van het convenant Digitale onderwijsmiddelen en Privacy voldoet. Dit laatste is bijvoorbeeld ook van toepassing op de omgevingen van Google, Microsoft en Apple omdat met deze partijen geen één op één overeenkomsten kunnen worden afgesloten.
- Bij alle overeenkomsten is het geldende convenant Digitale onderwijsmiddelen en Privacy met de bijbehorende modelovereenkomst van o.a. de PO-raad het uitgangspunt.
- Een getekend, exemplaar van iedere bewerkingsovereenkomst wordt bovenschools bewaard in de contractadministratie.

3.8 Rechten van de betrokkenen

- a. Het bevoegd gezag informeert de medewerkers en andere gebruikers voorafgaand aan de invoering van voor hen geldende afspraken zoals in dit handboek opgenomen.
- b. Medewerkers of andere gebruikers die problemen ervaren met betrekking tot de naleving van de afspraken rond IBP kunnen dit melden bij de directeur of de functionaris gegevensbescherming (FG). Daarnaast kan ook gebruik gemaakt worden van de geldende klachtenregeling of kunnen ze zich wenden tot de vertrouwenspersoon.

4. Slotbepaling

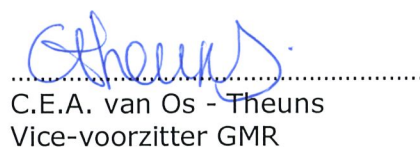
De dagelijkse digitale praktijk verandert voortdurend en in een alsmaar hoger tempo. We zullen dan ook dit handboek als daar aanleiding voor is aanpassen, uitbreiden en bijstellen. Bij elke nieuwe versie zullen we de gebruikers waarop dit handboek betrekking heeft op de hoogte stellen van de aanpassingen.

Dit protocol is na instemming van de GMR vastgesteld op 25 juni 2019.

Stichting Primair Onderwijs in de gemeente Zundert,



L.B. van Breda
Voorzitter College van Bestuur



C.E.A. van Os - Theuns
Vice-voorzitter GMR