Privacyreglement Onderwijsgroep Zuid Hollandse Waarden voor PO en VO

NAAM DOCUMENT(EN)	Privacyreglement Onderwijsgroep Zuid Hollandse Waarden voor PO en VO	
VERANTWOORDELIJKE	Lisette van de Weijer - FG	
AUTEUR	Paul Schijff - PO	
TREFWOORDEN	IBP, AVG, Privacy, Sociale media, E-mail, Internet, Netwerk	
Versie	**Datum**	**Wijziging / Actie**
0.9	**Maart 2020**	**Concept Paul Schijff**
1.0	**Mei 2020**	**Concept aanpassing, naar Lisette van de Weijer**
		Concept naar CvB
1.1.		**Raadpleging in (G)MR 22 juni en met aanvullingen verwerkt**
2.0	**Juli 2020**	**Vastgesteld 14 juli 2020**

Leeswijzer

Dit product is een nadere uitwerking van het Privacyreglement OZHW.

Doelgroep

Dit document is van belang voor alle medewerkers binnen OZHW

Relatie met overige producten

- Informatiebeveiliging en Privacy van OZHW

Inhoudsopgave

Vastgesteld door het College van Bestuur op 14-07-2020 na raadpleging (G)MR d.d. 22-06-2020

Inleiding

Stichting Onderwijsgroep Zuid Hollandse Waarden voor PO en VO, in deze de daarbij behorende scholen (hierna te noemen OZHW), verwerkt persoonsgegevens om haar taak als onderwijsinstelling uit te voeren. Hierbij geldt vanaf 25 mei 2018 de Algemene verordening gegevensbescherming (AVG); dit is de Europese privacyregelgeving die sinds die datum ook in Nederland van toepassing is en de Wet bescherming persoonsgegevens opvolgt.

OZHW biedt haar leerlingen een veilige leeromgeving en onze medewerkers een veilige werkplek. Een goede en zorgvuldige omgang met persoonsgegevens binnen de organisatie is daarvoor een randvoorwaarde.
De Algemene Verordening Gegevensbescherming (AVG) stelt nieuwe en verdergaande eisen aan de omgang met deze persoonsgegevens. Het privacyreglement en het beleid dat daaraan ten grondslag ligt wordt dan ook herzien en aangevuld op punten indien de AVG dit vereist.
Met dit reglement beoogt OZHW ervoor zorg te dragen dat de verwerking van persoonsgegevens plaatsvindt conform de Verordening, de sectorgedragscodes, sectorbeveiligingscodes en organisatie-specifieke (interne) regelingen. Dit houdt onder andere in dat:
a. de persoonlijke levenssfeer van betrokkene wordt beschermd tegen onrechtmatige verwerking en/of misbruik van die gegevens, tegen verlies en tegen het verwerken van onjuiste gegevens;
b. wordt voorkomen dat persoonsgegevens worden verwerkt voor een ander doel dan het doel waarvoor ze verzameld zijn; en
c. de verwerkingen niet leiden tot een hoog risico voor de betrokkenen.

Het college van bestuur zal in samenspraak met de functionaris gegevensbescherming passende maatregelen ten uitvoer leggen en verantwoording afleggen over het gevoerde beleid aan de ouder- en personeelsgeleding van de medezeggenschapsraad en aan de Raad van Toezicht.

PRIVACYREGLEMENT ONDERWIJSGROEP ZUID HOLLANDSE WAARDEN VOOR PO EN VO

Artikel 1 Toepasselijkheid

Dit reglement geldt voor de gehele organisatie die deel uitmaakt van STICHTING OZHW. STICHTING OZHW is gevestigd aan de Hakwei 2, 2992 ZB te Barendrecht.

Artikel 2 Definities

Persoonsgegevens

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'), zoals bijvoorbeeld naam, adres, geboortedatum, titel(s), geslacht, adres, telefoonnummer, e-mailadres, functie, personeelsnummer, medische rapportages, inhoud van e-mails, prestaties/cijfers, brieven, klachten, foto's, video's, IP-adressen, tracking cookies, loginnamen en wachtwoorden.

Verwerking van persoonsgegevens

Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, geautomatiseerd of handmatig, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

Bijzondere persoonsgegevens

Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, genetische gegevens (DNA/RNA) of biometrische gegevens (bijv. foto's) met het oog op de unieke identificatie van een persoon, en gegevens over gezondheid, of iemands seksueel gedrag of seksuele gerichtheid

Betrokkene

Degene op wie een persoonsgegeven betrekking heeft, en die al dan niet wordt vertegenwoordigd door een wettelijk vertegenwoordiger. Betrokkenen kunnen bijvoorbeeld zijn: leerlingen, ouders, medewerkers en bezoekers.

Wettelijk vertegenwoordiger

Degene die het ouderlijk gezag over een minderjarige uitoefent. Meestal zal dit een ouder zijn, maar het kan ook gaan om een voogd. Als een leerling 16 jaar of ouder is, beslist hij in voorkomende gevallen zelf over zijn privacy.

*Verwerkingsverantwoordelijk*e

De entiteit die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. In het kader van dit reglement is het Stichting OZHW, te weten de Stichting Voortgezet Onderwijs Kennemerland (STICHTING OZHW), vertegenwoordigd door het College van Bestuur, de verwerkingsverantwoordelijke.

Verwerker

De natuurlijke persoon of rechtspersoon die ten behoeve van de verwerkingsverantwoordelijke (STICHTING OZHW) persoonsgegevens verwerkt, zoals bijvoorbeeld de leverancier van een leerlingvolgsysteem of leerlingadministratiesysteem. Een verwerker heeft een uitvoerende taak, ten behoeve van de activiteiten van de verwerkingsverantwoordelijke.

Derde

Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, de verwerkingsverantwoordelijke, de verwerker, of de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om persoonsgegevens te verwerken.

Stichting OZHW

STICHTING OZHW, de verwerkingsverantwoordelijke in de zin van dit reglement.

Artikel 3 Reikwijdte en doelstelling

1. Dit reglement stelt regels over de verwerking van persoonsgegevens van alle betrokkenen bij de organisatie, waaronder leerlingen en hun wettelijk vertegenwoordigers, medewerkers, bezoekers en externe relaties (bijv. leveranciers en opdrachtnemers).

2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door de STICHTING OZHW worden verwerkt. Het reglement heeft tot doel:

a. de persoonlijke levenssfeer van de betrokkenen te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens;
b. vast te stellen met welk doel en op welke (juridische) grondslag persoonsgegevens binnen STICHTING OZHW worden verwerkt;
c. ook overigens te borgen dat persoonsgegevens binnen STICHTING OZHW rechtmatig, transparant en behoorlijk worden verwerkt;
d. de rechten van betrokkenen vast te leggen en te borgen dat deze rechten door STICHTING OZHW worden gerespecteerd.

Artikel 4 Doelen van de verwerking van persoonsgegevens

Bij de verwerking van persoonsgegevens houdt STICHTING OZHW zich aan de relevante wet- en regelgeving waaronder de Algemene Verordening Gegevensbescherming (AVG), de uitvoeringswet AVG en de onderwijswetgeving

1. De verwerking van persoonsgegevens vindt plaats voor:
a. de organisatie of het geven van het onderwijs, de begeleiding van leerlingen, het voorzien in hun (extra) ondersteuningsbehoefte, dan wel het geven van studieadviezen;
b. het verstrekken en/of ter beschikking stellen van leermiddelen;
c. het bewaken van de veiligheid binnen de scholen en het beschermen van eigendommen van medewerkers, leerlingen en bezoekers;
d. het bekend maken van informatie over de organisatie en leermiddelen als bedoeld, onder a en b, alsmede van informatie over de leerlingen op de eigen website;
e. het bekend maken van de activiteiten van de organisatie, bijvoorbeeld op de website van STICHTING OZHW of van de scholen, in brochures of de schoolgids of via social media;
f. het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, waaronder begrepen het in handen van derden stellen van vorderingen;
g. het aanvragen van bekostiging, het behandelen van geschillen daarover en het doen uitoefenen van accountantscontrole;
h. het onderhouden van contacten met oud-leerlingen;
i. het aangaan en uitvoeren van arbeidsovereenkomsten, samenwerkingsrelaties met opdrachtnemers en contracten met leveranciers;
j. de uitvoering of toepassing van wet- en regelgeving;
k. juridische procedures waarbij STICHTING OZHW betrokken is.

2. De verwerking van persoonsgegevens mag ook plaatsvinden voor doelen die verenigbaar zijn met de doelen zoals beschreven in lid 1.

Artikel 5 Doelbinding

Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. STICHTING OZHW verwerkt niet meer gegevens dan noodzakelijk is om de betreffende doelen te bereiken.

Artikel 6 Soorten persoonsgegevens

De categorieën van persoonsgegevens zoals deze binnen STICHTING OZHW worden verwerkt, worden geregistreerd in een verwerkingsregister.

Artikel 7 Grondslagen van verwerking

Verwerking van persoonsgegevens gebeurt alleen indien aan een van de onderstaande voorwaarden is voldaan:
- De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan STICHTING OZHW is opgedragen.
- De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op STICHTING OZHW rust.
- De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (bijvoorbeeld de arbeidsovereenkomst) of om op verzoek van de betrokkene vóór de sluiting van een

overeenkomst maatregelen te nemen.

- De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van STICHTING OZHW of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen, met name wanneer de betrokkene een kind is; in het kader van deze grondslag zal dus een belangenafweging moeten plaatsvinden.
- De verwerking is noodzakelijk om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen (levensbelang).
- De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.

Artikel 8 Bewaartermijnen

STICHTING OZHW bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor deze worden verwerkt, tenzij het langer bewaren van de persoonsgegevens op grond van wet- of regelgeving verplicht is.

Artikel 9 Toegang

Binnen de organisatie van STICHTING OZHW geldt dat personen slechts toegang hebben tot persoonsgegevens voor zover dat daadwerkelijk nodig is. De toegang van medewerkers tot persoonsgegevens is dan ook beperkt tot de gegevens die noodzakelijk zijn voor de goede uitoefening van hun functie en (dus) hun werkzaamheden. Verder wordt slechts toegang verschaft tot de in de administratie en systemen van de school opgenomen persoonsgegevens aan:

a. de verwerker die van STICHTING OZHW de opdracht heeft gekregen om persoonsgegevens te verwerken, maar alleen voor zover dat noodzakelijk is in het licht van de gemaakte afspraken;
b. derden voor zover uit de wet voortvloeit dat STICHTING OZHW verplicht is om toegang te geven of sprake is van een (andere) grondslag voor deze verwerking, bijvoorbeeld de vervulling van een taak van algemeen belang.

Artikel 10 Beveiliging en geheimhouding

STICHTING OZHW neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. Deze maatregelen zijn er mede op gericht om niet noodzakelijke verzameling en verdere (niet noodzakelijke) verwerking van persoonsgegevens te voorkomen. Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van betrokkenen. Een ieder die betrokken is bij de verwerking van persoonsgegevens binnen STICHTING OZHW is verplicht tot geheimhouding van de betreffende persoonsgegevens, en zal deze gegevens slechts verwerken voor zover dat noodzakelijk is voor de uitoefening van de betreffende functie, werkzaamheden of taak.

Artikel 11 Verstrekking van gegevens aan derden

STICHTING OZHW kan persoonsgegevens aan derden verstrekken als daarvoor een grondslag bestaat in de zin van artikel 7 van dit reglement.

Artikel 12 Sociale Media

Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt in het sociale mediaprotocol van STICHTING OZHW.

Artikel 13 Rechten van Betrokkenen

STICHTING OZHW erkent de rechten van betrokkenen, handelt daarmee in overeenstemming en bewerkstelligt dat betrokkenen deze rechten daadwerkelijk kunnen uitoefenen. Het betreft in het bijzonder de volgende rechten:

1. Inzage

Een betrokkene heeft recht op inzage van de door STICHTING OZHW verwerkte persoonsgegevens die op hem betrekking hebben, behalve voor zover het gaat om werkdocumenten, interne notities en andere documenten die uitsluitend bedoeld zijn voor intern overleg en beraad. Indien en voor zover dit recht op inzage ook de rechten en

vrijheden van anderen raakt, bijvoorbeeld als in de documenten ook persoonsgegevens van anderen dan de betrokkene zijn vermeld, kan STICHTING OZHW het recht op inzage beperken.

Bij het verstrekken van de betreffende gegevens verschaft STICHTING OZHW voorts informatie over:

- de verwerkingsdoeleinden;
- de categorieën van persoonsgegevens die worden verwerkt;
- de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- (indien van toepassing) ontvangers in derde landen of internationale organisaties;
- (indien mogelijk) hoe lang de gegevens worden bewaard;
- dat de betrokkene het recht heeft om te verzoeken dat de persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van de persoonsgegevens wordt beperkt, alsmede dat hij het recht heeft om bezwaar te maken tegen de verwerking van de persoonsgegevens;
- het feit dat de betrokkene een klacht kan indienen bij de Autoriteit Persoonsgegevens;
- de bron van de persoonsgegevens, indien de persoonsgegevens niet van de betrokkene zelf zijn verkregen;
- het eventueel toepassen van geautomatiseerde besluitvorming en de betreffende onderliggende logica en het belang en de gevolgen voor de betrokkene;
- de passende waarborgen indien de persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie.

2. Verbetering, aanvulling, verwijdering
STICHTING OZHW verbetert de persoonsgegevens van een betrokkene in het geval de betrokkene terecht heeft aangegeven dat de gegevens onjuist zijn, en STICHTING OZHW vult de persoonsgegevens van een betrokkene aan indien de betrokkene terecht om aanvulling heeft verzocht. Voorts kan de betrokkene verzoeken om verwijdering van zijn persoonsgegevens. STICHTING OZHW gaat daartoe over indien is voldaan aan een wettelijke grondslag voor het verzoek, tenzij het onmogelijk is om aan het verzoek te voldoen of dit een onredelijke inspanning zou vergen.
3. Bezwaar
Indien STICHTING OZHW persoonsgegevens verwerkt op de grondslag van artikel 7 onder a of artikel 7 onder d van dit reglement, kan de betrokkene bezwaar maken tegen de verwerking van zijn persoonsgegevens. In dat geval staakt STICHTING OZHW de verwerking van de betreffende persoonsgegevens, behalve als naar het oordeel van STICHTING OZHW het belang van STICHTING OZHW, het belang van derden of het algemeen belang in het betreffende concrete geval zwaarder weegt.
4. Beperken verwerking
De betrokkene kan voorts verzoeken om de verwerking van zijn persoonsgegevens te beperken, namelijk indien hij een verzoek tot verbetering heeft gedaan, indien hij bezwaar heeft gemaakt tegen de verwerking, als de persoonsgegevens niet meer nodig zijn voor het doel van de verwerking of als de gegevensverwerking onrechtmatig is. STICHTING OZHW staakt dan de verwerking, tenzij de betrokkene toestemming heeft gegeven voor de verwerking, STICHTING OZHW de gegevens nodig heeft voor een rechtszaak of de verwerking nodig is ter bescherming van de rechten van een andere persoon of vanwege gewichtige redenen.
5. Kennisgevingsplicht
Als STICHTING OZHW op verzoek van een betrokkene een verbetering of verwijdering van persoonsgegevens heeft uitgevoerd, of de verwerking van persoonsgegevens heeft beperkt, zal STICHTING OZHW eventuele ontvangers van de betreffende persoonsgegevens daarover informeren.
6. Procedure
STICHTING OZHW handelt een verzoek van een betrokkene zo spoedig mogelijk, maar uiterlijk binnen een maand na ontvangst van het verzoek, af. Afhankelijk van de complexiteit en van het aantal verzoeken kan die termijn indien nodig met twee maanden worden verlengd. Als deze verlenging plaatsvindt, wordt de betrokkene daarover binnen een maand na de ontvangst van het verzoek geïnformeerd. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt. Wanneer STICHTING OZHW geen gevolg geeft aan het verzoek van de betrokkene, deelt STICHTING

OZHW onverwijld en uiterlijk binnen een maand na ontvangst mede waarom het verzoek niet wordt ingewilligd en informeert hij de betrokkene over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens of beroep bij de rechter in te stellen.

7. Intrekken toestemming

Indien voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming te allen tijden door de betrokkene of zijn wettelijk vertegenwoordiger worden ingetrokken. Als de toestemming wordt ingetrokken, staakt STICHTING OZHW de verwerking van persoonsgegevens, behalve als er een andere grondslag (zoals bedoeld in artikel 7) voor de gegevensverwerking is. Het intrekken van de toestemming tast de rechtmatigheid van verwerkingen die reeds hebben plaatsgevonden niet aan.

Artikel 14 Transparantie

STICHTING OZHW informeert de betrokkene(n) actief over de verwerking van hun persoonsgegevens, in ieder geval door middel van een laagdrempelige privacyverklaring. In de privacyverklaring wordt in ieder geval de volgende informatie vermeld:

a. de contactgegevens van STICHTING OZHW;
b. de contactgegevens van de functionaris voor gegevensbescherming van STICHTING OZHW;
c. de doeleinden van de gegevensverwerking en de grondslagen voor de verwerking;
d. een omschrijving van de belangen van STICHTING OZHW indien de verwerking wordt gebaseerd op het gerechtvaardigd belang van STICHTING OZHW;
e. de (categorieën) ontvangers van de persoonsgegevens, zoals verwerkers of derden;
f. in voorkomend geval: of de persoonsgegevens worden verzonden aan landen buiten de Europese Economische Ruimte (EER);
g. hoe lang de persoonsgegevens zullen worden bewaard;
h. dat de betrokkene het recht heeft om STICHTING OZHW te verzoeken om inzage, verbetering of verwijdering van persoonsgegevens, en dat hij het recht heeft om te verzoeken om beperking van de verwerking, om bezwaar te maken of om een beroep te doen op het recht van gegevensoverdraagbaarheid;
i. dat de betrokkene het recht heeft om zijn toestemming in te trekken, als de gegevensverwerking is gebaseerd op toestemming;
j. dat de betrokkene het recht heeft om een klacht in te dienen bij de Autoriteit Persoonsgegevens;
k. of de verstrekking van de persoonsgegevens een wettelijke of contractuele verplichting is, dan wel een noodzakelijke voorwaarde is om een overeenkomst te kunnen sluiten, en of de betrokkene verplicht is om de persoonsgegevens te verstrekken en wat de gevolgen zijn indien hij de persoonsgegevens niet verstrekt;
l. het bestaan van geautomatiseerde besluitvorming, vergezeld van nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Artikel 15 Meldplicht datalekken

Een ieder die betrokken is bij een verwerking van persoonsgegevens is verplicht om een datalek per ommegaande te melden bij het meldpunt (servicedesk@ozhw.nl), conform het protocol beveiligingsincidenten en datalekken van STICHTING OZHW. Een datalek is elke inbreuk waarbij persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk zijn gemaakt.

Artikel 16 Klachten

1. Wanneer een betrokkene van mening is dat het doen of nalaten van STICHTING OZHW niet in overeenstemming is met de AVG, dit reglement of (andere) toepasselijke wet- of regelgeving, dan kan een klacht worden ingediend overeenkomstig de binnen STICHTING OZHW geldende klachtenregeling. Een betrokkene kan zich eveneens wenden tot de functionaris voor gegevensbescherming van STICHTING OZHW.
2. Als een klacht naar de mening van betrokkene door STICHTING OZHW niet correct is afgewikkeld, kan hij zich wenden tot de rechter of de Autoriteit Persoonsgegevens.

Artikel 17 Onvoorziene situaties

Indien zich een situatie voordoet die niet beschreven is in dit reglement, neemt het College van Bestuur van STICHTING OZHW de benodigde maatregelen, en wordt beoordeeld of dit reglement dientengevolge moet worden aangevuld of aangepast.

Artikel 18 Wijzigingen Reglement

1. Dit reglement is na instemming van de Gemeenschappelijke Medezeggenschapsraad (GMR) vastgesteld door het College van Bestuur van STICHTING OZHW. Het reglement wordt gepubliceerd op de website van STICHTING OZHW en de websites van de scholen. Het reglement wordt verder actief onder de aandacht gebracht, bijvoorbeeld door middel van verwijzing in de schoolgids.

2. Het College van Bestuur kan dit reglement wijzigen na instemming van de GMR

Artikel 19 Slotbepaling

Dit reglement wordt aangehaald als het privacyreglement van STICHTING OZHW en treedt in werking op 07 juni 2018.

PRIVACY TOELICHTING; HOE GAAT STICHTING OZHW OM MET PERSOONSGEGEVENS.

1.1 Waarom verwerken wij gegevens van uw kind

1. OZHW verwerkt persoonsgegevens van uw kind om onze verplichtingen als onderwijsinstelling te kunnen nakomen. Zo hebben wij bijvoorbeeld de gegevens nodig om uw kind aan te melden als leerling op onze school, om de studievoortgang bij te houden en om uw kind in staat te stellen een diploma te halen. Daarnaast hebben wij de wettelijke verplichting om bepaalde gegevens door te sturen naar andere partijen, zoals DUO (ministerie van Onderwijs) en leerplicht.
2. Wij verwerken gegevens van uw kind voor het uitvoeren van de *onderwijsovereenkomst* die we met uw kind hebben en/of voor het nakomen van onze *wettelijke verplichtingen.*
3. Gegevens die hier niet aan voldoen zullen wij alleen met uw toestemming verwerken. Als voor het verwerken van gegevens toestemming wordt gevraagd zoals voor het gebruik van beeldmateriaal (foto's en video's) dan kunt u de toestemming op elk moment intrekken of alsnog geven. (Wijziging van toestemming is niet van toepassing op inmiddels gepubliceerd beeldmateriaal).

1.2. Welke gegevens verwerken wij van uw kind

1. Wij verwerken diverse soorten gegevens, waarvan wij de meeste gegevens rechtstreeks van u als ouders hebben gekregen. U kunt hierbij denken aan contactgegevens en geboorteplaats. Als u weigert de voor ons noodzakelijke gegevens te verstrekken, kunnen wij onze verplichtingen niet nakomen. De verstrekking van deze gegevens is dan ook een voorwaarde om uw kind in te kunnen schrijven bij OZHW.

2. Welke persoonsgegevens wij van uw kind verwerken kun u terugvinden onderaan deze toelichting bij categorieën van persoonsgegevens.
3. Op uw eigen verzoek en met uw uitdrukkelijke toestemming verwerken wij ook medische gegevens van uw kind. Dit beperkt zich enkel tot gegevens die nodig zijn om in noodgevallen goed te kunnen handelen. U kunt bijvoorbeeld doorgeven dat uw kind epilepsie heeft, zodat wij adequaat kunnen optreden in noodsituaties. OZHW zal u nooit dwingen dergelijke gegevens te overleggen.

1.3. Hoe gaan wij om met de gegevens van uw kind

1. Bij het verwerken van de gegevens gaan wij altijd uit van noodzakelijkheid, wij zullen niet meer gegevens verwerken dan noodzakelijk is om onze rechten en plichten als onderwijsinstelling na te komen. Dit betekent ook dat we de gegevens niet zullen gebruiken voor andere doeleinden dan wij in deze toelichting noemen.
2. In een aantal gevallen zijn wij, zoals eerder aangegeven, verplicht om gegevens van uw kind te delen met andere organisaties. Dit zijn onder andere DUO, leerplicht, de onderwijsinspectie, GGD/schoolarts, samenwerkingsverband en accountant.
3. Wij kunnen commerciële derde partijen verzoeken om te ondersteunen bij het verwerken van de gegevens voor de eerder genoemde doeleinden. Denk hierbij aan applicaties om leerlingen in de les te ondersteunen, een administratie systeem waarbij de gegevens niet op ons eigen netwerk worden opgeslagen, maar bij een andere organisatie of een lesroosterprogramma. Dit gebeurt altijd in opdracht en onder de verantwoordelijkheid van OZHW. Met deze organisaties sluiten we overeenkomsten af, waarin o.a. is vastgelegd welke gegevens er verwerkt worden en hoe deze gegevens beveiligd worden.
4. Wij zullen de gegevens van uw kind niet delen met commerciële derde partijen voor andere doeleinden. Ook zullen wij de gegevens van uw kind nooit verkopen of verhuren aan derde partijen.
5. De persoonsgegevens worden zoveel mogelijk gecodeerd bewaard en alleen die medewerkers kunnen bij de gegevens, die dat ook voor de uitvoering van hun werk nodig hebben. Daarnaast bewaren wij de gegevens niet langer dan noodzakelijk is. Wij hanteren hiervoor verschillende bewaartermijnen die wettelijk geregeld en vastgesteld zijn. De bewaartermijn van gemaakte examens is bijvoorbeeld 2 jaar na het beëindigen van de onderwijsovereenkomst. Gegevens uit de leerling administratie worden over het algemeen 7 jaar bewaard. Als u er belangstelling voor heeft kunnen wij u een overzicht hiervan geven.

1.4. Welke rechten hebben een leerling en ouders van leerlingen jonger dan 16 jaar

1. Als ouders heeft u een aantal rechten als het gaat om persoonsgegevens. Deze rechten zijn in de wet vastgelegd. Leerlingen en/of ouders kunnen op elk moment gebruik maken van deze rechten. Dit betekent bijvoorbeeld dat u altijd een verzoek kunt indienen om inzage te krijgen in de gegevens die wij van uw kind verwerken.
2. Daarnaast kunt u ook een verzoek indienen om gegevens te rectificeren, te beperken of helemaal te wissen uit de systemen van OZHW. U heeft altijd het recht om onjuiste gegevens aan te vullen of te verbeteren. Wij zullen er vervolgens voor zorgen dat deze gegevens ook bij organisaties waarmee wij deze gegevens van uw kind delen en/of uitwisselen worden aangepast.
3. Als u ons verzoekt om gegevens van uw kind te beperken of te wissen, zullen wij toetsen of dit mogelijk is. In deze toets houden wij ons aan de wettelijke voorschriften en kijken wij bijvoorbeeld of wij geen wettelijke plicht hebben om de gegevens te bewaren.
4. Tevens heeft u het recht om te vragen om de gegevens, die wij van uw kind verwerken en wij van u hebben ontvangen, aan u over te dragen of op uw verzoek aan een andere organisatie over te dragen.
OZHW zal geen besluiten nemen over uw kind, die alleen gebaseerd zijn op geautomatiseerde verwerking van gegevens (profiling). Beslissingen worden nooit zonder menselijke tussenkomst genomen.

Als u het niet eens bent met hoe wij omgaan met de gegevens van uw kind, dan kunt u altijd opheldering vragen bij onze Functionaris voor Gegevensbescherming (zie de contactgegevens bovenaan deze toelichting). Indien uw probleem volgens u niet goed wordt opgelost, dan kunt u dat melden bij Autoriteit voor de Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

1.5. Opsomming van de categorieën van persoonsgegevens:

Categorie	**Toelichting**
1. Contactgegevens	**1a:** naam, voornaam, e-mail, opleiding *(bv. sector techniek)*; **1b:** geboortedatum, geslacht; **1c:** overige gegevens te weten: adres, postcode, woonplaats, telefoonnummer en eventueel andere voor communicatie benodigde gegevens, alsmede ook een bankrekeningnummer voor het afhandelen van betalingen**;**
2. Leerling nummer	Een administratienummer dat geen andere informatie bevat dan bedoeld onder categorie 1
3. Nationaliteit en geboorteplaats	
4. Ouders, voogd	Contact gegevens van de ouders/verzorgers van leerlingen (naam, adres, postcode, woonplaats, telefoonnummer en e-mailadres)
5. Medische gegevens	Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling, indien van belang zijn bij het nemen van aanvullende maatregelen om goed onderwijs te kunnen volgen (bv. extra tijd bij toetsen);
6. Godsdienst	Gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor het te volgen onderwijs (bijvoorbeeld: leerling vrij op bepaalde dag).
7. Studievoortgang	Gegevens betreffende de aard en het verloop van het onderwijs en de behaalde studieresultaten te weten: • Examinering (gegevens rondom het examen) • Studietraject • Begeleiding leerling (inclusief ontwikkelperspectief OPP) • Aanwezigheidsregistratie • Medisch dossier (papier) • Klas, leerjaar, opleiding
8. Onderwijsorganisatie	Gegevens met het oog op het organiseren van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen; hieronder vallen ook lesroosters, boekenlijsten, schoolpasjes etc.
9. Financiën	Gegevens voor het berekenen, vastleggen en innen van inschrijvingsgelden, school- en/of lesgelden, bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten. (denk hierbij aan een bankrekeningnummer van de ouders)

10. Beeldmateriaal	Foto's en videobeelden (met of zonder geluid) van activiteiten van de school op basis van toestemming. **Let op:** Voor pasfoto voor identificatiedoeleinden is geen toestemming nodig (schoolpas en als aanvulling op het dossier).
11. Docent/ Decaan/ Mentor/ IB-er/ Zorgcoördinator	Gegevens van **docenten en begeleiders,** voor zover deze gegevens van belang zijn voor de organisatie van de instelling en het geven van onderwijs, opleidingen en trainingen
12. BSN (PGN)	In het onderwijs heet het BSN het persoonsgebonden nummer (PGN). Ook wel *onderwijsnummer* genoemd. Het PGN is hetzelfde nummer als het BSN. Scholen zijn verplicht het PGN te gebruiken in hun administratie.
13. Keten-ID (Eck-Id)	Unieke iD voor de 'educatieve contentketen'. Hiermee kunnen scholen gegevens delen, zonder dat ze direct herleidbaar zijn naar leerlingen of docenten.
14 Overige gegevens, te weten ….	Andere dan de onder 1 tot en met 11 bedoelde gegevens waarvan de verwerking wordt vereist of noodzakelijk is met het oog op de toepassing van een andere wet. Deze zullen apart vermeld en toegelicht worden.

OZHW PROTOCOL VOOR SOCIAL MEDIA, VASTGESTELD DOOR CvB, 17 MAART 2020

INLEIDING

Onderwijsgroep Zuid Hollandse Waarden voor PO en VO, hierna te noemen OZHW, is zich ervan bewust dat sociale media een onlosmakelijk onderdeel zijn van de huidige samenleving en de leefomgeving van haar studenten, leerlingen en hun ouders. Waar OZHW wordt genoemd kan ook worden gelezen “de school of de scholen behorend tot OZHW”. OZHW verstaat onder sociale media een verzamelbegrip van huidige en toekomstige online platforms waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen. Onder de noemer sociale media worden op dit moment onder andere weblogs of blogs, WhatsApp, videosites als YouTube, Vimeo, fora, op samenwerking gebaseerde projecten als Wikipedia, en sociale netwerken als Facebook, Twitter en Instagram geschaard. Via deze media worden verhalen, kennis, ervaringen en beeld en/of geluidmateriaal gedeeld. OZHW ziet het (mede) als haar verantwoordelijkheid leerlingen te leren de voordelen van sociale media te benutten, maar ook om de nadelen bespreekbaar te maken en zoveel mogelijk te beperken. Alle betrokkenen nemen de reguliere fatsoensnormen tegenover betrokkenen van de onderwijsinstelling in acht. Indien handelingen worden verricht die in strijd zijn met de reguliere fatsoensnormen en/of (mogelijk) een strafbaar karakter hebben (bijvoorbeeld: hacken van een account, radicalisering, sexting, pesten, stalken, bedreigen, het verspreiden van memes of anderszins beschadigen) dan neemt de onderwijsinstelling passende maatregelen. Indien een betrokkene kennis heeft van ontoelaatbare en/of grensoverschrijdende communicatie in woord, beeld en/of geluid dan dient hij dat te melden bij de schoolleiding of het bestuur. Om een kader en richtlijnen aan te geven heeft OZHW het protocol sociale media opgesteld met als doel de positieve elementen van sociale media te waarborgen en mogelijke schadelijke effecten daarvan te voorkomen.
Met de invoering van de Algemene Verordening Gegevensbescherming (AVG), 25 mei 2018, is het door OZHW verspreiden van persoonsgegevens, geluid- en beeldmateriaal van personen, zonder de uitdrukkelijke toestemming van de betrokkene, verboden. Dit heeft invloed op het gebruik van de sociale media door OZHW. Sociale media bieden een mogelijkheid om te laten zien dat je trots bent op je school en kunnen een bijdrage leveren aan een positief imago van OZHW. Sociale media worden door veel mensen dan ook gebruikt voor de onderlinge communicatie. Indien sociale media voor onderwijsdoeleinden, werving en selectie of bedrijfsvoering worden gebruikt, dient dit – met het oog op de bescherming van leerlinggegevens – plaats te vinden conform het Privacyreglement OZHW.

Artikel 1. UITGANGSPUNTEN

1. OZHW onderkent het grote belang en de impact van sociale media en wil voldoen aan de wet- en regelgeving op het terrein van de privacy.
2. De doelstelling van dit protocol is een bijdrage te leveren aan een goed en veilig school- en onderwijsklimaat. 3.
3. Dit protocol bevordert dat de scholen van OZHW sociale media gebruiken zonder inbreuk te maken op de privacy van medewerkers, studenten, leerlingen en ouders.
4. Medewerkers, studenten, leerlingen en ouders wordt gevraagd op sociale media te communiceren op een wijze die niet strijdig is met de missie en visie van de scholen en de reguliere fatsoensnormen. Dat betekent dat we respect voor de school en elkaar hebben en iedereen in zijn/haar waarde laten.
5. De gebruikers van sociale media houden rekening met de goede naam van de school en van eenieder die betrokken is bij de school.
6. Het protocol dient ervoor OZHW, haar medewerkers, studenten, leerlingen en ouders te beschermen tegen de mogelijke negatieve gevolgen van sociale media door uitingen van henzelf of van andere betrokkenen.

Artikel 2 DOEL EN REIKWIJDTE

1. Deze gedragsregels zijn bedoeld voor alle betrokkenen die deel uitmaken van OZHW, dat wil zeggen medewerkers met en zonder dienstverband, leerlingen, ouders/verzorgers, stagiaires en mensen die op een andere manier verbonden zijn aan OZHW (zzp-ers en consultants) ongeacht de plaats waar zij hun sociale media gebruiken.
2. De richtlijnen in dit protocol hebben betrekking op alle berichten en beelden die direct of indirect gerelateerd

zijn aan OZHW, zowel binnen als buiten school- en werktijden.

Artikel 3 GEBRUIK VAN SOCIALE MEDIA DOOR DE ORGANISATIE EN MEDEWERKERS

1. OZHW maakt gebruik van sociale media in het kader van PR-activiteiten met het doel om positieve informatie te verspreiden over de (activiteiten) van de scholen of organisatie en om zich te profileren in haar markt
2. OZHW maakt verder geen gebruik van sociale media, maar ziet zich genoodzaakt vooralsnog de volgende uitzondering toe te staan. Medewerkers mogen, rekening houdend met de geldende privacywetgeving, een professionele WhatsApp-groep aanmaken ten behoeve van internationalisering en onderwijsactiviteiten (stage, externe opdrachten, buitenschools activiteiten, huiswerk, rooster[wijzigingen], agendabeheer), om het "leren leren" te bevorderen en om de veiligheid van de leerlingen/studenten te kunnen waarborgen. Op deze WhatsAppgroep mogen alleen bijzondere aangelegenheden worden uitgewisseld, zoals tijden, bereikbaarheid en standplaatsen. De leerlingen die om welke reden dan ook geen deel kunnen uitmaken van deze Whatsappgroep worden op een andere wijze door de medewerker op de hoogte gesteld. Op deze Whatsappgroep zullen geen foto's worden uitgewisseld.
3. De school maakt ruimte in het onderwijsleerproces voor het gebruik van sociale media in de lessen om de leerlingen en studenten zelf de (on)mogelijkheden van sociale media te laten ontdekken, de voor- en nadelen bespreekbaar te maken en content, bijvoorbeeld in de vorm van You Tube filmpjes te gebruiken als leermiddel, als dit relevant is voor een bepaald onderwerp. De voorschriften van dit protocol zijn deels niet van toepassing voor zover het lesgeven over omgang met sociale media niet anders kan dan met het overtreden van een of meer clausules uit het protocol
4. Zonder uitdrukkelijke toestemming van betrokkenen (schriftelijk of in de vorm van een digitaal akkoord vastgelegd in de leerlingadministratiesysteem) worden door de instelling geen persoonsgegevens, maar ook geen geluid- of beeldmateriaal waarbij personen herkend kunnen worden, op sociale media geplaatst. Ouders van leerlingen tot 16 jaar en leerlingen vanaf 16 jaar beheren daarbij zelf hun toestemming in de Leerling administratiesystemen Magister, SomToday en Parro (module binnen ParnasSys). Voor activiteiten die hierin niet gedefinieerd worden bewaren de scholen de schriftelijke toestemming, welke wordt gevraagd aan de ouders en leerlingen vanaf 16 jaar, om hierover verantwoording te kunnen afleggen.
5. Als medewerkers eigen vakinhoudelijke, digitale content ontwikkelen, wordt van medewerkers verwacht deze ter beschikking te stellen voor andere OZHW-collega's.
6. Het komt voor dat medewerkers eigen YouTube-kanalen, websites of dergelijke media hebben opgezet en van content hebben voorzien. OZHW is niet verantwoordelijk voor deze media en de content. Het is medewerkers verboden via deze media persoonsgegevens te plaatsen of te verspreiden.

Artikel 4 GEBRUIK VAN SOCIALE MEDIA BINNEN OZHW / DE SCHOOL ALLE GEBRUIKERS

Onder alle gebruikers verstaan we medewerkers met en zonder dienstverband, studenten, leerlingen, ouders/verzorgers, stagiaires en mensen die op een andere manier verbonden zijn aan OZHW, als bijv. zzp-ers en consultants.

1. Het is niet toegestaan sociale media accounts op naam van OZHW of een van haar scholen, locaties of afdelingen aan te maken of daarbij de naam van OZHW op welke manier dan ook te gebruiken.
2. Medewerkers en leerlingen zijn tijdens de onderwijsactiviteiten niet actief op sociale media, behoudens in situaties toegestaan in artikel 3, en maken geen gebruik van mobiele telefoons of daarmee vergelijkbare communicatieapparatuur, tenzij de apparatuur gebruikt wordt ten behoeve van de onderwijsactiviteiten.
3. Het persoonlijk gebruik van sociale media is alleen toegestaan in de openbare ruimtes, zoals de aula, kantine, gangen en garderobe.
4. Het is niet toegestaan om persoonsgegevens, foto-, film- en geluidsopnamen van personen of school gerelateerde situaties op de sociale media te zetten. Dit geldt ook voor beeldmateriaal dat wordt gemaakt in de klas voor professionalisering- en opleidingsdoeleinden van docenten en stagiaires. Een uitzondering wordt gemaakt voor situaties toegestaan in artikel 3.
5. Het is betrokkenen toegestaan om kennis en informatie te delen, mits het andere betrokkenen niet schaadt
6. Betrokkenen zorgen ervoor dat ze weten hoe sociale media werken voordat ze deze gebruiken. Ook zorgen zij ervoor dat de instellingen van het gebruikte sociale medium zo zijn ingesteld dat niet meer informatie wordt

gedeeld dan gewenst.
7. De betrokkene is persoonlijk verantwoordelijk voor de inhoud die hij/zij publiceert op sociale media. Ook het doorsturen (forwarden), herplaatsen (retweeten) e.d. valt daar onder.
8. Elke betrokkene moet zich ervan bewust zijn dat de gepubliceerde teksten en uitlatingen voor onbepaalde tijd openbaar zullen zijn, ook na verwijdering van het bericht. De schade aan betrokkenen of OZHW kan dan (misschien onbedoeld) groot zijn.
9. Bij het persoonlijk gebruik in school van sociale media is het niet toegestaan om:
   a. sites te bezoeken of informatie te downloaden en te verspreiden die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend zijn;
   b. te hacken en ongeoorloofd toegang te krijgen tot niet-openbare sites of programma's;
   c. informatie, foto's of video's te delen waarvan duidelijk is dat die niet bedoeld zijn om verder te verspreiden of waarmee inbreuk wordt gemaakt op beeld- auteurs- of citaatrechten;
   d. verzonnen berichten te versturen of een fictieve naam te gebruiken als afzender;
   e. iemand lastig te vallen, te achtervolgen of te 'flamen' (het plaatsen van berichten die met opzet aanvallend of beledigend zijn).
10. Alle betrokkenen nemen de normale fatsoensnormen in acht. Als fatsoensnormen worden overschreden (bijvoorbeeld: mensen pesten, kwetsen, stalken, bedreigen, zwartmaken of anderszins beschadigen) dan neemt OZHW passende maatregelen.
11. Betrokkenen zijn zich bewust dat zij ook op sociale media ambassadeurs zijn van OZHW.

Artikel 5 GEBRUIK VAN SOCIALE MEDIA BINNEN OZHW / DE SCHOOL MEDEWERKERS SPECIFIEK
1. Medewerkers hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media: privé-meningen van medewerkers kunnen eenvoudig verward worden met de officiële standpunten van de school. Van medewerkers wordt verwacht dat ze zich hiervan bewust zijn en er zorgvuldig mee omgaan.
2. Voorts is het medewerkers niet toegestaan om traditionele media, zoals radio, tv, krant, zonder toestemming van leidinggevende/directie vooraf te woord te staan. Bij een verzoek daartoe dient onmiddellijk overleg worden gezocht met de directie van de school.
3. Door de medewerker worden geen persoonsgegevens, geluid- of beeldmateriaal van andere personen op sociale media geplaatst. Een uitzondering wordt gemaakt voor situaties toegestaan in artikel 3.
4. Als online communicatie op welke manier dan ook dreigt te ontsporen neemt de medewerker direct contact op met zijn/haar leidinggevende om vervolgstappen te bespreken. Deze neemt contact op met zijn/haar directeur van de school alsmede de Functionaris Gegevensbescherming (FG) van OZHW.
5. Bij twijfel of een publicatie in strijd is met deze richtlijnen neemt de medewerker contact op met zijn/haar leidinggevende. Deze neemt contact op met de Functionaris Gegevensbescherming (FG) van OZHW.
6. Medewerkers dragen via sociale media in hun rol als medewerkers geen standpunten en/of overtuigingen uit die in strijd zijn met de missie en visie van OZHW en de uitgangspunten van dit protocol.
7. Als de medewerker deelneemt aan een discussie die (op enigerlei wijze) te maken heeft met de onderwijsinstelling vermeldt hij/zij dat hij/zij medewerker is van OZHW.
8. Medewerkers is het niet toegestaan om 'vrienden' te worden met leerlingen op sociale media via hun privédomeinen of -pagina's. De pedagogisch-didactische relatie staat dit in de weg.
9. De medewerker onderhoudt via sociale media geen privé-contacten met leerlingen of ouders/verzorgers.

Artikel 6 MAATREGELEN EN GEVOLGEN VOOR MEDEWERKERS EN LEERLINGEN
1. Medewerkers die in strijd handelen met dit protocol maken zich mogelijk schuldig aan plichtsverzuim. Alle correspondentie omtrent dit onderwerp wordt opgenomen in het personeelsdossier.
2. Als OZHW, na consultatie van de leidinggevende en in overleg met het College van Bestuur, de wijze van communiceren door een medewerker als 'grensoverschrijdend' beschouwt, dan wordt dit telefonisch gemeld bij de Landelijke Vertrouwensinspecteur (0900 - 1113111).
3. Afhankelijk van de ernst van de uitlatingen, gedragingen en gevolgen worden naar medewerkers toe rechtspositionele maatregelen genomen die kunnen variëren van waarschuwing, schorsing, berisping tot ontslag en ontslag op staande voet.
4. Leerlingen en/of ouders/verzorgers die in strijd met dit protocol handelen maken zich mogelijk schuldig aan

verwijtbaar gedrag. Alle correspondentie omtrent dit onderwerp wordt opgenomen in het leerlingendossier.
5. Afhankelijk van de ernst van de uitlatingen, gedragingen en gevolgen worden naar leerlingen en/of ouders/verzorgers toe maatregelen genomen die kunnen variëren van waarschuwing, schorsing tot verwijdering van school.
6. Indien de uitlating van medewerkers, leerlingen en/of ouders/verzorgers mogelijk een strafrechtelijke overtreding inhoudt zal door OZHW aangifte bij de politie worden gedaan.
7. Controle door OZHW is mogelijk. Het College van Bestuur beslist of gegevens op persoonsniveau mogen worden gecontroleerd. Als die toestemming is gegeven bepaalt vervolgens de directie van de school welke acties worden ondernomen. Het College van Bestuur kan binnen het Onderwijs Service Bureau één of meerdere personen autoriseren tot het uitvoeren van controles onder geheimhoudingsplicht

PROTOCOL EMAIL, NETWERK EN INTERNETGEBRUIK (VASTGESTELD door CvB op 17 MAART 2020)

Artikel 1 DEFINITIES, DOEL EN WERKING

1. Dit protocol bevat een regeling voor het gebruik van het computernetwerk, e-mail en internet door medewerkers en leerlingen van OZHW, alsmede voor derden die gebruik maken van het computernetwerk, e-mail en internet van OZHW.
2. Deze regeling omvat gedragsregels voor verantwoord gebruik van het computernetwerk, e- mail en internet en geeft regels over de wijze waarop controle plaatsvindt
3. Het protocol is opgesteld conform de Algemene Verordening Gegevensbescherming (AVG) van 25 mei 2018, als opvolger van de Wet Bescherming Persoonsgegevens.
4. Het protocol bevat regels voor en afspraken over het computergebruik door medewerkers en leerlingen van OZHW, alsmede voor derden die gebruik maken van het computernetwerk, e- mail en internet van het OZHW (hierna gebruikers genoemd) en over de manier waarop OZHW omgaat met het registreren, verzamelen en monitoren van tot een persoon herleidbare data inzake het gebruik van hardware, software, e-mail en internet. Doelstelling hiervan is een goede balans te vinden tussen een verantwoord gebruik van internet en e-mail en de bescherming van de privacy van gebruikers op de werkplek.
5. Onverantwoord gebruik is gebruik dat tegenstrijdig is aan de doelstelling en identiteit van de school, zowel in persoonlijk gebruik als in relatie tot anderen binnen of buiten de school. Hierbij wordt in het bijzonder gedacht aan illegale toepassingen van bestanden, godslasterlijke, beledigende, aanstootgevende, gewelddadige, racistische, discriminerende, intimiderende, pornografische toepassingen, zinloos tijdverdrijf en toepassingen die strijdig zijn met de wet of als onethisch aan te merken zijn.
6. De controle op persoonsgegevens bij gebruik van het computernetwerk, e-mail en internet vindt plaats met als doel:
    - systeem- en netwerkbeveiliging;
    - tegengaan van onverantwoord gebruik.
7. Het protocol geldt voor alle gebruikers die op welke wijze dan ook gebruik maken van het netwerk van het OZHW.
8. Het protocol behelst e-mail, netwerk- en internetgebruik. Hieronder wordt verstaan ieder gebruik van de door het OZHW geboden faciliteiten: het gebruik van het netwerk van OZHW, het gebruik van het zakelijke e-mailadres en het gebruik maken van toegang tot internet.

Artikel 2 ALGEMENE UITGANGSPUNTEN

1. Gegevens die tot een persoon herleidbaar zijn, zullen niet worden geregistreerd, verzameld, gecontroleerd, gecombineerd dan wel bewerkt, anders dan in dit protocol is afgesproken.
2. Persoonsgegevens zullen alleen gebruikt worden voor het doel waarvoor ze verzameld zijn passend binnen de Algemene Verordening Gegevensbescherming.
3. Het registreren van gegevens die tot een persoon herleidbaar zijn, wordt tot het minimum beperkt. Hierbij wordt gestreefd naar een maximale bescherming van de privacy van de gebruikers op de werkplek.
4. Indien dit uit een oogpunt van noodzakelijk te verrichten werkzaamheden onvermijdelijk is, is het aan het beheer van het netwerk toegestaan om persoonlijke data van gebruikers tijdelijk ontoegankelijk te maken. Anders dan in acute noodsituaties, worden gebruikers tijdig op de hoogte gebracht van deze tijdelijke ontoegankelijkheid.
5. Persoonsgegevens over gebruik van het computernetwerk, e-mail en internet worden niet langer bewaard dan noodzakelijk.
6. Met het opslaan van de e-mails worden ook persoonsgegevens verzameld. Het ligt in de aard van e- mail dat de inhoud ook bijzondere persoonsgegevens kan bevatten. Op verzoek kunnen e-mails met bijzondere persoonsgegevens eerder worden vernietigd.
7. De schoolleiding treft voorzieningen voor de positie en integriteit van de systeembeheerder. Dit wordt geconcretiseerd door de systeembeheerder alleen technisch verantwoordelijk te laten zijn en dit laat onverlet het bepaalde in artikel 6.5.

Artikel 3 ALGEMENE BEPALINGEN t.a.v. GEBRUIKERS

1. Alle medewerkers en leerlingen van OZHW hebben toegang tot het computernetwerk. Ook derden kan toegang worden verschaft tot het netwerk.
2. De eerste keer dat iemand gebruik maakt van het computernetwerk wordt beschouwd als de totstandkoming

van een overeenkomst tussen OZHW en de gebruiker, waarbij de gebruiker instemt met de in dit protocol verwoorde regels en afspraken.
3. Het recht om gebruik te maken van het computernetwerk vervalt zodra iemand geen medewerker of leerling meer is van OZHW zoals beschreven in artikel 3.1.
4. Het computernetwerk kan door gebruikers worden benaderd op daartoe ingerichte werkplekken alsmede via de eigen laptop door middel van gebruikmaking van het draadloze netwerk.

Artikel 4 EMAIL EN INTERNETGEBRUIK GEBRUIKERS
1. Alle gebruikers van het netwerk mogen het e-mailsysteem en de toegang tot internet kortstondig, beperkt en incidenteel gebruiken voor niet-zakelijk (ofwel persoonlijk) verkeer voor het ontvangen en versturen van persoonlijke mailberichten, zowel intern als extern, mits dit niet storend is voor de dagelijkse werkzaamheden, voor anderen en het de goede werking van het netwerk niet verstoort en mits in overeenstemming met het bepaalde in deze regeling.
2. Het recht van de gebruiker om persoonlijke e-mailberichten te ontvangen en te versturen is gebonden aan de voorwaarde dat het niet is toegestaan dreigende, seksueel intimiderende, racistische dan wel andere berichten te versturen die in strijd zijn met de algemeen geldende normen en waarden en de huisregels van OZHW.
3. Het ontvangen en verzenden van persoonlijke e-mail dient voorts te geschieden met inachtneming van het bepaalde in artikel 1.
4. OZHW behoudt zich het recht voor de toegang tot bepaalde sites te beperken en/of te verbieden. Met name sites met een pornografische, racistische, discriminerende of op entertainment gerichte inhoud zullen worden geweerd.
5. Medewerkers van de afdeling ICT van OZHW zullen in principe niet de inhoud van persoonlijke en van zakelijke e-mailberichten lezen. Gegevens over het aantal mails, de e- mailadressen en andere data hieromtrent worden wel geregistreerd, voor zover dat vereist is in verband met wettelijke of contractuele verplichtingen. Dit laat onverlet dat controles op incidentele basis (steekproef) of vanwege een zwaarwichtige reden kunnen plaatsvinden. Hiervan wordt altijd vooraf melding gemaakt bij de directie door (een medewerker van) de afdeling ICT.
6. Voor het gebruik van e-mail geldt verder:
- Alleen het e-mailadres dat door de organisatie is toegewezen aan de gebruiker mag worden gebruikt. Bij communicatie via e-mail moet herleidbaar zijn wie de afzender is.
- De afzender is verantwoordelijk voor een juiste adressering van zijn of haar informatie.
- De normale gedragsregels, die gelden voor schriftelijke correspondentie (zoals correct taalgebruik) zijn ook van toepassing op e-mail en andere toepassingen (zoals nieuwsgroepen).
- Alle regels voor elektronische informatie gelden tevens voor bijlagen.
- Verzending van vertrouwelijke informatie of gevoelige informatie via e-mail is niet toegestaan.

Artikel 5 GEDRAGSREGELS / BEWUST ZIJN VAN DE RISICO'S VAN INTERNETGEBRUIK
1. Het internet is een open infrastructuur die voor iedereen toegankelijk is. De gebruiker moet zich ervan bewust zijn dat de betrouwbaarheid (beschikbaarheid, integriteit en exclusiviteit) van informatie op het internet niet altijd gewaarborgd is en dat alle activiteiten die de gebruiker op internet ontplooit, bekeken en vastgelegd kunnen worden door vele partijen. Berichtgeving die gevoelige informatie of persoonsgegevens bevat, zoals bedoeld in de Algemene Verordening Gegevensbescherming (AVG), mag niet per e-mail of internet worden verzonden, tenzij dit gebeurt via een veilige, gecodeerde verbinding.
Verder vraagt de kwetsbaarheid van de infrastructuur van internet om speciale aandacht op tenminste de volgende punten:
a. gebruikersnaam (inlognaam) en wachtwoord zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven; de geregistreerde gebruiker is verantwoordelijk voor alle acties die met behulp van zijn/haar gebruikersnaam worden uitgevoerd;
b. het downloaden en uploaden applicaties is niet toegestaan, tenzij vooraf schriftelijke toestemming is verleend door de verantwoordelijke en het hoofd van de afdeling ICT.
2. Onbedoelde inbreuken op beveiliging, van binnenuit of vanuit de buitenwereld, dienen aan een medewerker van de afdeling ICT gemeld te worden, via Security@ozhw.nl.
3. Het is in het bijzonder niet toegestaan op internet:
a. sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal

bevatten;
b. pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal dat op de een of andere manier in strijd is met de grondslagen van OZHW te bekijken, te uploaden, downloaden of te verspreiden;
c. spelletjes en muziekbestanden te uploaden, downloaden, uit te wisselen of uit te voeren, te winkelen, te gokken, deel te nemen aan kansspelen en/of chat-/babbelboxen te bezoeken, tenzij zoiets past in het kader van onderwijsactiviteiten;
d. zich ongeoorloofd toegang te verschaffen tot niet-openbare bronnen op het netwerk van OZHW of het internet;
e. opzettelijk informatie, waartoe men via het netwerk en/of internet toegang heeft verkregen, zonder toestemming te veranderen of te vernietigen.

Indien ongevraagd informatie wordt aangeboden die voldoet aan bovengenoemde beschrijvingen dient dat aan een medewerker van de afdeling ICT gemeld te worden. Het is bovendien niet toegestaan om door middel van e-mail:

a. berichten anoniem of onder een fictieve naam te versturen; dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten en ketting e- mailberichten te verzenden of door te sturen;
b. iemand elektronisch lastig te vallen.

Het is ook niet toegestaan op een andere manier op internet handelingen te verrichten die in strijd zijn met de wet of onethisch te handelen.

4. De gebruiker verplicht zich de computer waarop hij/zij gewerkt heeft te blokkeren of af te sluiten teneinde het ongeautoriseerde gebruik van het netwerk te voorkomen. Dit geldt ook voor laptops in eigendom van een gebruiker.

5. Het is niet toegestaan om foto's, video's of ander materiaal van op school werkzame personen, leerlingen of andere bij de school betrokkenen via elektronische informatie- en communicatiemiddelen bekend te maken. Voor het bekend maken van foto's waarop personen zijn afgebeeld, is voorafgaande toestemming van betrokkene of diens wettelijke vertegenwoordiger vereist.

Artikel 6 CONTROLE

1. Controle op gebruik van elektronische informatie- en communicatiemiddelen vindt slechts plaats in het kader van in artikel 1 genoemde doelen.

2. De schoolleiding informeert de gebruikers voorafgaand aan de invoering van de regeling over controle op elektronische informatie- en communicatiemiddelen, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling.

3. Niet toegestaan gebruik van elektronische informatie- en communicatiemiddelen wordt zo veel mogelijk technisch onmogelijk gemaakt.

4. Als een lid van de schoolleiding of de systeembeheerder merkt, of er op geattendeerd wordt, dat het email- en internetgedrag of het gebruik van het computernetwerk van een gebruiker niet binnen deze kaders verloopt, wordt de gebruiker hier op gewezen en wordt een controle van zijn e-mail en internetacties door bevoegde personen als mogelijkheid genoemd. Hiervan wordt melding gemaakt bij het bestuur. Het bestuur kan besluiten tot het instellen van een onderzoek en wijst medewerkers aan die daarmee worden belast, zij zijn gebonden aan strikte geheimhouding. Uitkomsten van dat onderzoek worden bij het bestuur gemeld.

5. Elektronische informatie- en communicatieberichten van de (bovenschoolse) schoolleiding, bestuursleden, vertrouwenspersonen en andere medewerkers met een vertrouwensfunctie, gecommuniceerd in het kader van hun functie, zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle bij een ernstig vermoeden van misbruik.

6. De geanonimiseerde rapportage wordt verstrekt aan de schoolleiding en aan het hoofd ICT. De schoolleiding kan naar aanleiding van deze rapportage vragen om een gepersonaliseerde rapportage.

7. Indien een gebruiker of een groep gebruikers ervan wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden (zie lid 4). De schoolleiding meldt dit aan het bestuur.

8. Het bestuur geeft indien nodig aan het hoofd ICT de opdracht om de elektronische informatie- en communicatiemiddelenacties van de betrokkene na te gaan.

9.De uitkomst van het onderzoek genoemd bij lid 4 wordt schriftelijk vastgelegd en gedeeld met het bestuur.

10. Gebruikers bij wie geconstateerd is dat zij zich niet aan deze regeling houden, worden zo spoedig mogelijk door de leidinggevende of de schoolleiding op hun gedrag aangesproken.

11. Binnenkomend en e-mailverkeer wordt zo goed mogelijk gecontroleerd op virussen en soortgelijk ongerief. Indien een e-mailbericht een virus bevat dan wordt dat bericht automatisch tegengehouden. Verzender en ontvanger worden zo mogelijk daarover ingelicht. Indien desondanks een e-mail wordt ontvangen dat mogelijk een virus bevat, dan dient de ontvanger zo snel mogelijk contact op te nemen met de afdeling ICT van OZHW.
12. Voor zover noodzakelijk worden derden ingeschakeld bij onderzoek en controlewerkzaamheden.

Artikel 7 SANCTIES

1. In eerste instantie geldt hier de gedragscode van OZHW.
2. Bij handelen in strijd met deze regeling, het schoolbelang of de algemeen geldende normen en waarden voor het gebruik van het netwerk, internet en e-mail, kunnen afhankelijk van de aard en de ernst van de overtreding maatregelen worden getroffen:

a. Voor medewerkers van OZHW gaat het eventueel om disciplinaire en arbeidsrechtelijke maatregelen zoals berisping, schorsing of beëindiging van de arbeidsovereenkomst.
b. Voor leerlingen zijn maatregelen denkbaar als tijdelijke of permanente ontzegging van de toegang tot het netwerk of tot internet.
c. Daarnaast kunnen voor leerlingen ook maatregelen getroffen worden zoals schorsing op grond van overtreding van de huis- en orderegels als bedoeld in het schoolreglement.
d. De meest vergaande sanctie voor leerlingen is verwijdering van de school. Aan derden kan de toegang tot het netwerk worden ontzegd.

3. Het is medewerkers van de afdeling ICT toegestaan om verboden, niet-zakelijk of aanstootgevend materiaal, bij wijze van voorlopige maatregel, direct te blokkeren.

Artikel 8 RECHTEN VAN DE GEBRUIKERS

1. Op grond van de Algemene Verordening Gegevensbescherming (AVG) hebben betrokkenen ten aanzien van de verwerking van persoonsgegevens de navolgende rechten. OZHW heeft deze rechten vastgelegd in het Protocol Inzageverzoek OZHW d.d. 28 mei 2019, te weten:

- Inzagerecht:
- Recht op dataportabiliteit;
- Kopierecht:
- Recht om vergeten te worden / Verwijderingsrecht;
- Recht om minder gegevens te verwerken;
- Bezwaarrecht;
- Correctierecht

PROTOCOL INZAGEVERZOEK OZHW (VASTGESTELD 28-05-2019)

OZHW voor PO en VO erkent in haar Privacyreglement , art.15 (bijlage 2) de rechten van betrokkenen en benoemt de mogelijkheid van een verzoek tot inzage. Een inzageverzoek is onderdeel van de 'rechten van betrokkene'. Naast het inzagerecht heeft de betrokkene ook het recht om gegevens over te kunnen dragen (dataportabiliteit), het recht om vergeten te worden, het recht op verbetering en aanvulling van gegevens, het recht om minder gegevens te verwerken en het recht om bezwaar te maken tegen gegevensverwerking. De betrokkene die een inzageverzoek indient heeft het recht op een document te ontvangen waarin OZHW een aantal zaken benoemt

OZHW mag geen kosten rekenen voor het behandelen van dit verzoek. De enige reden op basis waarvan een verzoek mag worden geweigerd is als deze ongegrond is of als het verzoek buitensporig van aard is. Een verzoek is ongegrond als een ouder/verzorger, leerling ouder dan 16 jr. of werknemer op basis van de AVG een verzoek in zou dienen voor een andere persoon. Een verzoek is bijvoorbeeld buitensporig als herhaaldelijk verzoeken tot inzage worden ingediend.

OZHW is verplicht om opvolging te geven aan inzageverzoeken van betrokkenen. Als het verzoek niet of niet-tijdig in behandeling wordt genomen, kan de betrokkene een klacht in dienen bij de Autoriteit Persoonsgegevens. Als na onderzoek van de Autoriteit Persoonsgegevens blijkt dat de rechten van de betrokkene worden geschonden, kan een boete worden opgelegd van maximaal €20.000.000,- of 4% van de jaaromzet als dit bedrag hoger is dan €20.000.000,- (artikel 83 lid 5 sub b AVG). De praktijk leert dat de Autoriteit niet direct overgaat tot het opleggen van een boete, maar een redelijke termijn geeft om de overtreding (van de AVG) te beëindigen..

Conclusie
Doordat we in beginsel 1 maand de tijd hebben om te reageren op een inzageverzoek, is het van groot belang om snel en efficiënt te reageren.

Procedure:

1. Het verzoek (bijlage 1) dient schriftelijk, bij voorkeur per mail, te worden gericht aan de directeur van de school. De directeur houdt daarvan de frequentie bij.

2. De AVG verplicht OZHW binnen 1 maand te reageren. Wanneer OZHW veel verzoeken ontvangt of wanneer het inzageverzoek erg ingewikkeld is, kan de termijn worden verlengd met max. 2 maanden. De verzoeker dient daar tijdig over te worden geïnformeerd.

3. Indien we de identiteit van een verzoeker niet redelijkerwijs vaststellen dan, van de AVG mag niet zomaar om een kopie legitimatiebewijs worden gevraagd (dat mag alleen bij een wettelijke verplichting). Toch zijn we wel verplicht de identiteit vast te stellen maar met zo weinig mogelijk gegevens. Een e-mailadres in combinatie met een naam of adres kan bijvoorbeeld al voldoende zijn. Door het sturen van een verificatiemail kan de identiteit van de aanvrager en de juistheid van het verzoek tot inzage worden nagegaan.

4. Indien het verzoek gegrond wordt verklaard dan kan op verschillende manieren worden gereageerd. De meest praktische manier is door alle persoonsgegevens te exporteren naar – bijvoorbeeld – een Excelbestand. Soms komen dezelfde persoonsgegevens op meerdere plekken terug, bijvoorbeeld vanwege verschillende doeleinden van verwerking. In zo'n Excelbestand zullen veel gegevens dus dubbel staan. In sommige gevallen kan een verzoeker worden uitgenodigd om de persoonsgegevens ter plekke in te zien. Dat kan bijvoorbeeld wenselijk zijn wanneer het gaat om audiologs of camerabeelden.

Welke manier dan ook, het overzicht moet in ieder geval ook het volgende bevatten:
Informatie over het doel waarvoor de persoonsgegevens worden gebruikt;

- Welke categorieën van persoonsgegevens er gebruikt worden;
- Aan welke partijen de persoonsgegevens zijn of worden verstrekt;
- Hoelang de persoonsgegevens worden bewaard en de criteria die zijn vastgesteld om de bewaartermijn te bepalen;
- Of er op basis van de persoonsgegevens automatische besluiten (profilering) worden genomen en als dit het geval is, wat de achterliggende logica is;
- Of er gegevens worden doorgegeven aan landen buiten de Europese Unie en als dit het geval is, welke (veiligheids) waarborgen zijn genomen om de persoonsgegevens te beschermen;
- Welke rechten de betrokkene – naast het inzagerecht – heeft en het feit dat de betrokkene een klacht in kan dienen bij de toezichthouder, de Autoriteit Persoonsgegevens.

BIJLAGE 1

Verzoek om inzage in persoonsgegevens voor ouders, medewerkers, leerlingen

[datum]

Geachte […],

Met verwijzing naar artikel 15 van de Algemene Verordening Gegevensbescherming (AVG) wil ik graag binnen vier weken van u weten of u mijn gegevens verwerkt. Als dat het geval is, verzoek ik u mij binnen vier weken een overzicht van de gegevens te geven. Ik verzoek u ook inlichtingen te verstrekken over het doel van de verwerking(en), de ontvangers van de gegevens en over de herkomst van de gegevens.

Hoogachtend,

BIJLAGE 2

Zie privacyreglement artikel 13, lid 1 t/m lid 7.

REGELING TAKEN EN VERANTWOORDELIJKHEDEN FUNCTIONARIS VOOR GEGEVENSBESCHERMING (vastgesteld 14-07-2020)

Artikel 1 Definities

AVG
Algemene Verordening Gegevensbescherming;
FG
functionaris voor gegevensbescherming conform artikel 37 van de AVG;
Verwerkingsverantwoordelijke
het bestuur van Stichting OZHW voor PO en VO;
Verwerker
een natuurlijke persoon of rechtspersoon, een overheidsinstantie, bedrijf, organisatie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt;
Persoonsgegeven
alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (betrokkene) waarbij als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
Verwerking van persoonsgegevens: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;
Personeel
medewerkers in loondienst en/of extern ingehuurde medewerkers die in opdracht van de Verwerkingsverantwoordelijke werkzaamheden verrichten.

Artikel 2 Taken

De FG heeft de volgende taken:

- Toezicht houden op bestaande en nieuwe (DPIA) verwerkingen van persoonsgegevens;
- Controleren van het verwerkings- en incidentenregister en logbestanden;
- Geven van (ongevraagd) advies en doen van aanbevelingen over privacy in het algemeen, vaak op basis van actuele ontwikkelingen;
- Overleg met (de contactpersoon van) de Autoriteit Persoonsgegevens;
- Jaarlijkse afstemming met de Privacy Officer en het bestuur van OZHW alsmede het opstellen van een verslag van zijn werkzaamheden;
- Het (laten) afhandelen van klachten inzake privacy;
- het begeleiden en afhandelen van datalekken incl. meldingen bij de AP na overleg met verwerkingsverantwoordelijke;
- Het personeel meldt bij de FG alle (nieuwe) verwerkingen van persoonsgegevens alsmede eventuele incidenten met betrekking tot privacy.

Artikel 3 Bevoegdheden

- De FG is bevoegd, zo nodig met medeneming van de benodigde apparatuur, elke plaats in de gebouwen op de terreinen die bij uw bestuur in gebruik zijn en waar persoonsgegevens worden verwerkt, te betreden.
- De FG is bevoegd inlichtingen te vorderen van eenieder die onder gezag of in opdracht van uw bestuur werkzaam is of overeenkomstig voor of namens uw bestuur persoonsgegevens verwerkt.
- De FG is bevoegd inzage te vorderen van zakelijke gegevens en bescheiden waarin

persoonsgegevens zijn verwerkt.

- De FG is bevoegd van de gegevens en bescheiden kopieën te maken. Indien het maken van kopieën niet ter plekke kan gebeuren, is de FG bevoegd de gegevens en bescheiden voor de duur van maximaal één werkdag mee te nemen.
- De FG is bevoegd tot het geven van een opdracht tot:

a) Het aanmaken van een registratie van persoonsgegevens in overeenstemming met de AVG;
b) Vernietiging van persoonsgegevens, waarvan de bewaartermijn is overschreden of indien de gegevensverwerking onrechtmatig is.

- De FG is bevoegd zich te laten vergezellen en bijstaan door personen die daartoe door hem zijn aangewezen.
- De FG maakt van de bevoegdheden als bedoeld in dit artikelen slechts gebruik voor zover dit redelijkerwijs voor de uitoefening van de taak noodzakelijk is.

Artikel 4 Weigering

1. Eenieder, die werkzaam is bij en/of in opdracht werkt van de verantwoordelijke, is verplicht aan de FG medewerking te verlenen, die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden.
2. Indien de medewerking aan de uitoefening van de bevoegdheden van de FG zoals bedoeld in artikel 3, wordt geweigerd, kan het bestuur, op een met redenen omkleed verzoek, toestemming verlenen aan de FG de benodigde handelingen zelfstandig uit te voeren in weerwil van de weigering tot medewerking.
3. Het bestuur wordt zo spoedig mogelijk in kennis gesteld over de uitvoering van het bepaalde in dit artikel.

Artikel 5 Geheimhouding

De FG is verplicht tot geheimhouding van al hetgeen hem op grond van deze regeling bekend is geworden, tenzij de betrokkene in bekendmaking toestemt.

Artikel 6 Regeling

Deze regeling wordt vastgesteld en gewijzigd bij besluit van de Verwerkingsverantwoordelijke. Deze regeling treedt in werking na ondertekening en zal intern aan het personeel bekend worden gemaakt.

GEDRAGSCODE VOOR VERANTWOORD GEBRUIK VAN BEDRIJFSMIDDELEN VOOR MEDEWERKERS VAN OZHW VOOR PO EN VO (vastgesteld 14-07-2020)

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

Hoofdstuk 1 'Inleiding' beschrijft wat onder bedrijfsmiddelen verstaan wordt, de uitgangspunten van de gedragscode en de driedeling van gegevens (openbaar, intern en vertrouwelijk) die verwerkt worden.
Hoofdstuk 2 'Gedragscode' bevat de 'bouwstenen' waarmee de afspraken kunnen worden vastgelegd die relevant zijn voor de gewenste gedragscode van een school. Elke school kan met de bijbehorende paragrafen een gedragscode ***'op maat'*** maken.
Per onderwerp en/of per onderdeel (bullet) binnen een onderwerp kunnen keuzes en aanpassingen gemaakt worden.
Hoofdstuk 3: 'Controle gebruik bedrijfsmiddelen' beschrijft de voorwaarde van controle, de uitvoering ervan, de eventuele sancties en de mogelijkheid van bezwaar maken.
Hoofdstuk 4: 'GMR' laat de rol van de (G)MR zien.
Hoofdstuk 5: 'Slotbepaling' toont de datum van de eerstvolgende evaluatie en eventuele aanpassing van de gedragscode.

1. Inleiding

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

- Hardware: *pc, laptop, tablet, telefoon, hardware token (tag).*
- Software (of -systemen): *alle applicaties voor het uitvoeren van de werkzaamheden, zoals de school e-mailomgeving, Microsoft Office, administratiesystemen 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 als FTP en maar ook 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 OZHW voor PO en VO wordt verwacht dat zij verantwoord omgaan met de beschikbaar gestelde bedrijfsmiddelen. Dit wordt ook verwacht als medewerkers hun eigen middelen inzetten om werkzaamheden voor de school uit te voeren.

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

1.1. Uitgangspunten gedragscode

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

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

De controle op het gebruik van bedrijfsmiddelen is een verwerking van persoonsgegevens in de zin van de privacywetgeving. OZHW voor PO en VO 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.

2. Gedragscode

In deze gedragscode voor verantwoord gebruik van bedrijfsmiddelen geeft OZHW voor PO en VO 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.
- 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 door het sturen van een e-mail aan servicedesk@ozhw.nl of een telefonische melding bij de daarvoor aangewezen persoon (Zie hiervoor de procedure meldplicht datalekken van OZHW voor PO en VO).

2.2. Computergebruik

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

- Zorg dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden.
- Weet welke gegevens er mogen worden gebruikt (mag iedereen het zien?) en welke ict-voorzieningen kunnen worden ingezet (is het veilig genoeg?) bij het verrichten van de verschillende schoolwerkzaamheden.
- Sla (persoons)gegevens alleen op de daarvoor aangewezen systemen op. (Opslaan van gegevens in public Cloud omgevingen, zoals een persoonlijke dropbox, is niet toegestaan).
- Versleutel alle gegevens met betrekking tot OZHW voor PO en VO, indien deze gegevens, om welke reden dan ook, elders opgeslagen worden (denk hierbij ook aan een usb-stick).
- Om te voorkomen dat mogelijk privacygevoelige informatie in verkeerde handen valt is het gebruik van USB-sticks en/of externe harddisks zonder encryptie niet toegestaan.
- 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-afdeling via servicedesk@ozhw.nl

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 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. Sluit het e-mail programma af en zorg voor een opgeruimd digitaal bureaublad.
- Laat geen afdrukken bij de printer liggen, zeker niet als er persoonsgegevens op staan.
- Haal overbodig geworden papieren documenten met persoonsgegevens erop altijd door de papierversnipperaar.

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 OZHW voor PO en VO.

2.4. Gebruik eigen Devices (BYOD)

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor OZHW voor PO en VO worden uitgevoerd. OZHW voor PO en VO is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen van de school.

Voor 'Own Devices' ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:
- Beveilig het device met een sterk wachtwoord of in het geval van een smartphone of tablet, met een pincode die langer is dan 4 tekens.
- Vergrendel het device bij het verlaten van de werkplek (windowstoets+L).
- Sla persoonsgegevens van OZHW voor PO en VO niet op het eigen device op; dit is niet toegestaan.
- Versleutel alle gegevens, anders dan persoonsgegevens, met betrekking tot OZHW voor PO en VO als deze, om welke reden dan ook, niet op het schoolnetwerk opgeslagen worden (denk hierbij aan het eigen device of usb-stick).
- Scheid (versleutelde)gegevens, anders dan persoonsgegevens, van OZHW voor PO en VO 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.

OZHW voor PO en VO mag controles uitvoeren op bovenstaande maatregelen. Op verzoek van OZHW voor PO en VO 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 OZHW voor PO en VO. 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 OZHW voor PO en VO 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 OZHW voor PO en VO persoonsgegevens verwerkt. Regel dit vooraf aan het gebruik.
- Aanvragen van digitaal lesmateriaal en/of andere software volgt bij OZHW voor PO en VO de 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

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

- Gebruik het school e-mail adres *alléén* voor school gerelateerde zaken.
- 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 school e-mailadres is incidenteel toegestaan.
- 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 devices (tablet, telefoon) dan kan OZHW voor PO en VO, bij verlies of diefstal van het device, gebruik maken van de mogelijkheid om de e-mail op afstand te wissen, ook als daarmee alle (privé)gegevens van het device gewist worden.
- Aanvullende afspraken rondom internet, email en netwerk in het algemeen heeft OZHW voor PO en VO vastgelegd in een apart internet, email en netwerkprotocol (zie bijlage).

2.7. Gebruik van Internet

OZHW voor PO en VO 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 afspraken zoals geformuleerd in het protocol internet ,email en netwerk. Aanvullende afspraken rondom sociale media in het algemeen heeft OZHW voor PO en VO vastgelegd in een apart sociale media protocol (zie bijlage).

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.
OZHW voor PO en VO 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 OZHW voor PO en VO
- 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 OZHW voor PO en VO netwerk is, eduroam 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 de school. Medewerkers zijn altijd de vertegenwoordiger van OZHW voor PO en VO ook als zij online een privémening verkondigen.

Bij OZHW voor PO en VO gelden de afspraken voor het gebruik van sociale media, zoals vastgelegd in het OZHW protocol voor sociale media (zie bijlage).

2.10. Gebruik van beeld- en geluidsmateriaal

Het gebruiken van beeld- en geluidsmateriaal, het delen van foto's, video's en geluidsfragmenten van leerlingen door medewerkers vallend onder OZHW voor PO en VO mag alleen als daar vooraf toestemming voor gegeven is door ouders als de leerling jonger is dan 16 jaar of de leerling zelf als deze ouder dan 16 jaar is. Zonder deze toestemming mogen geen foto's, video's en geluidsfragmenten van leerlingen gebruikt worden.

- OZHW voor PO en VO 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.

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.
- Wachtwoorden moeten volgens de afspraken binnen OZHW voor PO en VO op aangegeven tijden 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 via security@ozhw.nl volgens de procedure meldplicht datalekken van OZHW voor PO en VO.

3. Controle gebruik bedrijfsmiddelen

OZHW voor PO en VO handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving, te weten:

- De Grondwet,
- Algemene Verordening Gegevensbescherming (AVG)
- Wet Medezeggenschap op Scholen (WMS)
- Burgerlijk Wetboek (BW)
- Wetboek van Strafrecht
- Cao PO en
- Cao VO.

OZHW voor PO en VO 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 OZHW voor PO en VO gerichte controle plaatsvinden.
- Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van OZHW voor PO en VO, 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. OZHW voor PO en VO 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 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 OZHW voor PO en VO worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
- Door OZHW voor PO en VO 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 OZHW voor PO en VO, 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 de (voorgenomen) disciplinaire maatregel, dan kan daar in een aantal gevallen bezwaar en/of beroep tegen worden ingesteld conform de geldende CAO.

4. Medezeggenschap

Dit document heeft betrekking op verwerking van persoonsgegevens en/of controle van het gedrag of de prestaties van medewerkers. De GMR PO en de MR VO zijn om deze reden instemming plichtig. De MR VO en GMR PO hebben ingestemd met de inhoud van deze gedragscode. De organisatie kan deze gedragscode met instemming van de MR VO en GMR PO 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 aan het einde van het schooljaar geëvalueerd door OZHW voor PO en VO.

BEWAARTERMIJNEN LEERLINGGEGEVENS EN PERSONEELSGEGEVENS (WETTELIJK BEPAALD)

Bewaartermijnen persoonsgegevens - Leerlingadministratie en het Leerlingdossier

Het leerlingdossier bestaat uit twee componenten: de leerlingadministratie en het leerlingdossier. Een basisschool of middelbare school mag verschillende gegevens over een leerling bewaren. De l**eerlingadministratie** bevat persoonsgegevens die vallen onder de Algemene Verordening Gegevensbescherming (AVG 28 mei 2018), waarvan de gegevensverwerking gebaseerd is op een wettelijke grondslag. De gegevens worden bewaard in een leerlingdossier en bestaan voor een deel uit administratieve gegevens. Verder zit er in het leerlingdossier informatie die nodig is om de leerling onderwijs en begeleiding te geven. Het leerlingdossier is privacygevoelig omdat de ontwikkeling, het gedrag en de leerprestaties van een leerling systematisch in beeld te brengen is en te volgen is middels het leerlingdossier. Stapt een leerling van de basisschool over naar de middelbare school of naar een andere basisschool, dan is de (oude) (basis)school verplicht een onderwijskundig rapport op te stellen over de leerling. In het onderwijskundig rapport staat de belangrijkste informatie uit het leerlingdossier. De school stuurt dit rapport vervolgens door naar de nieuwe school.

Voor de verwerking van persoonsgegevens in het leerlingdossier gelden de volgende regels:

- Het bevat slechts gegevens voor zover die noodzakelijk zijn voor het doel.
- De gegevens moeten juist zijn.
- De beveiliging van- en de toegang tot de leerlingdossiers is goed.
- Bij het gebruik van leerlingdossiers worden de regels van de AVG nageleefd (verantwoordingsplicht).
- De gegevensverwerking in leerlingdossiers is opgevoerd in ons register van verwerkingsactiviteiten.
- Er wordt met regelmaat een data protection impact assessment (DPIA) uitgevoerd op het gebruik van het leerlingdossier.
- Ouders en/of leerlingen ouder dan 16 jaar hebben het recht op dataportabiliteit. Dat is het recht om gegevens mee te nemen, bijvoorbeeld naar een andere school.

Het leerlingdossier bevat rapporten, uitslagen van toetsresultaten, gegevens uit het leerlingvolgsysteem, verslagen van gesprekken met ouders en afspraken die er over de leerling zijn gemaakt. De verwerking dient alleen voor de organisatie of het geven van onderwijs aan de leerling en de begeleiding van die leerling

Inhoud van het leerlingdossier

De Autoriteit Persoonsgegevens geeft aan dat het leerlingdossier de volgende gegevens mag bevatten:

· Gegevens over in- en uitschrijving
· Gegevens over afwezigheid
· Adresgegevens
· Gegevens die nodig zijn om te berekenen hoeveel geld de school krijgt
· Het onderwijskundig rapport
· Gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen
· Gegevens over de vorderingen en de resultaten van de leerling
· Verslagen van gesprekken met de ouders
· De resultaten van eventueel psychologisch onderzoek

Welke wettelijke bepalingen zijn van toepassing?

In het algemeen geldt dat het leerlingdossier 2 jaar moet worden bewaard nadat de leerling van school is gegaan. Op papier moeten worden bewaard inschrijfformulieren/aanmeldingsformulieren, gewichtenformulier P.O. en, van het SWV, formulieren en beschikkingen LWOO/PRO etc. Het op papier bewaren met een handtekening van ouders is nodig om als bewijs te kunnen dienen naar instanties als bijv. politie, accountant, inspectie. In sommige situaties staat er een langere bewaartermijn in andere wet- en regelgeving waar we ons aan moeten houden:

- In het primair en voortgezet onderwijs geldt dat gegevens over verzuim en afwezigheid en in- en uitschrijving 5 jaar bewaard moeten worden nadat de leerling is uitgeschreven.
- Gegevens over een leerling die naar een school voor speciaal onderwijs is doorverwezen, moeten t/m 3 jaar na het vertrek van de leerling bewaard worden. In het Examenbesluit staat onder meer dat het centraal examen, inclusief de cijferlijsten, minstens 6 maanden bewaard moeten worden. (School)examenwerk wordt binnen OZHW bewaard tot 1 januari van het kalenderjaar volgend op het jaar van het centraal examen).
- Adresgegevens van oud-leerlingen mogen worden bewaard voor het organiseren van reünies. Let er wel op dat daarvoor eerst toestemming aan de oud-leerlingen wordt gevraagd. De gegevens mogen ook alleen voor dát doel worden gebruikt.

Kinderen van 16 jaar of ouder hebben zelf recht op inzage in hun leerlingdossier. Ouders met wettelijk gezag over hun kind jonger dan 16 jaar of de wettelijk vertegenwoordiger van een kind jonger dan 16 jaar hebben recht op inzage in het dossier van het kind. Ouders zonder gezag over hun kind jonger dan 16 jaar hebben geen recht op inzage in het dossier van hun kind. Wel hebben zij recht op belangrijke informatie over hun kind, zoals de schoolprestaties. Maar dit geldt alleen als het belang van het kind hiermee niet wordt geschaad. Als school maak je vóór het verstrekken van informatie een afweging tussen het belang van ouders en het belang van het kind. Als school moeten er wél zware argumenten zijn om ouders niet te informeren. Alleen als blijkt dat het geven van informatie nadelig is voor een kind, mag de school de informatie weigeren.

Er dient binnen een termijn van vier weken te worden voldaan aan het verzoek tot inzage door ouders. Ook bestaat er **kopierecht**, dat wil zeggen dat ten behoeve van de ouders kopieën van de gegevens gemaakt mogen worden. De school mag hier een vergoeding voor vragen. Er bestaat daarnaast nog het **recht tot corrigeren** van de gegevens en **verwijdering** van de gegevens. Dit houdt in dat ouders het recht hebben op verbeteren, aanvullen, verwijderen, afschermen of op een andere manier ervoor te laten zorgen dat onjuiste gegevens niet langer gebruikt worden. Er is alleen een verplichting om dit als school ook daadwerkelijk te doen als er sprake is van feitelijk onjuiste, onvolledige of niet ter zake doende gegevens of gegevens die in strijd zijn met de AVG. Ouders mogen het originele leerlingdossier **niet** meenemen buiten de school.
Ten aanzien van collega-scholen worden dezelfde richtlijnen gehanteerd. Zonder toestemming van ouder(s) mag het dossier niet worden ingezien en verstrekt.

Examen, toetsen en gemaakt schoolwerk.

Het is naar aanleiding van het signaal van de Erfgoedinspectie gebleken dat er sprake is van een discrepantie tussen de Archiefwet en het eindexamenbesluit VO, waar gesproken wordt van een bewaartermijn van 6 maanden (artikel 57 EB). Een school moet het werk van het centraal examen en de rekentoets bewaren tot minimaal 6 maanden na de uitslag. Dit geldt ook voor de bijbehorende cijferlijst. Leerlingen kunnen in die periode hun examen inzien. Bij het werk horen ook de opgaven die de leerling gebruikt heeft bij de centrale examens. Voor schoolexamens geldt geen minimale bewaartermijn. Deze gegevens mogen maximaal 2 jaar bewaard blijven op school. (School)examenwerk wordt binnen OZHW bewaard tot 1 januari van het kalenderjaar volgend op het jaar van het centraal examen).

Er is geen wettelijke minimum termijn voor het bewaren van toetsen, scholen stellen hierover hun eigen beleid op. Meer informatie is terug te vinden op het DigiPlein onder:

https://eduozhw.sharepoint.com/sites/ozhw-onderwijs-kwaliteit/SitePages/Toetsing-%26-afsluiting.aspx?web=1

Bewaartermijn archiefbescheiden toekennen diploma's
In het kader van de Archiefwet moeten overheidsinstellingen belangrijke documenten bewaren. Welke documenten dat zijn en hoe lang ze bewaard moeten worden is vastgelegd in zogeheten selectielijsten. Er zijn onderwijsinstellingen die onderdeel zijn van de overheid (gemeentelijke scholen) en scholen die deel uitmaken van een stichting of vereniging. Voor de eerste categorie is er een selectielijst vastgesteld door de VNG. De meeste scholen vallen onder die tweede categorie. Voor hen gaat het niet om het gehele archief, maar alleen om gegevens omtrent openbaar gezag taken: examinering en vrijstelling van de leerplicht. Dit houdt in dat informatie die onder de Archiefwet valt, niet vernietigd mag worden, zolang er geen selectielijst is vastgesteld. Advies van de VO-raad is om voorlopig geen persoonsgegevens te vernietigen rondom examens (diploma's en cijferlijsten) en gegevens rondom vrijstelling van de leerplicht. Anonimiseer persoonsgegevens die de bewaartermijn hebben overschreden zo veel mogelijk en bewaar ze op een aparte, extra beveiligde plek, waar alleen een zeer selecte groep medewerkers toegang toe heeft. **Omdat de Archiefwet boven het Eindexamenbesluit staat, dienen wij alle examengegevens tot nader order te bewaren.**

BEWAARTERMIJN LEERLINGGEGEVENS	
Inschrijf/aanmeldingsformulier en uitschrijfbewijs (van basisschool of voorgaande V.O. school)	5 jaar (i.v.m. bekostiging/accountantscontrole)
Kopie inzage ID	1 maand
Beheersmaatregel gezondheid	5 jaar (i.v.m. bekostiging/accountantscontrole
Overdrachtsformulier	2 jaar na beëindiging opleiding
Centraal examen en de rekentoets	(school)examenwerk wordt bewaard tot 1 januari van het kalenderjaar volgend op het jaar van het centraal examen.
Schoolexamen	(school)examenwerk wordt bewaard tot 1 januari van het kalenderjaar volgend op het jaar van het centraal examen.
Specifieke documenten	Tot 5 jaar na beëindiging opleiding

BEWAARTERMIJNEN PERSONEELSGEGEVENS

Werkgevers verwerken veel persoonsgegevens van hun werknemers. Deze zijn vaak opgeslagen in een personeelsdossier. Werkgevers mogen alleen een personeelsdossier aanleggen als dat noodzakelijk is om een arbeidsovereenkomst of een aanstelling als ambtenaar uit te voeren. En zij moeten daarbij rekening houden met de privacy van hun werknemers. Zie hiervoor ook de site van de AP:

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-en-uitkering/personeelsdossiers

Voorwaarden personeelsdossier

De Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) geven de voorwaarden voor het aanleggen van personeelsdossiers. Werkgevers:

- zijn verantwoordelijk voor de juistheid en nauwkeurigheid van de gegevens in het personeelsdossier;
- mogen niet meer gegevens in het personeelsdossier vastleggen dan nodig is, en de gegevens moeten ter zake doen;
- moeten de werknemers informeren, onder andere over welke gegevens zij verzamelen, voor welke doeleinden en op basis van welke rechtsgrond;
- moeten de persoonsgegevens passend beveiligen, zodat ze niet verloren raken of in verkeerde handen terechtkomen;
- mogen de persoonsgegevens niet langer bewaren dan noodzakelijk is;
- moeten werknemers de mogelijkheid bieden hun gegevens in te zien - dit geldt in principe voor het gehele personeelsdossier - en eventueel te rectificeren te beperken of te verwijderen;
- moeten werknemers afzonderlijk wijzen op het recht van bezwaar bij de verwerking van gegevens op grond van het gerechtvaardigd belang;
- moeten werknemers in voorkomende gevallen de mogelijkheid bieden hun recht op dataportabiliteit uit te oefenen.

BRON:

- site AP
- VOS/ABB
- https://www.avghelpdeskzorg.nl/onderwerpen/bewaartermijnen/bewaartermijnen-persooneelsdossier
- https://www.tuxx.nl/bewaartermijnen/documenten/

Onderwijsgroep Zuid-Hollandse Waarden
voor primair en voortgezet onderwijs

WAT	BEWAARTERMIJNEN PERSONEELSGEGEVENS	GRONDSLAG
Correspondentie benoemingen, promotie, demotie en ontslag	Maximaal 2 jaar nadat de werknemer uit dienst is.	Vastgelegd in art. 52 Wet Rijksbelastingen. let op: deze moeten ook minimaal 2 jaar worden bewaard.
Loonbelastingverklaringen en kopieën identiteitsbewijzen	Maximaal 5 jaar nadat de werknemer uit dienst is.	Vastgelegd in art. 66 lid 4 Uitvoeringsregeling LB.
Gegevens betreffende etniciteit en herkomst	Minimaal 5 jaar nadat de werknemer uit dienst is.	Vastgelegd in: Wet Samen (Wet Stimulering Arbeidsdeelnamen Minderheden).
Identiteitspapieren van derden met tewerkstellingsvergunning	Minimaal 5 jaar, geen maximum	Ingangsdatum: na afloop van het kalenderjaar waarin arbeid door ingeleende vreemdeling is beëindigd. Vastgelegd in: Wet Arbeid Vreemdelingen.
Afspraken salaris en arbeidsvoorwaarden	Maximaal 7 jaar nadat de werknemer uit dienst is.	Vastgelegd in Wet Rijksbelastingen.
Persoonsgegevens werknemer- NAW en Burgerlijke staat	Maximaal 7 jaar nadat de werknemer uit dienst is.	Vastgelegd in Wet Rijksbelastingen.
Loonbeslagen	Maximaal tot eind opheffing.	Vastgelegd in: Vrijstellingsbesluit Wet Bescherming Persoonsgegevens, loopt door in de AVG
Sollicitatiebrieven (en correspondentie), getuigschrift e.d.	Maximaal 4 weken na eind sollicitatieprocedure (met toestemming sollicitant 1 jaar)	Ingangsdatum bewaartermijn: na beëindiging sollicitatieprocedure Vastgelegd in: AVG.
Arbeidsovereenkomst en wijzigingen	Maximaal 2 jaar nadat de werknemer uit dienst is.	Vastgelegd in art. 52 Wet Rijksbelastingen.
Verslagen van functioneringsgesprekken	Maximaal 2 jaar nadat de werknemer uit dienst is.	Vastgelegd in de AVG; let op: deze moeten ook minimaal 2 jaar worden bewaard.
Verslaglegging Wet Verbetering Poortwachter	Maximaal 2 jaar nadat de werknemer uit dienst is.	vastgelegd in: AVG.
Beveiligingscamera's	4 weken of tot incident is afgehandeld na start opname	Vastgelegd in: AVG.
Opsporingscamera's tbv fraude, diefstal e.d.	Zo lang als nodig is voor doel	
BEWAARPLICHT MEDISCHE / ARBO DOCUMENTEN		
Algemeen	Minimaal 10 jaar	Werknemer kan om vernietiging vragen. Uit: art. 7: 456 Wet op de Geneeskundige Behandelingsovereenkomst

PRIVACYVERKLARING OZHW TBV OUDERS EN/OF VERZORGERS

Privacyverklaring OZHW voor PO en VO

Ten behoeve van ouders/verzorgers

Contactgegevens

Contactgegevens OZHW, namens de scholen voor PO en VO	:	Postbus 206, 2990AE Barendrecht E-mail: avg@ozhw.nl
Verwerkingsverantwoordelijke bestuurder	:	Mevr. J. Everts-van Driel
Contactgegevens Functionaris Gegevensbescherming	:	Mevr. L. van de Weijer functionarisgegevensbescherming@ozhw.nl

Hoe gaan wij om met persoonsgegevens

OZHW verwerkt namens de scholen voor PO en VO van al zijn leerlingen persoonsgegevens. OZHW vindt een goede omgang met persoonsgegevens van groot belang en is zich bewust van de privacywetgeving. OZHW is namens de scholen verantwoordelijk voor het zorgvuldig omgaan met de persoonsgegevens van uw kind. In deze privacyverklaring leggen wij u graag uit hoe wij met de persoonsgegevens van uw kind omgaan.

Waarom verwerken wij gegevens van uw kind

Onze scholen verwerken persoonsgegevens van uw kind voor het uitvoeren van de *onderwijsovereenkomst* die we met uw kind hebben en om onze *wettelijke verplichtingen* als onderwijsinstelling te kunnen nakomen. Zo hebben wij bijvoorbeeld de gegevens nodig om uw kind aan te melden als leerling op onze school, om de studievoortgang bij te houden en om uw kind in staat te stellen een diploma te halen. Daarnaast hebben wij de wettelijke verplichting om bepaalde gegevens door te sturen naar andere partijen. Gegevens die hier niet aan voldoen zullen wij alleen met uw toestemming verwerken. Als voor het verwerken van gegevens toestemming wordt gevraagd, zoals voor het gebruik van beeldmateriaal (foto's en video's), dan kunt u de toestemming op elk moment intrekken of alsnog geven. Intrekking van toestemming is echter niet van toepassing op inmiddels gepubliceerd beeldmateriaal. Wel kunt u ons in dat geval verzoeken om eerder met uw toestemming gepubliceerd beeldmateriaal, waarop uw zoon of dochter herkenbaar voorkomt, te verwijderen. Indien dit binnen redelijke grenzen nog mogelijk is, zullen wij aan uw verzoek gehoor geven.

Welke gegevens verwerken wij van uw kind

Wij verwerken diverse soorten gegevens, waarvan wij de meeste gegevens rechtstreeks van u als ouders hebben gekregen. U kunt hierbij denken aan contactgegevens en geboorteplaats. Als u weigert de voor ons noodzakelijke gegevens te verstrekken, kunnen wij onze verplichtingen niet nakomen. De verstrekking van deze gegevens is dan ook een voorwaarde om uw kind in te kunnen schrijven bij één van de scholen behorend bij OZHW. Welke persoonsgegevens wij van uw kind verwerken kun u terugvinden aan het einde van deze privacyverklaring, in het Overzicht categorieën van persoonsgegevens.
Op uw eigen verzoek en met uw uitdrukkelijke toestemming verwerken wij ook medische gegevens van uw kind. Dit beperkt zich enkel tot gegevens die nodig zijn om in noodgevallen goed te kunnen handelen. U kunt bijvoorbeeld doorgeven dat uw kind epilepsie heeft, zodat wij adequaat kunnen optreden in noodsituaties. Wij zullen u nooit dwingen dergelijke gegevens te overleggen.

Hoe gaan wij om met de gegevens van uw kind
Bij het verwerken van de gegevens gaan wij altijd uit van noodzakelijkheid. Wij zullen daarom niet meer gegevens verwerken dan noodzakelijk is om onze rechten en plichten als onderwijsinstelling na te komen. Dit betekent ook dat wij de gegevens niet zullen gebruiken voor andere doeleinden dan wij in deze toelichting noemen. In een aantal gevallen zijn wij, zoals eerder aangegeven, verplicht om gegevens van uw kind te delen met andere organisaties. Dit zijn onder andere DUO, leerplicht, de onderwijsinspectie, GGD/schoolarts, samenwerkingsverband en accountant. Wij kunnen commerciële organisaties verzoeken om te ondersteunen bij het verwerken van de gegevens voor de eerder genoemde doeleinden. Denk hierbij aan applicaties om leerlingen in de les te ondersteunen, een administratie systeem waarbij de gegevens niet op ons eigen netwerk worden opgeslagen, maar bij een andere organisatie of een lesroosterprogramma. Dit gebeurt altijd in opdracht en onder onze verantwoordelijkheid. Met deze organisaties sluiten we overeenkomsten af, waarin o.a. is vastgelegd welke gegevens er verwerkt worden en hoe deze gegevens beveiligd worden. Wij zullen de gegevens van uw kind met deze organisaties niet delen voor andere doeleinden. Ook zullen wij de gegevens van uw kind nooit verkopen of verhuren aan overige derde partijen. De persoonsgegevens worden zoveel mogelijk gecodeerd bewaard en alleen die medewerkers kunnen bij de gegevens, die dat ook voor de uitvoering van hun werk nodig hebben, daarvoor zijn geautoriseerd. Daarnaast bewaren wij de gegevens niet langer dan noodzakelijk is. Wij hanteren hiervoor verschillende bewaartermijnen die wettelijk geregeld en vastgesteld zijn.

Welke rechten hebben een leerling en ouders van leerlingen jonger dan 16 jaar
Als ouders heeft u een aantal rechten als het gaat om persoonsgegevens. Deze rechten zijn in de wet vastgelegd. Leerlingen en/of ouders kunnen op elk moment gebruik maken van deze rechten. Dit betekent bijvoorbeeld dat u altijd een verzoek kunt indienen om inzage te krijgen in de gegevens die wij van uw kind verwerken.
Daarnaast kunt u ook een verzoek indienen om gegevens te rectificeren, te beperken of helemaal te wissen uit de systemen van de school. U heeft altijd het recht om onjuiste gegevens aan te vullen of te verbeteren. Wij zullen er vervolgens voor zorgen dat deze gegevens ook bij organisaties waarmee wij deze gegevens van uw kind delen en/of uitwisselen worden aangepast.
Als u ons verzoekt om gegevens van uw kind te beperken of te wissen, zullen wij toetsen of dit mogelijk is. In deze toets houden wij ons aan de wettelijke voorschriften en kijken wij bijvoorbeeld of wij geen wettelijke plicht hebben om de gegevens te bewaren.
Tevens heeft u het recht om te vragen om de gegevens, die wij van uw kind verwerken en wij van u hebben ontvangen, aan u over te dragen of op uw verzoek aan een andere organisatie over te dragen.

Onze scholen zullen geen besluiten nemen over uw kind, die alleen gebaseerd zijn op geautomatiseerde verwerking van gegevens (zogeheten "*profiling*"). Beslissingen worden nooit zonder menselijke tussenkomst genomen.

Als u het niet eens bent met hoe wij omgaan met de gegevens van uw kind, dan kunt u altijd opheldering vragen bij onze Functionaris voor Gegevensbescherming (zie de contactgegevens bovenaan deze toelichting). Indien uw probleem volgens u niet goed door ons wordt opgelost, dan kunt u dat melden bij de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Onderwijsgroep
Zuid-Hollandse Waarden
voor primair en voortgezet onderwijs

Overzicht categorieën van persoonsgegevens:

Categorie	Toelichting
1. Contactgegevens	**1a:** naam, voornaam, e-mail, opleiding; **1b:** geboortedatum, geslacht; **1c:** overige gegevens te weten: adres, postcode, woonplaats, telefoonnummer en eventueel ande voor communicatie benodigde gegevens, alsmede ook een bankrekeningnummer voor het afhandelen van betalingen**;**
2. Leerling nummer	Een administratienummer dat geen andere informatie bevat dan bedoeld onder categorie 1
3. Nationaliteit en geboorteplaats	
4. Ouders, voogd	Contact gegevens van de ouders/verzorgers van leerlingen (naam, voornaam, adres, postcode, woonplaats, telefoonnummer en eventueel e-mailadres)
5. Medische gegevens	Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling, voor zover deze van belang zijn bij het nemen van aanvullende maatregelen om goed onderwijs te kunnen volgen (bv. extra tijd bij toetsen);
6. Godsdienst	Gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor het te volgen onderwijs (bijvoorbeeld: leerling vrij op bepaalde dag).
7. Studievoortgang	Gegevens betreffende de aard en het verloop van het onderwijs en de behaalde studieresultaten te weten: - Examinering (gegevens rondom het examen) - Studietraject - Begeleiding leerling (inclusief ontwikkelperspectief OPP) - Aanwezigheidsregistratie -Medisch dossier (papier) - Klas, leerjaar, opleiding
8. Onderwijsorganisatie	Gegevens met het oog op het organiseren van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen; hieronder vallen ook lesroosters, boekenlijsten, schoolpasjes enz.
9. Financiën	Gegevens voor het berekenen, vastleggen en innen van inschrijvingsgelden, school- en/of lesgelden, bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten. (denk hierbij aan een bankrekeningnummer van de ouders)
10. Beeldmateriaal	Foto's en videobeelden (met of zonder geluid) van activiteiten van de school op basis van toestemming. **Let op:** Voor pasfoto voor identificatiedoeleinden is geen toestemming nodig (schoolpas en als aanvulling op het dossier).
11. Docent /zorgcoördi-nator/ intern begeleider/ decaan / mentor	Gegevens van **docenten en begeleiders,** voor zover deze Gegevens van belang zijn voor de organisatie van de instelling en Het geven van onderwijs, opleidingen en trainingen
12. BSN (PGN)	In het onderwijs heet het BSN het persoonsgebonden nummer (PGN). Ook wel onderwijsnummer genoemd. Het PGN is hetzelfde nummer als het BSN. Scholen zijn verplicht het PGN te gebruiken in hun administratie.
13. Keten-ID (Eck-Id)	Unieke iD voor de 'educatieve contentketen'. Hiermee kunnen scholen gegevens delen, zonder dat ze direct herleidbaar zijn naar leerlingen of docenten.
14 Overige gegevens	Andere dan de onder 1 tot en met 11 bedoelde gegevens waarvan de verwerking wordt vereist of noodzakelijk is met het oog op de toepassing van een andere wet. Deze zullen apart vermeld en toegelicht worden.

PRIVACYVERKLARING OZHW TBV LEERLINGEN

Privacyverklaring OZHW voor PO en VO

Ten behoeve van leerlingen

Contactgegevens

Contactgegevens OZHW, namens de scholen voor PO en VO	:	Postbus 206, 2990AE Barendrecht 088-3290710
Verwerkingsverantwoordelijke bestuurder	:	Mevr. J. Everts - van Driel
Contactgegevens Functionaris Gegevensbescherming	:	Mevr. L. van de Weijer functionarisgegevensbescherming@ozhw.nl

Hoe gaan wij om met jouw persoonsgegevens

OZHW verwerkt namens de scholen voor PO en VO van al zijn leerlingen persoonsgegevens. OZHW vindt het belangrijk om netjes om te gaan met jouw persoonsgegevens en is daar ook verantwoordelijk voor. In deze verklaring leggen wij jou graag uit hoe wij met jouw persoonsgegevens omgaan.

Waarom verwerken wij jouw gegevens

Onze scholen verwerken jouw persoonsgegevens om jouw onderwijs te kunnen geven en om ons aan de wet te houden. Zo hebben wij bijvoorbeeld jouw gegevens nodig om je aan te melden als leerling op onze school, om jouw studievoortgang bij te houden en om je in staat te stellen een diploma te halen. Daarnaast zijn wij wettelijk verplicht om bepaalde gegevens door te sturen naar andere partijen. Gegevens die hier niet aan voldoen zullen wij alleen met jouw toestemming verwerken of – als je jonger bent dan 16 – met toestemming van je ouders / verzorgers. Als voor het verwerken van gegevens toestemming aan jou of je ouders wordt gevraagd, zoals voor het gebruik van foto's en video's, dan kunnen jullie de toestemming op elk moment intrekken of alsnog geven. Intrekking kan alleen niet bij foto's en video's die al gepubliceerd zijn. Wel kun je ons vragen om eerder met jullie toestemming gepubliceerde foto's of video's, waarop je herkenbaar voorkomt, te verwijderen. Indien dit binnen redelijke grenzen nog mogelijk is, dan zullen we de foto's of video's verwijderen.

Welke gegevens verwerken wij van jou

Wij verwerken diverse soorten gegevens, waarvan wij de meeste gegevens rechtstreeks van jou of je ouders hebben gekregen. Denk hierbij bijvoorbeeld aan contactgegevens en geboorteplaats. Als je weigert de gegevens te verstrekken die wij nodig hebben, kunnen wij jou geen onderwijs geven en ons niet aan de wet houden. Het ontvangen van deze gegevens is dan ook een voorwaarde om je in te kunnen schrijven op onze school. Welke persoonsgegevens wij van jou verwerken kun je terugvinden aan het einde van deze privacyverklaring, in het overzicht categorieën van persoonsgegevens.
Op verzoek en met uitdrukkelijke toestemming van jou of je ouders verwerken wij ook medische gegevens van jou. Dit is dan alleen om in noodgevallen goed te kunnen handelen, bijvoorbeeld als je epilepsie hebt. Wij zullen je nooit dwingen dit soort gegevens met ons te delen.

Hoe gaan wij om met jouw gegevens
Wij zullen niet meer gegevens verwerken dan noodzakelijk is om onze rechten en plichten als school na te komen. Dit betekent ook dat wij de gegevens niet zullen gebruiken voor andere doelen dan wij in deze verklaring noemen. In een aantal gevallen zijn wij verplicht om gegevens van jou te delen met andere organisaties, zoals DUO, leerplicht, de onderwijsinspectie, GGD/schoolarts, samenwerkingsverband en accountant. Wij kunnen bedrijven vragen om ons te helpen bij het verwerken van de gegevens voor de eerder genoemde doelen. Denk hierbij aan softwareprogramma's om jou in de les te ondersteunen, of aan een administratie systeem waarbij de gegevens niet op ons eigen netwerk worden opgeslagen, maar bij een andere organisatie of een lesroosterprogramma. Dit gebeurt altijd in onze opdracht en onder onze verantwoordelijkheid. Met deze bedrijven maken we goede afspraken, onder andere over welke gegevens er verwerkt worden en hoe deze gegevens beveiligd worden. Wij zullen jouw gegevens met deze bedrijven niet delen voor andere doelen. Ook zullen wij jouw gegevens nooit verkopen of verhuren. Jouw persoonsgegevens worden zoveel mogelijk gecodeerd bewaard en alleen die medewerkers kunnen bij de gegevens, die dat ook voor hun werk op school nodig hebben, zoals jouw docenten. Daarnaast bewaren wij de gegevens niet langer dan nodig. Hoe lang dat is staat meestal in een wet. Als je dat wilt kunnen wij jou een overzicht geven.

Welke rechten hebben een leerling en ouders van leerlingen jonger dan 16 jaar
Als leerling heb je vanaf 16 jaar zelf een aantal rechten als het gaat om persoonsgegevens en/of hebben je ouders die rechten als je nog geen 16 jaar bent. Deze rechten zijn in de wet vastgelegd. Leerlingen en/of ouders kunnen op elk moment gebruik maken van deze rechten. Dit betekent bijvoorbeeld dat je altijd een verzoek kunt (laten) indienen om inzage te krijgen in de gegevens die wij van jou verwerken. Daarnaast kunt je ook een verzoek (laten) indienen om gegevens te rectificeren, te beperken of helemaal te wissen uit de systemen van de school. En je hebt altijd het recht om onjuiste gegevens aan te (laten) vullen of te verbeteren. Wij zullen er vervolgens voor zorgen dat deze gegevens ook bij bedrijven waarmee wij deze gegevens van jou delen en/of uitwisselen worden aangepast.
Als je ons verzoekt om jouw gegevens te beperken of te wissen, zullen wij eerst toetsen of dit mogelijk is, in verband met wat er in de wet staat. Tevens heb je het recht om te (laten) vragen om de gegevens, die wij van jou verwerken en wij van jou of je ouders hebben ontvangen, aan jou of je ouders over te dragen of op jullie verzoek aan een andere organisatie over te dragen. Onze scholen zullen nooit besluiten over jou nemen, die alleen gebaseerd zijn op geautomatiseerde verwerking van gegevens.

Als jij (of jouw ouders) het niet eens zijn met hoe wij omgaan met jouw gegevens, dan kunnen jullie altijd opheldering vragen bij onze Functionaris Gegevensbescherming (zie de contactgegevens bovenaan deze toelichting). Indien het probleem volgens jullie niet goed door ons wordt opgelost, dan kunnen jullie dat melden bij een speciale instantie: de Autoriteit Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Onderwijsgroep
Zuid-Hollandse Waarden
voor primair en voortgezet onderwijs

Overzicht categorieën van persoonsgegevens:

Categorie	Toelichting
1. Contactgegevens	**1a:** naam, voornaam, e-mail, opleiding; **1b:** geboortedatum, geslacht; **1c:** overige gegevens te weten: adres, postcode, woonplaats, telefoonnummer en eventueel andere voor communicatie benodigde gegevens, alsmede ook een bankrekeningnummer voor het afhandelen van betalingen**;**
2. Leerling nummer	Een administratienummer dat geen andere informatie bevat dan bedoeld onder categorie 1
3. Nationaliteit en geboorteplaats	
4. Ouders, voogd	Contact gegevens van de ouders/verzorgers van leerlingen (naam, voornaam, adres, postcode, woonplaats, telefoonnummer en eventueel e-mailadres)
5. Medische gegevens	Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling, voor zover deze van belang zijn bij het nemen van aanvullende maatregelen om goed onderwijs te kunnen volgen (bv. extra tijd bij toetsen);
6. Godsdienst	Gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor het te volgen onderwijs (bijvoorbeeld: leerling vrij op bepaalde dag).
7. Studievoortgang	Gegevens betreffende de aard en het verloop van het onderwijs en de behaalde studieresultaten te weten: - Examinering (gegevens rondom het examen) - Studietraject - Begeleiding leerling (inclusief ontwikkelperspectief OPP) - Aanwezigheidsregistratie -Medisch dossier (papier) - Klas, leerjaar, opleiding
8. Onderwijsorganisatie	Gegevens met het oog op het organiseren van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen; hieronder vallen ook lesroosters, boekenlijsten, schoolpasjes enz.
9. Financiën	Gegevens voor het berekenen, vastleggen en innen van inschrijvingsgelden, school- en/of lesgelden, bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten. (denk hierbij aan een bankrekeningnummer van de ouders)
10. Beeldmateriaal	Foto's en videobeelden (met of zonder geluid) van activiteiten van de school op basis van toestemming. **Let op:** Voor pasfoto voor identificatiedoeleinden is geen toestemming nodig (schoolpas en als aanvulling op het dossier).
11. Docent /zorgcoördi-nator/ intern begeleider/ decaan / mentor	Gegevens van **docenten en begeleiders,** voor zover deze Gegevens van belang zijn voor de organisatie van de instelling en Het geven van onderwijs, opleidingen en trainingen
12. BSN (PGN)	In het onderwijs heet het BSN het persoonsgebonden nummer (PGN). Ook wel onderwijsnummer genoemd. Het PGN is hetzelfde nummer als het BSN. Scholen zijn verplicht het PGN te gebruiken in hun administratie.
13. Keten-ID (Eck-Id)	Unieke iD voor de 'educatieve contentketen'. Hiermee kunnen scholen gegevens delen, zonder dat ze direct herleidbaar zijn naar leerlingen of docenten.
14 Overige gegevens	Andere dan de onder 1 tot en met 11 bedoelde gegevens waarvan de verwerking wordt vereist of noodzakelijk is met het oog op de toepassing van een andere wet. Deze zullen apart vermeld en toegelicht worden.


Onderwijsgroep
Zuid-Hollandse Waarden
voor primair en voortgezet onderwijs