Geleding	Besproken d.d.	Besluitvorming d.d.
Staf	Staf	
Directeuren	MT 3 juli 2018	
GMR (instemming)	GMR	
College van Bestuur		CvB 3 juli 2018

Beleidsnotitie
Openbaar Primair Onderwijs Almelo

Privacyreglement OPOA
conform AVG

Inhoudsopgave

Privacyreglement Stichting Openbaar Primair Onderwijs Almelo

1. Inleiding

Informatie-uitwisseling en ICT zijn noodzakelijke onderdelen in de ondersteuning van het onderwijs. Hierbij wordt gebruik gemaakt van persoonsgegevens en is privacywetgeving van toepassing. De wet beschermt de privacy door regels op te stellen voor de verwerking van persoonsgegevens. Persoonsgegevens zijn alle gegevens waarmee direct of indirect een natuurlijk persoon (mens) kan worden geïdentificeerd, bijvoorbeeld een naam, BSN-nummer, geboortedatum etc. De wet verstaat onder verwerken alles wat er met persoonsgegevens wordt gedaan, zoals online en offline persoonsgegevens verzamelen, kopiëren, opslaan, verspreiden, publiceren, delen én uitdelen.

In Nederland is privacy onder andere uitgewerkt in de Algemene Verordening Gegevensbescherming (AVG). Dit betreft Europese privacywetgeving. In deze Verordening wordt meer nadruk gelegd op de verantwoordelijkheid van organisaties zelf ten aanzien van privacy en informatiebeveiliging. Organisaties moeten kunnen aantonen dat zij zich aan de wet houden.

1.1 Uitgangspunt van de Algemene Verordening Gegevensbescherming (AVG)

Het College van Bestuur stichting OPOA is eindverantwoordelijk voor de privacy van leerlingen en medewerkers op de openbare basisscholen. Stichting OPOA is verplicht om volgens de wet te handelen en daarbij behoorlijk en zorgvuldig te werk te gaan. Dit houdt concreet in dat het bevoegd gezag samen met de scholen vaststelt welke persoonsgegevens er verwerkt worden en wat het doel is van die verwerking. Die verantwoordelijkheid houdt ook in dat scholen ouders en leerlingen volledig moeten informeren over het gebruik van persoonsgegevens en hoe ouders gebruik kunnen maken van hun rechten. Daarnaast dient Stichting OPOA de verwerking van informatie en de beveiliging van persoonsgegevens zo optimaal mogelijk uit te voeren.

In dit privacyreglement staat aangegeven hoe stichting OPOA en haar scholen omgaat met (het beschermen van de) privacy van leerlingen en medewerkers. Het privacyreglement is (gedeeltelijk) opgenomen in de schoolgids en staat op de schoolwebsite en op de website van stichting OPOA. Het privacy-beleid maakt onderdeel uit van het sociaal veiligheidsbeleid van OPOA.

Het OPOA privacy-beleid heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering
- Het garanderen van de privacy van leerlingen en medewerkers waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan zoveel mogelijk worden voorkomen.

Het privacy-beleid van stichting OPOA geldt voor alle medewerkers (vaste dienst-betrekking/inhuur/detachering), leerlingen, ouders/verzorgers, bezoekers en externe relaties alsmede voor alle organisatieonderdelen.

Uitgangspunten stichting OPOA:

- Het OPOA privacyreglement dient te voldoen aan alle relevante wet- en regelgeving. De verwerking van persoonsgegevens gebeurt volgens de algemene voorwaarden en is gebaseerd op een van de wettelijke grondslagen (zie hoofdstuk 2);
- Op de OPOA scholen is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen;
- Het bevoegd gezag van stichting OPOA/College van Bestuur is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt alsmede eindverantwoordelijke;
- Het bevoegd gezag van stichting OPOA maakt met alle (nieuwe) partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy;

- Informatiebeveiliging en privacy is een continu proces, waarbij regelmatig (minimaal een keer per jaar) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is;
- Er is een balans tussen privacy, functionaliteit/werkbaarheid en veiligheid echter met in achtneming van de AVG.

2. Algemene voorwaarden voor het werken met persoonsgegevens

De uitgangspunten voor de privacywetgeving zijn:
- Doelbepaling
- Doelbinding
- Grondslag
- Dataminimalisatie
- Transparantie
- Data integriteit

Doelbepaling
Persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen. Persoonsgegevens worden door de scholen van OPOA verzameld voor een of meerdere van onderstaande doelen:

a. Onderwijs geven en organiseren *(bijv. de groepsindeling)*
b. Leerlingen begeleiden *(o.a. cijfers en voortgang)*
c. Het verstrekken of ter beschikking stellen van leermiddelen verstrekken *(t.b.v. inloggen bij leverancier/digitale leermiddelen)*
d. Informatie verstrekken over de hierboven genoemde organisatie en leermiddelen *(bijv. t.b.v. rapportgesprekken)*
e. Informatie over leerlingen bekendmaken (*bijv. via de eigen communicatiekanalen zoals website, ouderavond, rapport)*
f. Activiteiten van de stichting/de scholen bekendmaken op de eigen website *(en daarbij het e-mailadres bekendmaken van de leraar of leerlingen in de organisatie)*
g. Berekenen, vastleggen en innen van inschrijvingsgelden, schoolgelden, bijdragen en vergoedingen
h. Het behandelen van geschillen
i. Accountantscontrole uitoefenen
j. Uitvoering of toepassing van wet- of regelgeving *(bijv. verstrekken van info aan DUO)*

Doelbinding
De persoonsgegevens worden uitsluitend gebruikt om de omschreven doelen van de verwerking te bereiken. De scholen verwerken niet meer persoonsgegevens dan noodzakelijk is. Stichting OPOA legt in het OPOA dataregister vast welke persoonsgegevens voor welke doelen gebruikt worden en hoe lang bewaard blijven (documentatieplicht conform de AVG).

Grondslag
Persoonsgegevens mogen alleen verwerkt worden als dit is gebaseerd op een van de wettelijke grondslagen. Voor het basisonderwijs geldt dat persoonsgegevens alleen worden verwerkt op grond van:

a. Toestemming: er is toestemming gegeven door de betrokkene (hier de wettelijke vertegenwoordiger/ouderlijk gezag)
b. Overeenkomst: het gebruik van de gegevens is nodig om een overeenkomst uit te (gaan) voeren *(bijv. een overeenkomst t.b.v. tussenschoolse opvang)*
c. Wet: de wetgeving eist dat persoonsgegevens verwerkt worden *(zoals DUO)*
d. Publiekrechtelijke taak: op basis van een opgedragen publiekrechtelijke taak is gegevensverwerking noodzakelijk (*bijv. een toelaatbaarheidsverklaring speciaal onderwijs door het samenwerkingsverband)*

e. Vitaal belang: de verwerking van persoonsgegevens is noodzakelijk om een ernstige bedreiging van de gezondheid v.d. betrokkene te beperken/voorkomen *(bijv. het rechtstreeks contact opnemen met de huisarts bij een ongeval op school indien ouders niet bereikbaar zijn)*
f. Gerechtvaardigd belang: persoonsgegevens verwerken is belangrijker dan het privacybelang v.d. betrokkene *(bijv. de uitwisseling van gegevens met een uitgever t.b.v. gebruik digitaal lesmateriaal/mits op basis v. afspraak/overeenkomst)*

Dataminimalisatie
Bij de persoonsgegevens die de OPOA scholen verwerken, blijft de hoeveelheid en het soort gegevens beperkt. Ze staan in verhouding tot het doel (proportioneel/relevantie). Dit doel kan niet met minder, alternatieve of andere gegevens worden bereikt.

Dit betekent ook dat de OPOA scholen de data niet langer bewaren dan noodzakelijk. Aan ieder gegeven zit een bewaartermijn gekoppeld.

Transparantie en rechten van de betrokkene
De betrokkene (de leerling en/of zijn ouders/wettelijke vertegenwoordiger) wordt door de OPOA-scholen op transparante wijze vooraf geïnformeerd over wat er precies aan informatie wordt verwerkt, wat het doel daarvan is en welke rechten zij hebben als het gaat om (de verwerking van) persoonsgegevens. In **bijlage 1** wordt een overzicht van alle rechten en de mogelijkheid om deze rechten uit te oefenen weergegeven.

Het OPOA-privacyreglement is in te zien op de schoolwebsite en op www.opoa.nl.

Mocht de betrokkene van oordeel zijn dat aan het verzoek niet op correcte wijze is voldaan kan betrokkene de procedure zoals vermeld in de 'OPOA klachtenregeling' volgen. Ook is het conform de rechtsbescherming die de AVG biedt, mogelijk om naar de rechter te gaan.

Data-integriteit
Verwerkingen die door of namens de school gedaan worden moeten juist zijn en op het juiste moment op de juiste plaats aanwezig zijn (datakwaliteit en databeveiliging). OPOA beschikt over bewerkersovereenkomsten met leveranciers. Hierin wordt expliciet de aanwezige technische en organisatorische beveiligingsmaatregelen en het privacy-beleid weergegeven.

OPOA werkt met passende procedures om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn, zoals de autorisatiematrix, het wachtwoordbeleid en de procedure bewaar en verwijdering van gegevens.

Daarnaast werkt OPOA met een netwerkbeheerder om te zorgdragen voor een goed functionerend ICT netwerk op alle scholen en het stafbureau. De netwerkbeheerder voert het technisch beheer alsmede de back-up- en antivirusprogramma's uit op de scholen. De netwerkbeheerder voorziet haar servers van de meest recente beveiligingsupdates en beschikt over incident-continuïteitsmanagement om de continuïteit van de dienstverlening te kunnen garanderen.

Risico-analyse
Door middel van een jaarlijkse **Risico-analyse** worden de risico's ten aanzien van informatiebeveiliging en privacy en de gewenste maatregelen om deze risico's te verlagen voor stichting OPOA in beeld gebracht.

Privacy by design en privacy by default
Bij nieuwe verwerkingen/ontwikkelingen wordt vooraf aandacht besteed aan privacy verhogende maatregelen (**Privacy by design**). De voorwaarden/uitgangspunten worden vanaf de start van een project of wijziging van een applicatie waarbij persoonsgegevens verwerkt worden toegepast. De Functionaris Gegevensbescherming (FG) treedt hierbij op als adviseur.

Het is OPOA scholen niet toegestaan om zonder vooroverleg met het College van Bestuur of de Functionaris Gegevensbescherming:
- een nieuwe verwerking/applicatie aan te schaffen en/of toe te passen;
- een nieuwe ontwikkeling in te voeren

Vooraf bij nieuwe ontwikkelingen en in ieder geval bij de aankoop van (nieuwe) applicaties vindt een **Gegevensbeschermingseffect-beoordeling** plaats.

Privacy bij default vereist dat de standaardinstellingen en functies altijd zo privacy-vriendelijk mogelijk zijn (afschermen gebruikersprofielen, toestemming voor delen persoonsgegevens etc.) en dat er zo min mogelijk persoonsgegevens worden gevraagd en verwerkt. De Functionaris Gegevensbescherming (FG) treedt hierbij op als adviseur.

3. Beveiliging en geheimhouding

De scholen vallend onder stichting OPOA voldoen aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder o.a. Wet op het Primair Onderwijs en de Algemene Verordening Gegevensbescherming. Daarnaast zijn de bepalingen van het convenant 'Digitale onderwijsmiddelen en privacy 3.0' leidend bij het maken van afspraken met leveranciers.

3.1 Rollen rondom het OPOA privacy-beleid

Het **college van bestuur** is eindverantwoordelijk voor het privacy-beleid en stelt het beleid en basismaatregelen vast op het gebied van informatiebeveiliging en privacy, waaronder het aanstellen van een Functionaris Gegevensbescherming (FG).

De toepassing en werking van het InformatieBeveiliging en Privacy-beleid (IBP beleid) wordt op basis van regelmatige rapportages geëvalueerd.

Onafhankelijke Functionaris voor Gegevensbescherming (FG)
De FG houdt binnen stichting OPOA toezicht op de toepassing en naleving van de AVG. De FG:
- adviseert het schoolbestuur (bevoegd gezag) over privacy en houdt toezicht daarop;
- handelt vragen en klachten over privacy af;
- ontwikkelt (interne) regelingen rondom privacy;
- geeft advies over technologie en beveiliging (privacy by design);
- handelt zelfstandig of in samenwerking met het stafbureau (vertrouwelijke) informatiebeveiligingsincidenten af.

Stichting OPOA is bezig met een oriëntatie op de mogelijkheden om een externe FG in te huren. De verwachting is rond december 2018/januari 2019 over een onafhankelijke FG te kunnen beschikken.

Directeuren
De schooldirecteur is de proceseigenaar op de school. Hij/zij is verantwoordelijk voor de wijze van uitvoering van het OPOA privacy-beleid en vormt het aanspreekpunt voor incidenten en informatiebeveiliging op de school. De proceseigenaar heeft de volgende specifieke taken op het gebied van bescherming van privacy:
- Samen met de bovenschoolse i-coaches en het stafbureau toezien op het beleid voor toegang tot applicaties/netwerk/netwerkbeheer;
- Informeren van het schoolteam over het privacy- en beveiligingsbeleid en periodiek onder de aandacht brengen in werkoverleggen en IPB gesprekken;
- toezien op naleving van het privacy- en beveiligingsbeleid, waarbij de leidinggevende een voorbeeldrol heeft ten opzichte van de medewerkers;
- als aanspreekpunt beschikbaar zijn voor alle privacy- en beveiliging gerelateerde onderwerpen.

Bovenschoolse i-coaches
Adviseert samen met de stafmedewerker Privacy het College van Bestuur en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen de OPOA-scholen, waaronder:

- samen met het stafbureau en College van Bestuur het beleid van toegang tot applicaties/netwerk en netwerkbeheer vaststellen;
- toezien op de uitvoering van dit toegangsbeleid;
- het (regelmatig) beoordelen van toegangsrechten van gebruikers.

De **stafmedewerker Privacy** geeft terugkoppeling en advies aan het College van Bestuur en directeuren. Het stafbureau:

- vertaalt beleid naar richtlijnen, procedures, maatregelen en documenten voor de gehele organisatie;
- bewaakt de uniformiteit binnen de scholen;
- is, samen met de schooldirecteuren, aanspreekpunt voor incidenten op het gebied van informatiebeveiliging en privacy.
- Informeert de FG en neemt, in overleg met de FG, passende vervolgstappen in het geval van (mogelijke) datalekken waaronder het uitvoeren van de wettelijke meldplicht;
- coördineert in overleg met de schoolleiding de verdere afhandeling van incidenten binnen de scholen;
- draagt, in gezamenlijkheid met de FG, zorg voor regelmatig terugkerende beveiliging-bewustwording campagnes.

Medewerkers
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in dit privacyreglement en de OPOA-gedragscode.

Medewerkers wordt gevraagd om actief betrokken te zijn bij informatiebeveiliging bijvoorbeeld door het doen van verbetervoorstellen aan de schoolleiding of het stafbureau. Hiervoor is een speciaal e-mailadres aangemaakt: privacy@opoa.nl

Medewerkers zijn verplicht om melding te maken van privacy- en beveiligingsincidenten bij de schoolleiding. Hiervoor dient het 'Meldingsformulier t.b.v. (systeem)beveiligingsincident/ datalek' gebruikt te worden (**bijlage 3a**, onderdeel v.h. incidentenregistratieformulier (**bijlage 3**). Het 'Protocol bij privacy-incidenten en mogelijke datalekken' **(bijlage 2**) is hierbij van kracht.

De schoolleiding meldt het incident per direct aan de voorzitter College van Bestuur. De voorzitter College van Bestuur informeert vervolgens de FG. Afhankelijk van de ernst van het incident worden passende stappen genomen, waaronder het verscherpen, aanvullen of verbeteren van de informatiebeveiliging of het toepassen van de wettelijke meldplicht datalekken (zie ook hoofdstuk 3.4 Datalekken).

Informeren:
Informatiebescherming en privacy wordt op regelmatige basis onder de aandacht gebracht bij medewerkers, leerlingen en ouders. Dit gebeurt via bijeenkomsten, trainingen, nieuwsbrieven op initiatief van OPOA/bovenschools en tijdens reguliere school-overleg/contactmomenten.

3.2 Beveiliging

De OPOA-scholen zijn verplicht om persoonsgegevens te beveiligen tegen risico's zoals verlies, onbevoegde toegang, vernietiging, gebruik, wijziging of openbaarmaking van gegevens:

a) De OPOA-scholen nemen passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. De maatregelen zijn er

tevens op gericht om onnodige verzameling en verdere verwerking van gegevens te voorkomen.
Het is medewerkers niet toegestaan om met USB-sticks te werken.

Netwerkbeheer infrastructuur
Stichting OPOA heeft een contract afgesloten met netwerkbeheerder De Rolfgroep. De netwerkbeheerder draagt zorg voor de inrichting, het onderhoud, de veilige dataopslag en het beheer van de ict netwerkinfrastructuur van de OPOA-scholen (vastgelegd in het ServiceLevelAgreement behorende bij het contract).

b) De OPOA-scholen zorgen ervoor dat medewerkers, invallers, stagiaires en vrijwilligers niet meer inzage of toegang hebben tot de persoonsgegevens dan zij strikt noodzakelijk nodig hebben voor de goede uitvoering van hun werk. OPOA scholen werken met Office365. Iedere medewerker beschikt over een persoonlijke inlog. Op de scholen wordt gewerkt met een autorisatiematrix **(bijlage 4)** waarin staat beschreven welke medewerker welke software gebruikt, wie toegang heeft tot welke programma's en tot op welk niveau.

c) Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek en de kosten van de tenuitvoerlegging. Daarbij houden de scholen rekening met de concrete risico's die van toepassing kunnen zijn op de verwerkte persoonsgegevens.

d) Iedereen die betrokken is bij de uitvoering van dit reglement, en daarbij beschikking krijgt over persoonsgegevens die vertrouwelijk zijn of geheim moeten worden gehouden, en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift een geheimhoudingsplicht geldt, is verplicht tot geheimhouding van die persoonsgegevens. Voor invallers, stagiaires en vrijwilligers zal een verklaring tot geheimhouding worden opgesteld en ter ondertekening voorgelegd.

3.3 Controle, naleving en sancties

Toetsing
1. Het OPOA privacy-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door het College van Bestuur en het MT, hierin ondersteund door de FG. Hierbij wordt gekeken naar:
- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's en incidenten)
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

2. Daarnaast houdt de FG binnen stichting OPOA toezicht op de toepassing en naleving van de AVG en adviseert en doet aanbevelingen over privacy in het algemeen.

3. Er zal via de bovenschoolse i-coaches, de bovenschoolse ICT-er en de stafmedewerker Privacy in samenspraak met de schoolleiding, een jaarlijkse control cyclus voor informatiebeveiliging en privacy worden uitgevoerd op de OPOA-scholen. Dit is bedoeld om de inhoud en effectiviteit van de informatiebeveiliging en privacy-beleid te toetsen en waar nodig bij te stellen. De input zal op schoolniveau worden gebruikt ten behoeve van (het verhogen van de) beveiligingsbewustwording en het delen van kennis tijdens het werkoverleg. Op organisatieniveau zullen de uitkomsten van de scholen als input dienen om het privacy-beleid te evalueren en waar nodig aan te passen (zie punt 1). Het privacy-beleid maakt onderdeel uit van het sociaal veiligheidsbeleid van OPOA.

Naleving
De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het informatiebeveiliging en privacy-beleid. Binnen OPOA is sprake van een open communicatiecultuur, waarin eenieder zijn/haar verantwoordelijkheden neemt en collega's kunnen worden aangesproken in geval van tekortkomingen.
Voor de bevordering van de naleving van de AVG vervult de FG een belangrijke rol met een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt volgens een door het College van Bestuur vastgesteld reglement.

In geval van een privacy-incident en mogelijke datalekken treedt het 'Protocol bij privacy-incidenten en mogelijke datalekken' in werking **(zie ook bijlage 2)**

1. Incidenten en (mogelijke) datalekken worden direct gemeld bij de schoolleiding en/of het stafbureau. Hiervoor dient het 'Meldingsformulier t.b.v. (systeem)beveiligingsincident/datalek' gebruikt te worden (**bijlage 3a**, onderdeel v.h. incidentenregistratieformulier). De schoolleiding licht per direct de voorzitter College van Bestuur in. Dit geldt ook in het geval een privacy-incident/datalek wordt veroorzaakt of ontdekt door een 'bewerker' of andere externe.
2. Het incident wordt onderzocht door de schoolleiding, voorzitter CvB, stafmedewerker Privacy en bovenschoolse i-coaches (o.a. aard, oorzaak, beveiligingsprocedure, verwijtbaar gedrag). Indien nodig wordt de FG om advies gevraagd. Ook kan externe deskundigheid worden gezocht. Er worden passende vervolgstappen genomen waaronder het uitvoeren van de wettelijke meldplicht in het geval van een (mogelijk) datalek.
3. Het incident wordt opgenomen in de incidentenregistratie door middel van het incidentenregistratieformulier (**zie bijlage 3**). De input wordt gebruikt om het privacy-beleid te verbeteren maar ook als voorbeeld om binnen de OPOA organisatie het beveiligingsbewustzijn te vergroten.
4. Op alle OPOA scholen wordt actief aandacht besteed aan het item privacy, tijdens werkoverleggen, op OPOA workshopmiddagen, informatiebijeenkomsten etc.
5. Nieuwe medewerkers en invallers worden bij de aanstelling geïnformeerd over het OPOA beleid ten aanzien van sociale veiligheid en privacy.

Sancties
Mocht de naleving ernstig tekortschieten, dan kan de schoolleiding of het College van Bestuur de betrokken verantwoordelijke medewerker(s) een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Gevolgen bij niet naleven
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. Afhankelijk van de ernst van de gedragingen en gevolgen wordt naar de betreffende medewerker toe rechtspositionele maatregelen genomen welke variëren van waarschuwing, schorsing, berisping, ontslag en ontslag op staande voet.

3.4 Datalekken

Een **beveiligingsincident** is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.

Een **datalek** is een beveiligingsincident, waarbij persoonsgegevens verloren raken of onrechtmatig worden verwerkt (opgeslagen, aangepast, verzonden enz.). Als een persoon toegang heeft tot persoonsgegevens terwijl dat niet is toegestaan, spreken we dus over een datalek. Een voorbeeld hiervan is het verliezen van een usb-stick met leerlingdossiers. Het bevoegd gezag van stichting OPOA is verantwoordelijk voor de bescherming van persoonsgegevens van leerlingen en personeel.

Per 1 januari 2016 is de Wet meldplicht datalekken van kracht. Die wet geeft de privacy toezichthouder (Autoriteit Persoonsgegevens) een verzwaarde boetebevoegdheid. Het niet (tijdig) melden van een datalek kan bestraft worden met een forse financiële boete. De meldplicht is alleen van toepassing op datalekken die plaatsvinden in geautomatiseerde gegevensbestanden waarvoor de school verantwoordelijk is, zoals een document met de gegevens van een groep. Daarnaast moet er sprake zijn van een inbreuk op de beveiliging van persoonsgegevens die leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens *(bijvoorbeeld het hacken van een hele database met leerlinggegevens).*

Daarnaast moet de school in sommige gevallen ook de benadeelde informeren over een datalek. Met name wanneer het datalek waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer of zelfs de veiligheid van de betrokkene. De communicatie met betrokkene(n) verloopt in dit geval altijd via de voorzitter College van Bestuur.
Afhankelijk van de ernst van het incident wordt actief de pers gezocht.

Ook indien er sprake is van een datalek bij een 'verwerker' (een leverancier die in opdracht van de school en/of de stichting persoonsgegevens opslaat, verwerkt of verzamelt) is de school/stichting OPOA verplicht om een melding te doen bij de Autoriteit Persoonsgegevens.

In geval van een privacy-incident en mogelijke datalekken treedt het 'Protocol bij privacy-incidenten en mogelijke datalekken' in werking (**zie ook bijlage 2**)

In alle bovenstaande gevallen geldt voor de scholen vallend onder het bevoegd gezag van stichting OPOA dat een datalek direct wordt gemeld bij de schoolleiding en/of het stafbureau. Hiervoor dient het 'Meldingsformulier t.b.v. (systeem)beveiligingsincident/datalek' gebruikt te worden (**bijlage 3a**, onderdeel v.h. incidentenregistratieformulier). De schoolleiding licht per direct de voorzitter College van Bestuur in.

Afhankelijk van de ernst van het incident worden passende stappen genomen, waaronder het verscherpen, aanvullen of verbeteren van de informatiebeveiliging of het toepassen van de wettelijke meldplicht datalekken. Indien nodig wordt de FG om advies gevraagd.

3.5 Verstrekken gegevens aan derden

Als de wet dat verplicht kan de school/het bevoegd gezag de persoonsgegevens aan derden geven. Dit kan ook als de betrokkene aan de school/het bevoegd gezag toestemming geeft om zijn persoonsgegevens aan een derde te geven.
In alle andere gevallen gaat OPOA/gaan de OPOA-scholen terughoudend en op correcte wijze volgens het OPOA-privacyreglement en de AVG met dergelijke verzoeken om.

Verstrekken van informatie over leerlingen aan ouders
Artikel 11 van de Wet op het primair onderwijs (WPO) bepaalt dat de school over de vorderingen van de leerlingen rapporteert aan hun ouders.

Gescheiden ouders maar beide ouders hebben ouderlijk gezag
De school heeft een actieve informatieplicht. Zij moet ouders dezelfde mondelinge en schriftelijke informatie geven over de vorderingen van hun kind. De school heeft hierin een eigen verantwoordelijkheid.

Ouder zonder ouderlijk gezag
Boek 1 Burgerlijk Wetboek
Artikel 1:377b BW bepaalt dat de met het gezag belaste ouder verplicht is de andere, niet met gezag belaste ouder op de hoogte te houden van belangrijke zaken die het kind aangaan (bijv. schoolrapporten en informatie over extra begeleiding).

Indien de school ermee bekend is dat de gescheiden ouders elkaar niet informeren, dient de school mondelinge en schriftelijke informatie die zij over de leerling verstrekt, aan te bieden aan beide ouders.

De school moet de ouder zonder gezag informatie geven over belangrijke zaken over het kind of diens verzorging of opvoeding. De ouder moet daar wel zelf om vragen, de school hoeft dit dus niet uit eigen beweging te doen. De informatie kan gaan over de cognitieve en/of sociaal-emotionele ontwikkeling van het kind zoals leerprestaties of medische kwesties. Hieronder valt bijvoorbeeld een schoolrapport, maar niet een uitnodiging voor een algemene ouderavond of een schoolfoto. De informatie wordt niet verschaft als de school de informatie niet op dezelfde manier aan de ouder met het ouderlijk gezag zou verstrekken.

Op de informatieplicht kan ook een uitzondering worden gemaakt als het belang van het kind zich verzet tegen het verstrekken van de informatie. De school moet een eigen afweging over dat belang maken. De school moet de gezaghebbende ouder over een verzoek tot informatieverstrekking op de hoogte brengen. Als de ouder met gezag zich verzet tegen het verstrekken van informatie aan de andere ouder of dit niet in het belang van het kind acht, is dit onvoldoende. Deze ouder zal dit moeten onderbouwen, bij voorkeur met een gerechtelijke uitspraak waarin een beperking van de informatieplicht is opgenomen.

Op het OPOA-inschrijfformulier wordt ouders gevraagd om de juridische status met betrekking tot gezag, omgang en informatievoorziening aan te geven alsmede de mogelijkheid geboden om namen en adressen van beide ouders te noteren.

Oudergesprek: Indien een van de ouders aangeeft onder geen beding samen met de andere ouder het oudergesprek met school te kunnen voeren, behoort de school de mogelijkheid te bieden voor een afzonderlijk gesprek. Dit geldt niet alleen voor de 10-minutengesprekken en rapporten, maar ook voor gesprekken die in het kader van extra zorg voor de leerling met ouders worden gehouden.

De omvang van het aantal gescheiden ouders kan de school aanleiding geven om de contactmomenten met gescheiden ouders te reguleren.

3.6 Passend Onderwijs

Als leerlingen extra zorg of begeleiding nodig hebben, legt een school extra persoonsgegevens over de leerling vast, bijvoorbeeld over gezondheid of gedrag. Deze informatie ziet de wet als bijzondere persoonsgegevens. Een school moet extra zorgvuldig omgaan met deze gegevens.

Op het moment dat een OPOA-school gegevens wil uitwisselen met een andere organisatie, bijvoorbeeld een onderwijskundige, pedagoog of psycholoog, wordt er o.a. gewerkt met encryptie en een speciaal daarvoor aangeschaft programma in een beveiligde cloud-omgeving.

Bij het inschakelen van een externe deskundige zoals een psycholoog, is altijd de toestemming nodig van de wettelijke verzorgers (ouders). De gegevensuitwisseling met anderen moet worden vastgelegd in het leerlingdossier/Leerlingvolgsysteem, bij stichting OPOA is dat ESIS. De toegang tot het leerlingdossier met betrekking tot de bijzondere persoonsgegevens is goed beveiligd en beperkt toegankelijk door een wachtwoordautorisatie en rechtenstructuur.

Samenwerkingsverband 23-01 (SWV)

In de wetgeving passend onderwijs is vastgelegd dat de uitwisseling van persoonsgegevens tussen school en samenwerkingsverband is toegestaan voor de uitvoering van de taken van het samenwerkingsverband en voor advisering over begeleiding van leerlingen. Voor bredere uitwisseling met externen is toestemming van de ouders of wettelijke vertegenwoordiger nodig. Als andere instanties informatie over kinderen willen ontvangen, moeten ouders of wettelijke vertegenwoordiger daarvoor expliciet toestemming geven aan de school of het samenwerkingsverband.

Het samenwerkingsverband 23-01 Twente Noord is bevoegd zonder toestemming van de leerling dan wel diens wettelijk vertegenwoordiger persoonsgegevens betreffende de gezondheid van de leerling te verwerken, ten behoeve van:

a) het verdelen en toewijzen van ondersteuningsmiddelen en ondersteuningsvoorzieningen aan de scholen,
b) het beoordelen of leerlingen toelaatbaar zijn tot het onderwijs aan een speciale school voor basisonderwijs in het samenwerkingsverband of tot het speciaal onderwijs of tot

het voortgezet speciaal onderwijs, op verzoek van het bevoegd gezag van een school waar de leerling is aangemeld of ingeschreven, en

c) het adviseren over de ondersteuningsbehoefte van een leerling op verzoek van het bevoegd gezag van een school waar de leerling is aangemeld of ingeschreven, waaronder het bieden van orthopedagogische/didactische ondersteuning (OPDC) aan de leerling.

Het samenwerkingsverband is een zelfstandige organisatie die bestaat naast de school. In privacy-termen is het samenwerkingsverband dus een zelfstandige verwerkingsverantwoordelijke en zelf verantwoordelijk voor de gegevens van leerlingen. Zodra de school leerling-gegevens aanlevert aan het SWV, is het SWV verantwoordelijk voor de privacybescherming.

Voor het uitwisselen van persoonsgegevens met het SWV maken de OPOA scholen gebruik van encryptie en/of een speciaal daarvoor aangeschaft programma in een beveiligde cloud-omgeving.

Protocol gegevensuitwisseling met externen

Het OPOA 'Protocol gegevensuitwisseling met externe partijen en in het multidisciplinair overleg' is in ontwikkeling.

Op het moment dat een OPOA-school gegevens wil uitwisselen met een andere organisatie, bijvoorbeeld een onderwijskundige, pedagoog of psycholoog, of ten behoeve van een multi-disciplinair overleg, wordt er o.a. gewerkt met encryptie en een speciaal daarvoor aangeschaft programma in een beveiligde cloud-omgeving.

3.7 Bewaartermijnen

De wet vereist dat persoonsgegevens niet zomaar en onbeperkt worden bewaard. Stichting OPOA houdt voor haar scholen de wettelijke bewaartermijnen aan:

- Een bewaartermijn van 2 jaar nadat het onderwijs aan de leerling is beëindigd (tenzij de wet een andere termijn voorschrijft);
- Een bewaartermijn van 3 jaar voor het overstapdossier van een leerling die is doorverwezen naar een school voor speciaal onderwijs.

Voor de leerlingenadministratie geldt een bewaartermijn van minimaal vijf jaar vanaf datum uitschrijving.

4. Leerlinggegevens in de school

Inschrijfformulier

Op school worden veel gegevens van en over leerlingen verwerkt. Dit begint vaak bij het inschrijfformulier. Op het OPOA-inschrijfformulier wordt om niet meer informatie gevraagd dan strikt noodzakelijk om de leerling op juiste wijze in te kunnen schrijven en om te kunnen voldoen aan de wettelijke eisen van inschrijving volgens de richtlijnen van het Ministerie van Onderwijs.

Leerlingadministratiesysteem en Leerlingvolgsysteem

Nadat de leerling is ingeschreven op een van de OPOA-scholen wordt de leerling opgenomen in het Leerlingadministratiesysteem (LAS), conform de informatie zoals aangegeven op het inschrijfformulier. Het leerlingvolgsysteem wordt gebruikt om de voortgang en resultaten van de leerling, gespreksverslagen met ouders etc. te verzamelen en op te slaan.
De OPOA-scholen werken zowel voor de leerling administratie als voor het leerlingvolgsysteem met het (webbased) programma ESIS van de firma ROVICT.

Verwerking van leerlinggegevens
Op onze scholen wordt zorgvuldig omgegaan met de privacy van onze leerlingen. Het vastleggen en gebruik van persoonsgegevens van leerlingen is beperkt tot informatie die strikt noodzakelijk is voor het onderwijs. De gegevens worden beveiligd opgeslagen in een (administratief) leerlingvolgsysteem en de toegang daartoe is beperkt.

Per school is een overzicht beschikbaar van personen, waaronder begrepen derden en anderen, die zijn belast met of leidinggeven aan activiteiten die in verband staan met de verwerking van de gegevens of die daarbij noodzakelijk zijn betrokken. **Bijlage 5** 'Overzicht van diegenen die toegang hebben tot de leerling gegevens van obs ……..' wordt op schoolniveau ingevuld en jaarlijks bijgesteld.

Digitaal leermateriaal
Onze scholen maken gebruik van digitaal leermateriaal. Hierbij worden persoonsgegevens verstrekt aan leveranciers. De leveranciers leveren op hun beurt weer informatie over het leerproces van de leerling terug aan scholen. Op basis van deze informatie kunnen leerkrachten het onderwijs beter afstemmen op de leerling.

In 2015 hebben de PO-Raad en de VO-Raad als vertegenwoordigers van de scholen in Nederland met uitgevers, softwareleveranciers en distributeurs van digitaal leermateriaal het convenant 'Digitale Onderwijsmiddelen en Privacy-Leermiddelen en Toetsen' ondertekend. Dit convenant zorgt ervoor dat de scholen de regie hebben over wat er gebeurt met de gegevens die worden verwerkt bij het gebruik van digitale leermiddelen. Onderdeel van het convenant is de 'Verwerkersovereenkomst'. Hierin staan o.a. de afspraken over welke gegevens de leverancier mag gebruiken en welke beveiligingsmaatregelen door de leverancier zijn genomen om de veiligheid van de verwerkte persoonsgegevens te waarborgen staan.

Alle leveranciers die het convenant onderschrijven, zijn verplicht om een privacy-bijsluiter te verstrekken. Meer informatie over het convenant en hoe de leveranciers van digitale leermiddelen omgaan met leerling-gegevens is te vinden op de site van de PO-raad, www.poraad.nl.

Alle leveranciers van digitaal leermateriaal waar Stichting OPOA mee samenwerkt hebben het convenant onderschreven. In **bijlage 6** staat een overzicht van de huidige leveranciers en de gemaakte afspraken.

Bij het aangaan van een nieuwe overeenkomst met een (nieuwe) leverancier van digitale leermiddelen, wordt door stichting OPOA gewerkt met de 'bewerkersovereenkomst' afkomstig uit bovenvermeld convenant. Stichting OPOA/de school checkt of de leverancier aan de gewenste eisen voldoet.

Verder werken de OPOA-scholen met een autorisatiematrix: een helder overzicht van de software die door de school gebruikt wordt, welke medewerker toegang heeft tot welke software en op welk niveau.

Overstap naar een andere school
Als een leerling overstapt naar een andere school is het verplicht om informatie te delen met de nieuwe school. In de Wet primair onderwijs is geregeld dat de basisschool de nieuwe school voorziet van een onderwijskundig rapport (OKR). Voor een overstap van de basisschool naar het voortgezet onderwijs heet dit rapport het overstapdossier.

Het rapport is bedoeld om een goede, doorlopende leerlijn voor de leerling te garanderen. Via dit rapport worden alleen de gegevens overgedragen die relevant zijn voor de nieuwe school om de leerling goed te begeleiden en te laten leren.

Basisonderwijs/rechten ouders: voor de uitwisseling van het OKR/overstapdossier tussen de basisschool en de nieuwe school (basis of voortgezet) is geen toestemming van ouders nodig. Wel moeten de ouders inzage krijgen in het overstapdossier, voordat deze wordt uitgewisseld met de school voor voortgezet onderwijs. Ouders kunnen dus geen bezwaar

maken tegen de uitwisseling van informatie, maar bezwaren en opmerkingen van de ouders moeten wel opgenomen worden in het dossier.

Basisonderwijs/plicht scholen: De school moet de aan de ouders gegeven inzage ook vastleggen, d.m.v. een verslag van het gesprek met de ouders of via het aanvinken van 'inzage' in het leerling-administratiesysteem. Door de inzage schriftelijk vast te leggen, maakt de school het controleerbaar dat de wettelijk geregelde informatieplicht is nageleefd.

De OPOA-scholen maken gebruik van OverStapservice Onderwijs (OSO) om de persoonsgegevens over te dragen naar de nieuwe school. Dit gebeurt op een veilige wijze met waarborging van de privacy van de leerlingen.

Telefoonlijst/klassenlijsten
De OPOA-scholen vragen aan het begin van het nieuwe schooljaar aan ouders om contactgegevens en een telefoonnummer en/of een e-mailadres door te geven voor een klassenlijst. Hierbij wordt expliciet om toestemming voor het gebruik van deze gegevens gevraagd. Deze toestemming moet ieder jaar opnieuw worden gevraagd. Ouders kunnen hun toestemming altijd intrekken.

5. Rechten van ouders en de MR

De Algemene Verordening Gegevensbescherming (AVG) geeft de betrokkene een aantal rechten. Stichting OPOA erkent deze rechten en handelt in overeenstemming met deze rechten.
Het gaat hierbij om de volgende rechten:

Overzicht rechten

- Recht op informatie vooraf over het gebruik van persoonsgegevens door de school
- Recht op inzage in en correctie van de persoonsgegevens
- Recht op verwijdering van de persoonsgegevens die niet (langer) nodig zijn om de vastgestelde doelen te behalen
- Recht van verzet tegen verwerking van persoonsgegevens bij de grondslag gerechtvaardigd belang, of verzet tegen direct marketing en profilering. De school maakt een afweging van het privacybelang van de leerling, tegenover het belang van de school om gegevens wél te gebruiken.
- De betrokkene heeft het recht om bij toestemming, ook een beperkte toestemming te geven of toestemming te onthouden voor een onderdeel van de verwerking (granulaire toestemming)
- De betrokkene heeft het recht dat verbeteringen, aanvullingen of verwijderingen aan alle andere partijen worden doorgegeven aan wie een organisatie de persoonsgegevens van betrokkene heeft verstrekt
- Het recht op 'bevriezing van de verwerking' van gegevens
- De betrokkene heeft het 'recht om te worden vergeten' door het volledig wissen van de persoonsgegevens, tenzij er een wettelijke bewaarplicht geldt of het verwijderen in strijd is met de vrijheid van meningsuiting
- In geval van toestemming of een overeenkomst met de betrokkene, heeft de betrokkene het recht op dataportabiliteit (meenemen van data) als de verwerking van persoonsgegevens plaatsvindt op de grondslag toestemming
- Recht op melding datalek: bij een datalek heeft de betrokkene het recht om daarover geïnformeerd te worden indien zij daar een zwaarwegend belang bij hebben.

Bron: https://www.kennisnet.nl en https://autoriteitpersoonsgegevens.nl/

Deze rechten van ouders moeten binnen een termijn van (uiterlijk) 4 weken (na het verzoek) kunnen worden uitgeoefend. De school kan, onder opgave van redenen, deze termijn éénmaal verlengen met nogmaals 4 weken.

De rechten zijn alleen van toepassing op de eigen persoonsgegevens of de gegevens van de eigen kinderen of de kinderen van wie zij de wettelijke vertegenwoordiger zijn.

In **bijlage 1** wordt weergegeven op welke wijze deze rechten uitgeoefend kunnen worden.

Mocht de betrokkene van oordeel zijn dat aan het verzoek niet op correcte wijze is voldaan kan betrokkene de procedure zoals vermeld in de 'OPOA klachtenregeling' volgen. Ook is het conform de rechtsbescherming die de Algemene Verordening Gegevensbescherming (AVG) biedt, mogelijk om naar de rechter te gaan.

Medezeggenschapsraad
De Medezeggenschapsraad wordt door de school betrokken bij alle regelingen voor de verwerking van persoonsgegeven en het gebruik van leerlingvolgsystemen. De MR heeft hierbij een instemmingsrecht.

6. Gebruik van beeldmateriaal op school

Een foto waarop een leerling herkenbaar in beeld is, zegt iets over de leerling. De foto is een persoonsgegeven en daarop is de AVG van toepassing. Volgens deze wet moet door de OPOA-scholen wanneer ze beeldmateriaal of persoonlijke informatie van en over leerlingen (en ouders) publiekelijk wil delen, vooraf om toestemming van ouders/verzorgers/wettelijke vertegenwoordigers worden gevraagd.

De AVG gaat ervanuit dat de school telkens opnieuw om toestemming vraagt. Uit praktisch oogpunt is dit voor onze scholen niet haalbaar. De OPOA scholen vragen bij de inschrijving van een nieuwe leerling om toestemming om beeldmateriaal of persoonlijke informatie van leerlingen voor een specifiek doel te gebruiken (**bijlage 7** Toestemming gebruik beeldmateriaal). Deze toestemming geldt voor de duur van de schoolloopbaan van de leerling.

Ouders worden vervolgens via de schoolgids er jaarlijks op gewezen dat de school gebruik maakt van de leerlinggevens. In de schoolgids worden de rechten van ouders in deze, zoals het bezwaar kunnen maken tegen het gebruik en het intrekken van toestemming, aangegeven (**bijlage 8**).

Er is geen toestemming van ouders nodig voor het gebruik van beeldmateriaal in de klas en les voor onderwijskundige (onderzoeks)doeleinden of voor het plaatsen van een foto in bijv. het school-administratiesysteem. Wel zal de school de ouders hier apart over informeren.

Bij de ontwikkeling van een nieuwe schoolwebsite zal, in het kader van **Privacy by design** (zie hoofdstuk 2: bij nieuwe verwerkingen/ontwikkelingen wordt vooraf aandacht besteed aan privacy verhogende maatregelen), standaard worden overgegaan naar het aanbieden van beeldmateriaal via een besloten gedeelte van deze website waarbij er moet worden ingelogd met een wachtwoord.

Sociale media:
Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt en vastgelegd in het 'Sociaal mediaprotocol OPOA'. Dit protocol maakt onderdeel uit van het sociaal veiligheidsbeleid van onze scholen en is te vinden op www.opoa.nl
en de schoolwebsite.

Ouders en privacy
Op veel scholen is het zo dat ook door ouders foto's van leerlingen worden gemaakt tijdens schoolactiviteiten. En het kan voorkomen dat ouders het vervelend vinden dat andere ouders foto's maken van hun kinderen en deze vervolgens publiceren op sociale media. Stichting OPOA gaat er in eerste instantie van uit dat deze ouders samen overleggen over het maken en gebruik van die foto's.

Als er beeldmateriaal (op het beveiligde deel) van de website door ouders gekopieerd wordt en vervolgens gedeeld via sociale media is dat niet meer de verantwoordelijkheid van de school.

OPOA wil dat de school voor álle kinderen een veilige omgeving is, en niet een plek waar kinderen (en hun ouders) bang hoeven te zijn steeds te worden gefotografeerd. Het maken van foto's en video's op school kan moeilijk worden verboden, maar kan wel aan banden worden gelegd door aan te geven dat er bijv. niet in de klaslokalen mag worden gefilmd.
De OPOA scholen wijzen ouders op hun verantwoordelijkheid hierin en verzoeken ouders om terughoudend te zijn met het maken en plaatsen van foto's en video's op het internet.

De OPOA-scholen hanteren een sociale mediaprotocol, deze is in te zien op www.opoa.nl en de schoolwebsite.

7. Internet en sociale media

Internet en sociale media maken onderdeel uit van het schoolklimaat. Het gebruik van sociale media is onderdeel van het gedrag van leerlingen binnen de school.
Scholen zijn wettelijk verplicht om te zorgen voor een sociaal veilig klimaat op school. Stichting OPOA hanteert een OPOA sociale mediaprotocol. Hierin staat beschreven wat er van leerlingen en medewerkers verwacht wordt op sociale media. Het OPOA sociale mediaprotocol maakt onderdeel uit van het sociaal veiligheidsbeleid van onze scholen en is te vinden op www.opoa.nl en de schoolwebsite.

Gebruik van digitale diensten als sociale media en apps door de school
Onze OPOA-scholen maken zelf ook gebruik van sociale media tijdens de lessen. De scholen houden daarbij rekening met de privacy van de leerlingen, volgens de regels zoals in dit privacyreglement aangegeven. Voor het gebruik van sociale media door uw kind(eren), in de klas vragen wij om toestemming.

Voor leerkrachten geldt dat zij de eigen sociale media-accounts niet mogen delen met leerlingen. Wel is toegestaan om, voor onderwijsdoelstellingen, een klassenaccount op sociale media aan te maken. Ook hierop zijn de regels van het privacyreglement en het vragen van toestemming aan de wettelijk vertegenwoordiger van toepassing.

Voor het maken van content voor sociale media wordt waar mogelijk gebruik gemaakt van schoolapparatuur. Bij gebruik van privé-apparatuur wordt de gemaakte content na verwerking per direct gedeletet.

Sancties
Mocht de naleving ernstig tekortschieten, dan kan de schoolleiding of het College van Bestuur de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Gevolgen bij niet naleven
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. Afhankelijk van de ernst van de gedragingen en gevolgen wordt naar de betreffende medewerker toe rechtspositionele maatregelen genomen welke variëren van waarschuwing, schorsing, berisping, ontslag en ontslag op staande voet.

8. Personeelsgegevens

Stichting OPOA gaat zorgvuldig om met de privacy van onze leerlingen én medewerkers. Ook het vastleggen en gebruik van persoonsgegevens van medewerkers is beperkt tot informatie die strikt noodzakelijk is voor het uitvoeren van de arbeidsovereenkomst.

Persoonsgegevens worden op naam van het personeelslid verzameld. De verzameling van persoonsgegevens van het personeelslid vormt het dossier.
Verstrekken van persoonsgegevens omvat elke vorm van bekendmaken of ter beschikking stellen van persoonsgegevens (mondeling, schriftelijk, e-mail, raadplegen of meekijken). Het verstrekken van persoonsgegevens moet verenigbaar zijn met het doel van het verzamelen daarvan. Stichting OPOA mag persoonsgegevens verstrekken aan derden als:

- dit noodzakelijk is voor de uitvoering van een overeenkomst/arbeidscontract met de medewerker;
- als gegevens moeten worden verstrekt op grond van een wettelijk voorschrift of een gerechtelijke uitspraak;
- als de medewerker ondubbelzinnige toestemming heeft gegeven.

Toegang tot persoonsgegevens
Om de privacy te waarborgen is vereist dat duidelijk wordt aangegeven wie toegang hebben tot de persoonsgegevens. Toegang tot persoonsgegevens is alleen toegestaan aan degenen, waaronder begrepen derden, die zijn belast met of leidinggeven aan de activiteiten die in verband staan met de verwerking van de gegevens of die daarbij noodzakelijk zijn betrokken. Stichting OPOA hanteert hiervoor een toegangsoverzicht op school- en bovenschools niveau. In **bijlage 9** is een voorbeeldformulier opgenomen 'overzicht van diegenen die toegang hebben tot de personeelsregistratie OPOA'. Deze wordt op schoolniveau en op bovenschools niveau ingevuld en is in te zien bij de schoolleiding en P&O. Het formulier wordt jaarlijks ge-updatet.

Digitaal personeelsdossier
Stichting OPOA beschikt per 2014 over digitale personeelsdossiers. Dit betreft een samenvoeging van de gedigitaliseerde personeelsdossiers die het Onderwijsbureau Twente van OPOA medewerkers heeft. Verschillende partijen kunnen toegang krijgen tot het digitale personeelsdossier van een medewerker. De mate waarin is afhankelijk van de autorisatie die aan een persoon wordt toegekend. Er zijn vijf rollen, te weten de medewerker zelf, de manager, de adviseur P&O, de contactpersoon van de PSA en ObT-beheerder.

Het Onderwijsbureau Twente behandelt de digitale personeelsdossiers overeenkomstig de AVG met als drie belangrijke uitgangspunten:

- Toegang tot de personeelsgegevens wordt beperkt tot geautoriseerde medewerkers, voor zover deze toegang noodzakelijk is om hun functie goed te kunnen uitoefenen en mits er voldaan wordt aan de geheimhoudingsplicht.
- Medewerkers mogen zonder opgave van reden het volledige eigen personeelsdossier inzien, conform de AVG. Daarin wordt o.a. het recht op toegang tot het eigen dossier geregeld.
- Het Onderwijsbureau Twente heeft bovenop de waarborg Privacy een eigen gedragsrichtlijn opgesteld over de inrichting en autorisatie van de diverse gebruikers en rollen. Zorgvuldigheid bij de autorisatie staat hierbij voorop.

9. Gedragscode Personeel gebruik bedrijfsmiddelen

De OPOA scholen moeten kunnen aantonen dat zij de AVG naleven. Hiertoe zijn door stichting OPOA nadere afspraken opgesteld rondom ict, internet en e-mail gebruik omwille van het bedrijfsbelang. Het betreft aanvullende regels in de OPOA gedragscode over het veilig omgaan met persoonsgegevens, het melden van beveiligingsincidenten en datalekken, regels rondom aanschaf digitaal lesmateriaal en informatiesystemen en het gebruik van eigen devices alsmede beschrijft het de regels voor de controle op de naleving ervan.

Deze aanvulling op de OPOA gedragscode is in ontwikkeling.

10. Slotbepalingen

- Voor de inhoud van deze beleidsnotitie is gebruikgemaakt v.d. informatie van kennisnet.nl, Autoriteit Persoonsgegevens, LKC, PO en VO raad en NJI
- Stichting OPOA houdt zich aan/verwijst hiervoor naar de diverse wet- en regelgeving t.a.v. de privacy, waaronder de Algemene Verordening Gegevensbescherming en de Wet op het Primair Onderwijs.
- ……

11. Verdere acties

11.1 communicatie

Het privacyreglement wordt geplaatst op de website van stichting OPOA en op de schoolwebsites. In de schoolgidsen van de OPOA-scholen wordt een verwijzing opgenomen.

11.2 Evaluatie en bijstelling

Het bevoegd gezag zal de werking van het Privacyreglement tweejaarlijks evalueren met het MT, ingaande juli 2018.

Looptijd en inhoud Privacyreglement:
Het Privacyreglement kent een onbeperkte looptijd, afhankelijk van wet- en regelgeving. Tegelijkertijd met de tweejaarlijkse evaluatie vindt een eventuele bijstelling plaats (c.q. waar nodig eerder).

Evaluatie Privacyreglement

Geleding	Evaluatie/bijstelling d.d.	Besluitvorming d.d.
Staf	Staf	
Directeuren	MT	
GMR	GMR	
College van Bestuur		CvB

Bijlage 1 Procedure privacy-rechten

De betrokkene (de leerling en/of zijn ouders/wettelijke vertegenwoordiger) wordt door de OPOA-scholen op transparante wijze vooraf geïnformeerd over wat er precies aan informatie wordt verwerkt, wat het doel daarvan is en welke rechten er zijn als het gaat om (de verwerking van) persoonsgegevens. Deze informatie is te vinden in de schoolgids, de schoolwebsite en de OPOA website.

Overzicht rechten*

- Recht op informatie vooraf over het gebruik van persoonsgegevens door de school
- Recht op inzage in en correctie van de persoonsgegevens
- Recht op verwijdering van de persoonsgegevens die niet (langer) nodig zijn om de vastgestelde doelen te behalen
- Recht van verzet tegen verwerking van persoonsgegevens bij de grondslag gerechtvaardigd belang, of verzet tegen direct marketing en profilering. De school maakt een afweging van het privacybelang van de leerling, tegenover het belang van de school om gegevens wél te gebruiken.
- De betrokkene heeft het recht om bij toestemming, ook een beperkte toestemming te geven of toestemming te onthouden voor een onderdeel van de verwerking (granulaire toestemming)
- De betrokkene heeft het recht dat verbeteringen, aanvullingen of verwijderingen aan alle andere partijen worden doorgegeven aan wie een organisatie de persoonsgegevens van betrokkene heeft verstrekt
- Het recht op 'bevriezing van de verwerking' van gegevens
- De betrokkene heeft het 'recht om te worden vergeten' door het volledig wissen van de persoonsgegevens, tenzij er een wettelijke bewaarplicht geldt of het verwijderen in strijd is met de vrijheid van meningsuiting
- In geval van toestemming of een overeenkomst met de betrokkene, heeft de betrokkene het recht op dataportabiliteit (meenemen van data) als de verwerking van persoonsgegevens plaatsvindt op de grondslag toestemming
- Recht op melding datalek: bij een datalek heeft de betrokkene het recht om daarover geïnformeerd te worden indien zij daar een zwaarwegend belang bij hebben.

Bron: https://www.kennisnet.nl en https://autoriteitpersoonsgegevens.nl/

Uitoefenen van rechten

- Het verzoek om het uitoefenen van een van bovenstaande rechten kan alleen worden gedaan door de ouders/wettelijke vertegenwoordigers van de leerling, aangezien de leerling jonger dan 16 jaar is.
- Het verzoek moet worden ingediend worden bij de schoolleiding (bij voorkeur schriftelijk of digitaal, voorzien van handtekening en datum).
- De betrokkene ontvangt binnen vier weken na het indienen van zijn verzoek een gemotiveerd antwoord. De schoolleiding kan, onder opgave van redenen, de termijn om aan het verzoek te voldoen éénmaal verlengen met nogmaals vier weken.
- Als de ouders/wettelijk vertegenwoordiger toestemming hebben gegeven voor het gebruik van persoonsgegevens, dan kan dat op ieder moment weer ingetrokken worden via een schriftelijke verklaring aan de schoolleiding. Dit verzoek wordt in beginsel binnen (uiterlijk) vier weken na het verzoek uitgevoerd. De schoolleiding kan, onder opgave van redenen, de termijn om aan het verzoek te voldoen éénmaal verlengen met nogmaals vier weken, uiteraard alleen als de (veiligheid)belangen van de betrokkene niet op het spel staan.

Uitzondering bij recht op inzage
Als het in het belang van de betrokkene is om geen inzage te geven, blijft inzage achterwege (bijvoorbeeld in het geval van dossiervorming bij verdenking van misbruik of kindermishandeling).

Procedure voor het uitoefenen van rechten door betrokkenen

- Het ontvangen verzoek van betrokkene wordt binnen vier weken na het indienen beantwoord. De schoolleiding kan, onder opgave van redenen, de termijn om aan het verzoek te voldoen éénmaal verlengen met nogmaals vier weken.
- Met de betrokkene wordt een afspraak gemaakt om, afhankelijk van het recht, het verzoek uit te voeren. In geval van correctie/verwijdering zal de schoolleiding een afschrift van de gemaakte correctie/verwijdering naar betrokkene sturen.
- Mocht de betrokkene van oordeel zijn dat aan het verzoek niet op correcte wijze is voldaan kan betrokkene de procedure zoals vermeld in de 'OPOA klachtenregeling' volgen. Ook is het conform de rechtsbescherming die de Algemene Verordening Gegevensbescherming (AVG) biedt, mogelijk om naar de rechter te gaan.

*De uitvoering van privacy-rechten en bijbehorende procedure is uiteraard ook van toepassing op medewerkers van OPOA. Het woord 'schoolleiding' moet dan gelezen worden als 'College van Bestuur'.

Bijlage 2 Protocol melden privacy-incidenten en mogelijke datalekken
(versie juli 2018)

In geval van een privacy-incident en mogelijke datalekken treedt het 'Protocol bij privacy-incidenten en mogelijke datalekken' in werking.

1. Incidenten en (mogelijke) datalekken worden direct gemeld bij de schoolleiding en/of het stafbureau. Hiervoor dient het 'Meldingsformulier t.b.v. (systeem)beveiligingsincident/datalek' gebruikt te worden (**bijlage 3a**, onderdeel v.h. incidentenregistratieformulier). De schoolleiding licht per direct de voorzitter College van Bestuur in. Dit geldt ook in het geval een privacy-incident/datalek wordt veroorzaakt of ontdekt door een 'bewerker' of andere externe.
2. Het incident wordt onderzocht door de schoolleiding, voorzitter CvB, medewerker stafbureau en bovenschoolse i-coaches (o.a. aard, oorzaak, beveiligingsprocedure, verwijtbaar gedrag). Indien nodig wordt de FG om advies gevraagd. Ook kan externe deskundigheid worden gezocht. Er worden passende vervolgstappen genomen waaronder het uitvoeren van de wettelijke meldplicht in het geval van een (mogelijk) datalek.
3. Het incident wordt opgenomen in de incidentenregistratie door middel van het incidentenregistratieformulier (**zie bijlage 3**). De input wordt gebruikt om het privacy-beleid te verbeteren maar ook als voorbeeld om binnen de OPOA organisatie het beveiligingsbewustzijn te vergroten.
4. Op alle OPOA scholen wordt actief aandacht besteed aan het item privacy, tijdens werkoverleggen, op OPOA workshopmiddagen en informatiebijeenkomsten.
5. Nieuwe medewerkers en invallers worden bij de aanstelling geïnformeerd over het OPOA beleid ten aanzien van sociale veiligheid en privacy.

Sancties
Mocht de naleving ernstig tekortschieten, dan kan de schoolleiding of het College van Bestuur de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Gevolgen bij niet naleven
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. Afhankelijk van de ernst van de gedragingen en gevolgen wordt naar de betreffende medewerker toe rechtspositionele maatregelen genomen welke variëren van waarschuwing, schorsing, berisping, ontslag en ontslag op staande voet.

Bijlage 3 Incidentenregistratie
(versie juli 2018)

Incidentenregistratie

Onder een incident wordt in ieder geval verstaan:
fysiek geweld / verbaal geweld / dreigen / grof pesten / discriminatie / seksueel misbruik / seksuele intimidatie / vernielzucht / diefstal / wapenbezit / ongeluk / letsel / weglopen / (systeem)beveiligingsincident / datalek

Vul bij een incident het registratieformulier zo zorgvuldig mogelijk in.

Belangrijk:

- Een incident van ernstige aard wordt dezelfde dag gemeld bij de directeur van de school. Deze meldt het incident direct aan het College van Bestuur.
  (een meldplichtige datalek moet binnen 24 uur aan de Autoriteit Persoonsgegevens worden gemeld).

- Bij een incident van een werknemer (dus geen kind) met blijvend letsel of de dood als gevolg, wordt het incident dezelfde dag gemeld bij de arbeidsinspectie.

- Een ingevuld formulier gaat in de map incidentenregistratie.
  Een (digitale) kopie gaat naar het stafbureau, t.a.v. de stafmedewerker P&O.
  Een kopie in het dossier van slachtoffer/veroorzaker wordt aanbevolen.

- Een incident met meerdere betrokkenen wordt gezien als 1 incident en volstaat dan ook met 1 formulier.

Registratieformulier incidenten
Gegevens ten behoeve van de schriftelijke interne registratie van incidenten.

Naam school: **Naam invuller:**

Gegevens betrokkene(n)
(indien van toepassing)
Naam slachtoffer(s):
Adres(sen):
Slachtoffer(s) is/zijn: werknemer/stagiair/ouder/leerling/anders nl.:

(indien van toepassing)
Naam veroorzaker(s):
Adres(sen):
Veroorzaker(s) is/zijn: werknemer/stagiair/ouder/leerling/anders nl.:

Gegevens incident:
Plaats:
Dag en tijd:

Soort incident *(doorhalen wat niet van toepassing is)*
Incident is fysiek geweld / verbaal geweld/ dreigen/ grof pesten / discriminatie / seksueel misbruik / seksuele intimidatie / vernielzucht / diefstal / wapenbezit / ongeluk/ letsel/ weglopen/ (systeem)beveiligingsincident* / datalek* / anders;
Omschrijving incident:
……
……
……
……
……
……
……
*Indien sprake is van een (systeem)beveiligingsincident of datalek dient aanvullende informatie via het bijgaande meldingsformulier worden aangeleverd bij meldpunt privacy@opoa.nl

Behandeling *(doorhalen wat niet van toepassing is)*
Behandeling ziekenhuis / behandeling EHBO/ opname ziekenhuis/ ziekteverzuim/ leerverzuim/ geen/ anders, nl.:

……..

Afhandeling
Besproken met (ouders van) veroorzaker? Ja/nee
Bij ja, gespreksverslag toevoegen met namen, datum, gespreksonderwerp, afspraken en handtekening (ouder) veroorzaker.

Besproken met (ouders van) slachtoffer? Ja/nee
Bij ja, gespreksverslag toevoegen met namen, datum, gespreksonderwerp, afspraken en handtekening (ouder) slachtoffer.

Politie ingeschakeld? Ja/nee Aangifte gedaan? Ja/nee

Gemeld bij verzekering? Ja/nee

Psychische opvang geregeld? Ja/nee Nazorg nodig? Ja/nee

Kosten *(doorhalen wat niet van toepassing is)*
Materieel/ Fysiek letsel/ psychisch letsel/ geen/anders, nl.:……

Geschatte kosten: €……

Plaats:
Datum:

Handtekening invuller: Handtekening directie:

Openbaar Primair Onderwijs Almelo

Bijlage 3a Meldingsformulier t.b.v. (systeem)beveiligingsincident / datalek
(bijlage Incidentenregistratie versie juli 2018)

Let op: direct na ontdekking per mail opsturen naar meldpunt privacy@opoa.nl

Beveiligingsincident; een beveiligingsincident is een gebeurtenis die er voor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.

Datalek; een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken. Als er sprake is van een datalek moet daar binnen 72 uur na ontdekking melding van worden gedaan bij de Autoriteit Persoonsgegevens door het bevoegd gezag.

Datum/periode van het beveiligingsincident / datalek	
Gegevens van de melder	Naam: Functie: Werkzaam op: Hoe te bereiken:
Heeft het incident binnen de school plaatsgevonden, zo niet waar dan wel	
Toedracht van het incident	
Korte beschrijving van het incident (verlies, diefstal etc.)	
Wat voor soort gegevens zijn er bij het incident betrokken (wel of geen persoonsgegevens)	
Wie is er verantwoordelijk voor het datalek (welke persoon of organisatie)	
Welke actie is al ondernomen	

Scan dit formulier en mail het per direct door naar privacy@opoa.nl

Bijlage 4 Autorisatiematrix obs .....
(behorende bij het privacyreglement OPOA, versie juli 2018)

Leerlingen

Onderwerp/Software	Gebruiker	Rechten
ESIS a	Leerkracht, IB-er	Gebruiker
Esis b	IB-er	Gebruiker, beheer
BRON		
CITO		
Veilig leren lezen		
Digi duif		
Kurzweil		

Medewerkers

Onderwerp/Software	Gebruiker	Rechten
Digitaal personeelsdossier	Medewerker	Lezen
	Directeur	Lezen + schrijven
	Stafmedewerker P&O	Lezen + schrijven
	CvB	Lezen + schrijven
Vensters PO		

Bijlage 5 Overzicht van diegenen die toegang hebben tot de leerlinggegevens van obs ……..

(behorende bij het privacyreglement OPOA, versie juli 2018)

Functie en motivering gebruik	Toegang tot welke persoonsgegevens
Directeur	
IB	
Leerkracht	
OOP-er: administratie	
OOP-er: conciërge	
Invaller	
Stagiaire	

Deze bijlage is voor het laatst gewijzigd op …….

Bijlage 6 Uitwisseling digitale leerlinggegevens
(behorende bij het privacyreglement OPOA, versie juli 2018)

Eind 2015 hebben de PO-Raad en de VO-Raad als vertegenwoordigers van de scholen in Nederland met uitgevers, softwareleveranciers en distributeurs van digitaal leermateriaal het convenant 'Digitale Onderwijsmiddelen en Privacy-Leermiddelen en Toetsen' ondertekend. Dit convenant zorgt ervoor dat de scholen de regie hebben over wat er gebeurt met de gegevens die worden verwerkt bij het gebruik van digitale leermiddelen.

Bij het convenant hoort een 'Model Bewerkersovereenkomst'. Hierin maakt de school met de leverancier afspraken over welke gegevens de leverancier mag gebruiken. In de overeenkomst staat ook welke beveiligingsmaatregelen de leverancier treft om de veiligheid van de verwerkte persoonsgegevens te waarborgen.

Bij de Bewerkersovereenkomst hoort een 'privacy-bijsluiter'. Hierin leggen partijen vast met welk doel de gegevensverwerking plaatsvindt, wat de dienstverlening van de leverancier omvat en wat de producteigenschappen zijn en welke categorieën persoonsgegevens de leverancier verwerkt. De leverancier vult de privacy-bijsluiter in, de school gaat na of alles klopt en besluit uiteindelijk om wel of niet akkoord te gaan met de voorgestelde afspraken. Ook is er een bijlage 'Technische en organisatorische maatregelen'. Daarin staan alle beveiligingsmaatregelen beschreven. De leverancier vult deze bijlage in en de school checkt dit vervolgens.

Alle leveranciers waar stichting OPOA mee samenwerkt hebben het convenant onderschreven. Momenteel wordt door de betreffende leveranciers bekeken hoe uitvoering te geven aan de voorwaarden van de bewerkersovereenkomst met betrekking tot de huidige situatie/bestaande overeenkomsten.

Leverancier	Convenant Digitale onderwijs-middelen en Privacy-Leermiddelen en toetsen	Bewerkers-overeenkomst	Bijlage 'Privacy-bijsluiter'	Bijlage 'Technische en organisatorische maatregelen'
Stichting Basispoort (info.basispoort.nl/privacy)	√	√	√	√
Heutink Primair Onderwijs BV (www.heutink.nl/info/privacy)	√			
de Rolf groep (www.derolfgroep.nl)	√	√	√	√
L.C.G. Malmberg BV (www.malberg.nl)	√	√	√	√
Noordhoff Uitgevers (www.noordhoffuitgevers.nl/wps/portal/privacy)	√	√		
Reinders Oisterwijk BV (www.webshop.reinders-oisterwijk.nl)	√			
ThiemeMeulenhoff BV (www.thiememeulenhoff.nl/privacy)	√	√	√	

Leverancier	Convenant Digitale onderwijs-middelen en Privacy-Leermiddelen en toetsen	Bewerkers-overeenkomst	Bijlage 'Privacy-bijsluiter'	Bijlage 'Technische en organisatorische maatregelen'
Uitgeverij Zwijsen BV (www.zwijssen.nl)	√	√		
Rovict/Esis (www.rovict.nl)	√	√	√	√
Microsoft Office 365	√			
Snappet	√	√	√	√
Gynzy	√	√	√	√
CITO	√	√	√	√
CED (Nieuwsbegrip)	√	√	√	√
Overstapservice Onderwijs (OSO)	√	√	√	√
OnderwijsBureauTwente		√	√	√
Focus PO	√	√	√	√
HCS	√	√	√	√

Bijlage 7 Toestemming gebruik beeldmateriaal (via inschrijfformulier)

(Bron:www.kennisnet.nl)

Beste ouder/verzorger,

Op onze school laten wij u met beeldmateriaal (foto's en video's) zien waar we mee bezig zijn. Opnames worden gemaakt tijdens verschillende gelegenheden. Bijvoorbeeld tijdens activiteiten, schoolreisjes en lessen. Ook uw zoon/dochter kan op dit beeldmateriaal te zien zijn.

Wij gaan we zorgvuldig om met deze foto's en video's. Wij plaatsen geen beeldmateriaal waardoor leerlingen schade kunnen ondervinden. We plaatsen bij foto's en video's geen namen van leerlingen. Daarnaast zijn wij vanuit de wetgeving verplicht om uw toestemming te vragen voor het gebruik van beeldmateriaal van uw zoon/dochter als hij/zij jonger is dan 16 jaar. Ook vragen wij uw toestemming voor het gebruik van sociale media onder schooltijd voor onderwijsdoeleinden.

Uw toestemming geldt alleen voor beeldmateriaal die door ons, of in onze opdracht worden gemaakt. Het kan voorkomen dat andere ouders foto's maken tijdens schoolactiviteiten. De school heeft daar geen invloed op, maar wij vertrouwen erop dat deze ouders ook terughoudend zijn bij het plaatsen en delen van van beeldmateriaal op internet.

Wij vragen u op het toestemmingsformulier aan te geven waarvoor obs ..... beeldmateriaal van uw zoon/dochter mag gebruiken.

Als we foto's en video's willen laten maken voor onderzoeksdoeleinden, bijvoorbeeld om een les van een stagiaire op te nemen, zullen we u daar apart over informeren en zo nodig om toestemming vragen. Ook als we beeldmateriaal voor een ander doel willen gebruiken, dan op het antwoordformulier vermeld staat, nemen we contact met u op.

U mag natuurlijk altijd de door u gegeven toestemming intrekken. Ook mag u op een later moment alsnog toestemming geven. Zonder toestemming zal er geen beeldmateriaal van uw zoon/dochter gebruikt en gedeeld worden.

Wilt u getekende formulier toevoegen aan het OPOA inschrijfformulier?

Toestemmingsformulier gebruik beeldmateriaal **(behorende bij bijlage 7)**

Hierbij verklaart ondergetekende, ouders/verzorger van …….

dat beeldmateriaal door [SCHOOL] gebruikt mag worden:

Beeldmateriaal mag door [SCHOOL] gebruikt worden	Beeldmateriaal wordt gebruikt voor de volgende doelen
□ In de schoolgids en/of schoolbrochure	Informeren van (toekomstige) ouders en (toekomstige) leerlingen over de school en de onderwijsmogelijkheden. Voor PR-doeleinden van de school.
□ Op de openbare website van de school	Informeren van (toekomstige) ouders en (toekomstige) leerlingen over de school, het gegeven en te volgen onderwijs en diverse onderwijsactiviteiten zoals schoolreisjes, schoolfeesten, etc.
□ Op het besloten deel van de website van de school (indien van toepassing)	Informeren van ouders en leerlingen over de onderwijsactiviteiten zoals schoolreisjes excursies, schoolfeesten, etc.
□ In de (digitale) nieuwsbrief	Ouders en leerlingen informeren over activiteiten en ontwikkelingen op en om school
□ Op sociale-media accounts van de school (Twitter, Facebook, …..)	Informatie verspreiden over activiteiten (zoals schoolreisjes) en ontwikkelingen op school. Het delen van beeldmateriaal geeft een indruk over het gegeven onderwijs op school.
□	

* Aankruisen waar u toestemming voor geeft

De leerling mag onder schooltijd gebruik maken van sociale media voor onderwijs-doeleinden*
Ja / Nee

* doorstrepen wat niet van toepassing is

Datum: .....

Naam ouder/verzorger: .....

Handtekening ouder/verzorger: .....

****Naam ouder/verzorger: .....

Handtekening ouder/verzorger: .....

****Toestemming geven door één of twee ouders**
Als leerlingen jonger zijn dan 16 jaar beslissen de wettelijk vertegenwoordigers (de ouders) over de privacy. De wet gaat ervan uit dat je als school mag vertrouwen op de mededelingen van één ouder.
Indien sprake is van gescheiden ouders is het noodzakelijk dat beide ouders de handtekening plaatsen om toestemming te geven.

Bijlage 8 Tekst schoolgids inzake privacy
(behorende bij het privacyreglement OPOA, versie juli 2018)

Op obs …….. wordt zorgvuldig omgegaan met de privacy van de leerlingen. De school heeft leerling gegevens nodig om leerlingen goed onderwijs te kunnen geven en te begeleiden. Ook worden gegevens opgeslagen voor de goede administratieve organisatie van de school. De meeste leerling-gegevens komen van ouders (zoals bij de inschrijving op school), maar ook leerkrachten en ondersteunend personeel leggen gegevens vast over leerlingen (bijvoorbeeld cijfers en vorderingen). Soms worden er bijzondere persoonsgegevens, zoals medische informatie, geregistreerd als dat nodig is voor de juiste begeleiding van een leerling.

Tijdens de lessen wordt gebruik gemaakt van een aantal digitale leermaterialen. Hierdoor is een beperkte set met persoonsgegevens nodig om bijvoorbeeld een leerling te kunnen aanmelden in het programma. Met de leveranciers van deze leermiddelen zijn duidelijke afspraken gemaakt over het gebruik van de gegevens die ze van school krijgen. Een leverancier mag de leerling-gegevens alleen gebruiken als de school daar toestemming voor geeft.

De leerlinggegevens worden op school webbased opgeslagen in het digitale administratiesysteem ROVICT en leerlingvolgsysteem ESIS. Het programma is beveiligd en de toegang tot de persoonsgegevens is beperkt tot medewerkers van onze school. Omdat onze school onderdeel uit maakt van stichting Openbaar Primair Onderwijs Almelo (OPOA), worden daar ook (een beperkt aantal) persoonsgegevens mee gedeeld in het kader van de gemeenschappelijke administratie en het plaatsingsbeleid.

Op deze school is het Privacyreglement OPOA van toepassing, dat te vinden is op de schoolwebsite www…….. en op www.opoa.nl. Hierin is beschreven hoe op de scholen van stichting OPOA wordt omgegaan met leerling-gegevens, en wat de rechten zijn van ouders en leerlingen.

Privacy-rechten
Ouders hebben het recht om de gegevens van en over hun kinder(en) in te zien, te laten corrigeren of te verwijderen (als die gegevens niet langer nodig zijn). Deze en andere rechten staan opgenomen in het Privacyreglement OPOA. Voor vragen of het uitoefenen van deze rechten, kan contact opgenomen worden met de leerkracht van de leerling, of met de schoolleiding.

Gebruik van beeldmateriaal op school
Onze school vraagt bij de inschrijving van een nieuwe leerling om toestemming om beeldmateriaal of persoonlijke informatie van leerlingen voor een specifiek doel te gebruiken. Deze toestemming geldt voor de duur van de schoolloopbaan van de leerling. Via de schoolgids herinneren wij u jaarlijks aan de door u gegeven toestemming, de mogelijkheid om bezwaar te maken tegen het gebruik en het intrekken van uw toestemming. Ook mag u op een later moment alsnog toestemming geven.

Verstrekken gegevens aan derden
Als de wet dat verplicht kan de school/het bevoegd gezag de persoonsgegevens (informatie over een persoon) aan derden geven. Dit wordt wettelijke grondslag genoemd. Dit is bijvoorbeeld het geval bij de jaarlijkse gezondheidscheck van de Jeugd Gezondheidsdienst (JGZ/GGD). Voor meer informatie over deze wettelijke grondslag verwijzen wij u naar de website van de GGD: https://www.ggdtwente.nl/over-de-ggd/privacy

Het geven van persoonsgegevens aan een derde is ook mogelijk als de betrokkene hiervoor aan de school/het bevoegd gezag toestemming geeft. In alle andere gevallen gaat OPOA/gaan de OPOA scholen terughoudend en op correcte wijze (volgens het Privacyreglement OPOA en de AVG privacywetgeving) met dergelijke verzoeken om.

Gescheiden ouders / Ouderlijk gezag
In het Privacyreglement OPOA staat beschreven hoe de OPOA scholen omgaan met informatieverstrekking aan gescheiden ouders/ouders met ouderlijk gezag/ouders zonder ouderlijk gezag.

Op het OPOA inschrijfformulier wordt ouders gevraagd om de juridische status met betrekking tot gezag, omgang en informatievoorziening aan te geven alsmede de mogelijkheid geboden om namen en adressen van beide ouders te noteren.

Bijlage 9 Overzicht van diegenen die toegang hebben tot de personeelsregistratie OPOA

(behorende bij het privacyreglement OPOA, versie juli 2018)

Functie en motivering gebruik	Toegang tot welke persoonsgegevens
Directeur	

Deze bijlage is voor het laatst gewijzigd op …….