



Oegstgeest

Privacyreglement Medewerkers **Openbaar Primair Onderwijs Oegstgeest**

datum: 19-01-2026



Contactgegevens

Verwerkingsverantwoordelijke:

Openbaar Primair Onderwijs Oegstgeest
Adres: Jan Wolkerslaan 16, 2343BK Oegstgeest
Directeur-Bestuurder: Mevr. D. Petter
E-mail: d.petter@opoo.nl

Contactpersoon namens ons bestuur:

Contactpersoon: Dhr. R. Knijnenburg
Rol contactpersoon: IBP manager
E-mail: ibp@opoo.nl

Contactgegevens Functionaris Gegevensbescherming:

Organisatie: Privacy op School
Naam FG: Mevr. S. Koedam
Telefoonnummer: 085 01 88 313
E-mail: fg@privacyopschool.nl

Scholen:

Daltonschool Oegstgeest
Directeur: Mevr. A. ter Haar
E-mail: directie@daltonschooloegstgeest.nl

Gevers Deutz Terweeschool
Directeur: Dhr. L. Zomer
E-mail: lennartz@gdterwee.nl

Montessorischool Oegstgeest
Directeur: Mevr. H. Viëtor
E-mail: directie@montessorischool-oegstgeest.nl

OBS De Vogels
Directeur: Mevr. M. Beers
E-mail: directie@obsdevogels.nl

Inhoudsopgave

Inleiding	5
2. Totstandkoming van het privacyreglement	6
2.1 Vaststellen privacyreglement	6
2.2 Inwerkingtreding en duur van het privacyreglement	6
2.3 Reikwijdte van het privacyreglement	6
2.4 Doel van het privacyreglement	6
3. Verplichtingen van de school	7
3.1 Professioneel en integer handelen	7
3.2 Informeren van medewerkers	7
3.3 Functionaris Gegevensbescherming	7
3.4 Beveiliging van persoonsgegevens	7
3.5 DPIA (data protection impact assessment)	8
4. Soorten persoonsgegevens	9
4.1 Persoonsgegevens	9
4.2 Bijzondere persoonsgegevens	9
4.3 Wijze van verkrijgen van persoonsgegevens	10
5. Verwerken van persoonsgegevens	10
5.1 Verwerking van persoonsgegevens	10
5.2 Grondslagen voor verstrekking aan derden	11
5.3 Privacy beginselen	11
5.4 Schriftelijke afspraken over gegevensverstrekking	12
6. Doorgifte persoonsgegevens buiten de Europese economische ruimte	12
6.1 Voorwaarden voor doorgifte	12
7. Cameratoezicht	13
7.1 Doel en rechtsgrond	13
7.2 Informatie en toegang	13
7.3 Rechten van medewerkers	13
8. Beveiliging van persoonsgegevens	14
8.1 Toegang en beveiliging van persoonsgegevens	14
8.2 Aanmelden op ICT-voorzieningen	14
8.3 Monitoring	14
8.4 Datalekken	14
8.5 Bewaren en verwijderen van persoonsgegevens	15
9. Delen van persoonsgegevens	15
9.1 Verstrekking aan externe organisaties	15
10. Rechten van medewerkers	16
10.1 Recht op informatie	16



Oegstgeest

10.2 Recht op inzage persoonsgegevens	16
10.3 Recht op correctie van persoonsgegevens	17
10.4 Recht op gegevenswissing ('vergetelheid')	17
10.5 Recht op beperking van de verwerking	17
10.6 Recht van bezwaar	17
10.7 Recht overdraagbaarheid van gegevens (dataportabiliteit)	18
10.8 Geautomatiseerde besluitvorming	18
10.9 Profilering	18
10.10 Procedure bij verzoeken	19

Inleiding

Vanaf het moment dat je solliciteert naar een functie bij Openbaar Primair Onderwijs Oegstgeest (OPOO), worden er persoonsgegevens van je verwerkt. Dit gebeurt tijdens je dienstverband en soms ook daarna. In dit privacyreglement staat beschreven hoe OPOO omgaat met persoonsgegevens van medewerkers en hoe deze worden beschermd.

We verwerken naast gewone persoonsgegevens, zoals naam, geboortedatum en contactgegevens, in sommige gevallen ook bijzondere persoonsgegevens, bijvoorbeeld over je gezondheid. We vinden het belangrijk om zorgvuldig en transparant met deze gegevens om te gaan. Daarom volgen we de uitgangspunten uit de privacywetgeving (AVG) en de afspraken die in dit reglement zijn vastgelegd.

OPOO is verantwoordelijk voor de verwerking van persoonsgegevens en stelt dit privacyreglement vast. Het reglement is van toepassing op alle medewerkers van alle scholen die onder OPOO vallen. Het is voorgelegd aan de gemeenschappelijke medezeggenschapsraad (GMR) en met instemming van de personeelsgeleding vastgesteld.

Bij de verwerking van persoonsgegevens hanteren wij de volgende uitgangspunten:

1. **Rechtmatigheid, behoorlijkheid en transparantie** – persoonsgegevens worden op een eerlijke en toegankelijke manier verwerkt.
2. **Doelbinding** – gegevens worden alleen gebruikt voor vooraf bepaalde, gerechtvaardigde doelen.
3. **Dataminimalisatie** – alleen gegevens die noodzakelijk zijn, worden verwerkt.
4. **Juistheid** – we zorgen ervoor dat gegevens correct en actueel zijn.
5. **Opslagbeperking** – gegevens worden niet langer bewaard dan nodig is.
6. **Integriteit en vertrouwelijkheid** – gegevens worden goed beveiligd tegen onbevoegde toegang of verlies.
7. **Verantwoordingsplicht** – OPOO kan aantonen dat aan bovenstaande beginselen wordt voldaan.

In dit privacyreglement staat onder meer:

- Welke persoonsgegevens we verwerken;
- Voor welke doelen we dat doen;
- Hoe we de gegevens beveiligen;
- Hoe lang we gegevens bewaren;
- Welke rechten ouders en leerlingen hebben;
- Met wie we gegevens eventueel delen;
- En hoe we toezicht houden op naleving van de regels.



Oegstgeest

Het reglement is vastgesteld door het bestuur van OPOO en ter instemming voorgelegd aan de Gemeenschappelijke Medezeggenschapsraad (GMR). De Functionaris voor Gegevensbescherming (FG) houdt binnen de organisatie toezicht op de toepassing en naleving van de privacyregels.

mevr. D. Petter
Directeur bestuurder OPOO

2. Totstandkoming van het privacyreglement

2.1 Vaststellen privacyreglement

2.1.1 Dit privacyreglement is vastgesteld door het schoolbestuur, met instemming van de personeelsgeleding van de (G)MR. De datum van vaststelling staat op het voorblad.

2.1.2 Dit reglement vervangt alle eerdere privacyreglementen van de school.

2.1.3 In gevallen waarin dit privacyreglement geen duidelijkheid biedt, beslist het schoolbestuur.

2.2 Inwerkingtreding en duur van het privacyreglement

2.2.1 Het privacyreglement kan tussentijds worden aangepast op verzoek van het schoolbestuur.

2.3 Reikwijdte van het privacyreglement

2.3.1 Dit privacyreglement heeft betrekking op de verwerking van persoonsgegevens van medewerkers.

2.3.2 Met dit reglement wil de school openheid bieden aan medewerkers over hoe wordt omgegaan met de aan haar toevertrouwde gegevens.

2.3.3 Dit reglement is niet van toepassing op persoonsgegevens die zijn opgenomen in bestanden van instanties waarmee de school samenwerkt en die zelf als verwerkings-verantwoordelijke optreden, zoals de externe vertrouwenspersoon, interne vertrouwenspersonen, klachten- en geschillencommissies. In die gevallen gelden de privacyregels van die instanties.

2.4 Doel van het privacyreglement

Dit privacyreglement heeft als doel:

- De privacy van medewerkers te beschermen tegen onjuist en onbedoeld gebruik van persoonsgegevens;
- Uit te leggen welke persoonsgegevens worden verwerkt en met welk doel;
- De zorgvuldige verwerking van persoonsgegevens te waarborgen;
- De rechten van de medewerkers te beschermen.



Oegstgeest

3. Verplichtingen van de school

3.1 Professioneel en integer handelen

3.1.1 De school gaat zorgvuldig, veilig en betrouwbaar om met persoonsgegevens, met inachtneming van de wettelijke verplichtingen die voor de school gelden.

3.1.2 De school spant zich in om:

- De persoonlijke levenssfeer van de medewerkers te beschermen tegen verlies, misbruik of opslag van onjuiste gegevens;
- Te voorkomen dat gegevens voor andere doelen worden gebruikt dan waarvoor ze zijn verstrekt;
- De rechten van de medewerker te waarborgen.

3.2 Informeren van medewerkers

De school is verplicht de volgende informatie aan de medewerker te verstrekken:

- De identiteit van de school;
- De doeleinden van de gegevensverwerking;
- De contactgegevens van de vertegenwoordiger van de school;
- De contactgegevens van de functionaris gegevensbescherming;
- De ontvangers van persoonsgegevens;
- Het bestaan van de rechten van medewerkers;
- De bewaartermijnen van persoonsgegevens;
- Het recht om een klacht in te dienen bij de autoriteit persoonsgegevens;
- Nadere informatie voor zover nodig om een zorgvuldige verwerking te waarborgen.

Aanvullende informatie over verwerkingen staat in de [Privacyverklaring](#).

3.3 Functionaris Gegevensbescherming

3.3.1 Het schoolbestuur heeft een Functionaris Gegevensbescherming (FG) aangesteld. De Functionaris Gegevensbescherming is te bereiken via de contactgegevens in dit document.

3.3.2 De FG vervult ten minste de volgende taken:

- Toezicht houden op de naleving van wet- en regelgeving en het privacyreglement;
- Adviseren van het bestuur over privacyzaken;
- Adviseren over het uitvoeren van een DPIA;
- Fungeren als centraal aanspreekpunt voor vragen en klachten over het privacybeleid.

3.4 Beveiliging van persoonsgegevens

3.4.1 OPOO treft passende fysieke, technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies, onrechtmatige verwerking en onbevoegde toegang.



Oegstgeest

Deze maatregelen houden rekening met de stand van de techniek, de kosten van uitvoering, de aard van de gegevens en de risico's van de verwerking. Ook zijn ze erop gericht onnodige verzameling en verwerking van persoonsgegevens te voorkomen.

3.4.2 Medewerkers die toegang hebben tot persoonsgegevens waarvan zij het vertrouwelijke karakter kennen of redelijkerwijs kunnen vermoeden, zijn tot geheimhouding verplicht.

Dit geldt tenzij zij uit hoofde van hun beroep, functie of een wettelijke bepaling al een geheimhoudingsplicht hebben, of wanneer een wettelijk voorschrift of hun taak noodzaakt tot bekendmaking van die gegevens.

3.4.3 OPOO is verantwoordelijk voor de naleving van dit reglement en voor de juistheid en volledigheid van de verwerkte persoonsgegevens.

3.5 DPIA (data protection impact assessment)

3.5.1 In de volgende gevallen is het uitvoeren van een Data Protection Impact Assessment (DPIA) verplicht:

- Bij een systematische en uitgebreide beoordeling van persoonlijke kenmerken van medewerkers, waaronder profilering;
- Bij de grootschalige verwerking van bijzondere persoonsgegevens;
- Bij het grootschalig en systematisch volgen van personen in openbare ruimtes (zoals cameratoezicht);
- Bij de grootschalige verwerking en vastlegging van persoonsgegevens van medewerkers in centrale systemen.
- Bij inzet van AI-toepassingen, monitoringtools of nieuwe HR-analytics.

3.5.2 Een DPIA wordt minimaal eens per drie jaar uitgevoerd, of eerder als zich significante wijzigingen voordoen in de verwerking van persoonsgegevens.



Oegstgeest

4. Soorten persoonsgegevens

4.1 Persoonsgegevens

4.1.1 De school streeft bij het verwerken van persoonsgegevens naar een zo minimaal mogelijke vastlegging. Dit betekent dat alleen persoonsgegevens worden verwerkt die nodig zijn voor het uitvoeren van de overeenkomst en de daarbij komende werkzaamheden en verplichtingen.

4.1.2 De volgende persoonsgegevens van de medewerkers worden vastgelegd.

Identificatie- en contactgegevens:

Naam, geslacht, geboortedatum en plaats, burgerlijke staat, adres/woonplaats, telefoonnummer, e-mailadres, nationaliteit, BSN (of tijdelijk nummer), kopie ID, bankrekeningnummer en naam en telefoonnummer noodcontact.

Dienstverband & loopbaan:

Gegevens over (voorgaande) dienstverbanden, functies, kwalificaties, opleidingen, VOG, salaris en vergoedingen.

HR & inzetbaarheid:

Functioneren, medische informatie op eigen verzoek, verlof, verzuim en gegevens van arbodienst (alleen voor inzetbaarheid/arbobeleid).

Onderwijsuitvoering:

Personeelsnummer, klas/taak, planning, organisatorische eenheid, functie, roosters, werktijden, gegevens met betrekking tot de gesprekscyclus.

ICT & veiligheid:

Inlognaam en wachtwoord, IP-adres, gebruikersrechten, diagnostische/loggegevens, cookies/online gebruiksgegevens en e-mail- en berichtenverkeer (voor zover noodzakelijk in het kader van de functie en beveiliging).

Beeldmateriaal:

Foto's en video-opnamen, waaronder cameratoezicht (indien van toepassing op locatie)

4.1.3 Wijzigingen in wet- en regelgeving kunnen leiden tot meer of minder vastlegging van persoonsgegevens.

4.2 Bijzondere persoonsgegevens

4.2.1 De school neemt geen bijzondere persoonsgegevens op in haar systemen, tenzij dit strikt noodzakelijk is in het belang van de medewerker. Hierbij gaat het om:

- Gezondheidsgegevens;
- Godsdienst of levensovertuiging;
- Strafrechtelijke persoonsgegevens.



Oegstgeest

4.2.2 Het dossier van een medewerker wordt bewaard op een afgesloten fysieke locatie of een afgeschermd digitale omgeving.

4.3 Wijze van verkrijgen van persoonsgegevens

4.3.1 De persoonsgegevens worden, voor zover mogelijk, door de medewerker zelf verstrekt bij indiensttreding.

4.3.2 De medewerker is zelf verantwoordelijk voor het tijdig aanleveren en de juistheid van zijn of haar persoonsgegevens.

4.3.3 De persoonsgegevens worden uitsluitend verwerkt door daartoe bevoegde en geautoriseerde medewerkers en vastgelegd in de personeelsinformatiesystemen.

4.3.4 Als OPOO aanvullende informatie over een medewerker nodig heeft, wordt deze alleen opgevraagd als daar een geldige grondslag voor bestaat.

4.3.5 Als OPOO persoonsgegevens van derden ontvangt over een medewerker, heeft de medewerker het recht deze gegevens in te zien en, indien nodig, te laten corrigeren of aanvullen.

5. Verwerken van persoonsgegevens

5.1 Verwerking van persoonsgegevens

5.1.1 Bij de verwerking van persoonsgegevens houdt de school zich te allen tijde aan de geldende wet- en regelgeving.

5.1.2 De verwerking van persoonsgegevens vindt plaats voor onder andere, maar niet uitsluitend:

A. Uitvoering van de arbeidsovereenkomst

- Het aangaan en uitvoeren van een arbeidsovereenkomst of andere overeenkomst op basis waarvan de medewerker werkzaam is voor OPOO;
- Het verstrekken of beschikbaar stellen van middelen (zoals ict-middelen, toegangspassen);
- Het uitbetalen van salarissen, onkostenvergoedingen en declaraties;
- Het aangaan en uitvoeren van overeenkomsten met externe verwerkers of verantwoordelijken (zoals Google, pensioenfondsen).

B. Voldoen aan een wettelijke verplichting

- Het uitvoeren van controles (bijv. Door een accountant of de inspectie van het onderwijs);
- Het nakomen van fiscale en sociale zekerheidsverplichtingen (zoals richting belastingdienst of UWV).

C. Gerechtvaardigd belang van OPOO

- Het uitvoeren van videocameratoezicht (bijvoorbeeld op schoollocaties);
- Het intern gebruik van beeldmateriaal van medewerkers, voor zover geen toestemming vereist is.

D. Toestemming van de medewerker

- Het gebruik van beeldmateriaal voor externe of publicitaire doeleinden (zoals website of nieuwsbrief);
- Het vastleggen van gezondheidsgegevens op verzoek van de medewerker (bijvoorbeeld in het kader van begeleiding of aanpassing van werkzaamheden).

5.2 Grondslagen voor verstrekking aan derden

Het verstrekken van persoonsgegevens aan derden vindt uitsluitend plaats op basis van één van de grondslagen in de AVG.

De meest voorkomende grondslagen op basis waarvan we persoonsgegevens verstrekken:

A. Wettelijke verplichting

OPOO is gebonden aan onder meer de onderwijswetgeving. Op grond hiervan is het in bepaalde situaties verplicht persoonsgegevens van medewerkers aan externe partijen te verstrekken. Denk bijvoorbeeld aan het verstrekken van gegevens aan de belastingdienst of pensioenfondsen.

B. Uitvoering van een overeenkomst

Om de arbeidsovereenkomst of een andere overeenkomst goed uit te voeren, kan OPOO persoonsgegevens verstrekken aan derden, als dit noodzakelijk is voor de uitvoering van die overeenkomst.

C. Gerechtvaardigd belang

OPOO mag persoonsgegevens verstrekken aan derden wanneer dit noodzakelijk is voor de behartiging van een gerechtvaardigd belang van OPOO of van een derde, tenzij het belang of de rechten en vrijheden van de medewerker zwaarder wegen. In dat geval wordt een zorgvuldige belangenafweging gemaakt.

Verstrekking op grond van een gerechtvaardigd belang kan bijvoorbeeld plaatsvinden in de volgende situaties:

- Het uit handen geven van vorderingen;
- Het voeren van juridische procedures of behandelen van geschillen;
- Het laten uitvoeren van accountants- of inspectiecontroles.

D. Toestemming van de medewerker

Als geen van de bovenstaande grondslagen van toepassing is, zal OPOO persoonsgegevens alleen aan derden verstrekken met uitdrukkelijke toestemming van de medewerker. Een actuele verwerkerslijst is op verzoek beschikbaar.

5.3 Privacy beginselen

Elke verstrekking van persoonsgegevens aan derden moet, naast een geldige grondslag, voldoen aan de volgende beginselen:

A. Subsidiariteit

Het beoogde doel mag in redelijkheid niet op een andere, minder ingrijpende manier voor de medewerker kunnen worden bereikt.

B. Proportionaliteit

De inbreuk op de belangen van de medewerker mag niet onevenredig zijn in verhouding tot het doel dat met de gegevensverwerking wordt nagestreefd.

C. Dataminimalisatie

OPOO verstrekt niet méér en niet langer persoonsgegevens dan strikt noodzakelijk is voor het bereiken van het doel van de derde partij. Alleen die gegevens die nodig zijn om het doel te bereiken, worden verstrekt - niet de volledige administratie.

5.4 Schriftelijke afspraken over gegevensverstrekking

5.4.1 Bij regelmatige verstrekking van persoonsgegevens aan derden maken de school en de derde duidelijke afspraken over de veilige uitwisseling van die gegevens.

5.4.2 Wanneer de school een externe partij inschakelt die persoonsgegevens namens haar verwerkt, wordt altijd een verwerkersovereenkomst afgesloten.

6. Doorgifte persoonsgegevens buiten de Europese economische ruimte

De school geeft persoonsgegevens alleen door aan landen buiten de Europese economische ruimte als deze landen een passend beschermingsniveau bieden, zoals de algemene verordening gegevensbescherming (AVG) voorschrijft.

6.1 Voorwaarden voor doorgifte

6.1.1 Adequaatheidsbesluit: de school mag persoonsgegevens doorgeven aan landen waarvoor de Europese Commissie heeft vastgesteld dat zij een goed beschermingsniveau bieden.

6.1.2 Passende waarborgen: als er geen adequaatheidsbesluit is, zorgt de school voor andere passende maatregelen, zoals modelcontracten (standard contractual clauses), gedragscodes, certificeringen of interne afspraken binnen internationale organisaties (binding corporate rules).

6.1.3 Specifieke uitzonderingen: in bijzondere situaties mag de school persoonsgegevens doorgeven als er bijvoorbeeld toestemming is gegeven, dit nodig is voor het uitvoeren van een contract, of er belangrijke redenen zijn van algemeen belang.

7. Cameratoezicht

Op een aantal van onze scholen is sprake van cameratoezicht. Dit gebeurt uitsluitend op locaties waar dat noodzakelijk is, zoals buitenterreinen. Cameratoezicht vindt nadrukkelijk niet plaats in klaslokalen en privéruimtes zoals toiletten, kleedkamers of spreekkamers.

7.1 Doel en rechtsgrond

Het doel van het cameratoezicht is:

- De beveiliging en vastleggen van de toegang tot gebouwen en terreinen, waaronder mede is begrepen het weren van onbevoegde of onbevoegd verklaarde personen;
- Het voorkomen en registreren van overlast en strafbare feiten zoals vandalisme, diefstal en inbraak;
- De bewaking van zaken die zich op het terrein bevinden;
- De bescherming van de veiligheid en gezondheid van leerlingen, medewerkers en bezoekers op het terrein.

Het cameratoezicht is gebaseerd op een gerechtvaardigd belang. Daarbij is een belangenafweging uitgevoerd waarbij privacy en beveiliging zorgvuldig zijn meegewogen. Tevens is een Data Protection Impact Assessment (DPIA) uitgevoerd, gezien het structurele karakter van het toezicht op jongeren. De risico's zijn afgedekt met passende maatregelen, zoals een gerichte plaatsing van camera's en beperkte bewaartermijnen.

7.2 Informatie en toegang

Op de locaties waar cameratoezicht plaatsvindt, zijn duidelijke borden of stickers aangebracht die medewerkers informeren over het toezicht.

De camerabeelden worden beveiligd opgeslagen en zijn uitsluitend toegankelijk voor geautoriseerde functionarissen binnen onze organisatie. Beelden worden maximaal vier weken bewaard, tenzij er sprake is van een incident. In dat geval kunnen de beelden langer worden bewaard, uitsluitend zolang dat noodzakelijk is voor de afhandeling van het incident. Beelden worden uitsluitend verstrekt aan bevoegde instanties zoals de politie, en alleen in het kader van een onderzoek naar strafbare feiten.

7.3 Rechten van medewerkers

Medewerkers hebben het recht om:

- Bezwaar te maken tegen het cameratoezicht;
- Inzage te vragen in beelden waarop zij herkenbaar zijn;
- Verwijdering van beelden te verzoeken, indien daartoe aanleiding bestaat.

Verzoeken kunnen worden ingediend via de directeur van de school. De nadere uitwerking (locaties, plaatsingsplan, bewaartermijn, rollen & bevoegdheden,



logregistratie) is vastgelegd in een kwaliteitskaart welke op verzoek kan worden ingezien.

8. Beveiliging van persoonsgegevens

8.1 Toegang en beveiliging van persoonsgegevens

8.1.1 De school beperkt de toegang tot persoonsgegevens tot medewerkers die deze nodig hebben voor hun werk.

8.1.2 Iedereen die met persoonsgegevens werkt, moet geheimhouding beloven via een ondertekende geheimhoudingsverklaring.

8.1.3 Derden en verwerkers mogen alleen toegang krijgen als ze daartoe gemachtigd zijn of als dit wettelijk verplicht is of nodig is voor een gerechtvaardigd belang.

8.1.4 De school is verantwoordelijk voor het naleven van dit reglement en zorgt dat persoonsgegevens juist en volledig zijn.

8.1.5 Er worden technische, organisatorische en fysieke maatregelen genomen om persoonsgegevens te beschermen tegen verlies, misbruik of onbevoegde toegang.

8.2 Aanmelden op ICT-voorzieningen

8.2.1 Iedereen die de ICT-voorzieningen van de school wil gebruiken (zoals wifi) moet inloggen met een persoonlijk account.

8.2.2 Anoniem gebruik is niet toegestaan; aanmelden is altijd verplicht.

8.2.3 De voorwaarden voor het gebruik van ICT staan beschreven in het reglement verantwoord gebruik ICT middelen voor medewerkers, dat online beschikbaar is.

8.3 Monitoring

8.3.1 Door aan te melden op ICT-voorzieningen kan de school het gebruik monitoren. Dit helpt om het netwerk goed te laten werken en problemen snel op te sporen.

8.3.2 Monitoring wordt alleen gebruikt voor het beheren en beveiligen van het netwerk.

8.4 Datalekken

8.4.1 Bij een beveiligingsincident waarbij persoonsgegevens verloren gaan of onrechtmatig worden verwerkt, meldt OPOO dit aan de Autoriteit Persoonsgegevens, tenzij het risico voor betrokkenen als klein wordt beoordeeld.

8.4.2 Elk incident wordt geregistreerd, ook als er geen meldingsplicht geldt.

8.4.3 Als de inbreuk een hoog risico inhoudt voor de rechten en vrijheden van de medewerker, informeert OPOO de medewerker onverwijld over de inbreuk. Deze melding kan achterwege blijven wanneer:



Oegstgeest

- de persoonsgegevens versleuteld zijn en niet toegankelijk voor derden.
- er inmiddels maatregelen zijn getroffen die het hoge risico hebben weggenomen.
- de melding een onevenredige inspanning vereist. In dat geval kan een openbare mededeling volstaan.

8.4.4 OPOO volgt bij de afhandeling het geldende beleid en protocol voor datalekken.

8.4.5 Medewerkers kunnen vermoedens van datalekken melden via ibp@opoo.nl. Meld onmiddellijk en uiterlijk binnen 24 uur na constatering.

8.5 Bewaren en verwijderen van persoonsgegevens

8.5.1 Persoonsgegevens worden niet langer bewaard dan nodig is.

8.5.2 De school volgt wettelijke bewaartermijnen.

8.5.3 Gegevens kunnen langer bewaard worden als dit belangrijk is voor anderen, een goede administratie vereist is, een rechtszaak mogelijk is, of als er wettelijk verplichtingen zijn.

8.5.4 Gegevens die niet meer naar personen te herleiden zijn, kunnen geanonimiseerd blijven bestaan.

9. Delen van persoonsgegevens

9.1 Verstrekking aan externe organisaties

9.1.1 OPOO kan persoonsgegevens aan externe organisaties verstrekken, mits hiervoor een wettelijke verplichting of grondslag bestaat.

9.1.2 Persoonsgegevens van medewerkers worden in ieder geval gedeeld met:

- De belastingdienst;
- Het Uitvoeringsinstituut Werknemers Verzekeringen (UWV);
- Het ABP;
- Leveranciers van digitale diensten die OPOO gebruikt in het kader van het onderwijs en de begeleiding van leerlingen, bedrijfsvoering, HR en ondersteunende diensten;
- Overige derden, voor zover de verstrekking voortvloeit uit het doel van de gegevensverwerking, is vereist op grond van een wettelijk voorschrift, of noodzakelijk is voor de uitvoering van een overeenkomst waarbij de medewerker partij is.

9.1.3 OPOO houdt een actueel overzicht bij van alle externe partijen waarmee persoonsgegevens worden gedeeld. Dit overzicht is op verzoek beschikbaar.

9.1.4 Persoonsgegevens zoals bedoeld in lid 1 kunnen aan derden worden verstrekt indien OPOO dit in het belang van de medewerker acht. Dit gebeurt alleen nadat het voornemen daartoe aan de medewerker is medegedeeld, inclusief een mogelijkheid



bezwaar te maken binnen een termijn van zes weken, en er geen bezwaar is gemaakt.

10. Rechten van medewerkers

Op grond van de wet en dit privacyreglement heeft de medewerker een aantal rechten met betrekking tot zijn of haar persoonsgegevens.

De medewerker heeft in ieder geval recht op:

- Inzage in zijn of haar personeelsdossier;
- Correctie van onjuiste of onvolledige persoonsgegevens;
- Verwijdering van persoonsgegevens, voor zover er geen wettelijke verplichting tot bewaring bestaat;
- Beperking van de verwerking;
- Bezwaar tegen verwerking op grond van een gerechtvaardigd belang;
- Overdraagbaarheid van gegevens (dataportabiliteit), indien van toepassing.

De directeur is verantwoordelijk voor het behandelen van verzoeken zoals genoemd in dit hoofdstuk.

OPOO informeert de medewerker zo spoedig mogelijk, maar uiterlijk binnen één maand na ontvangst van het verzoek, over de uitkomst ervan.

Indien nodig kan deze termijn met maximaal twee maanden worden verlengd. In dat geval wordt de medewerker tijdig geïnformeerd over de verlenging en de reden daarvan.

Voor het indienen van een verzoek worden in beginsel geen kosten in rekening gebracht, tenzij sprake is van een kennelijk ongegrond of buitensporig verzoek.

10.1 Recht op informatie

De medewerker wordt, onder andere via dit privacyreglement, geïnformeerd over de verwerking van zijn of haar persoonsgegevens door OPOO.

Informatie over het gebruik van cookies en vergelijkbare technieken op onze (intra)net-omgevingen is opgenomen in de [Cookieverklaring](#).

Aanvullende informatie over verwerkingen staat in de [Privacyverklaring](#).

10.2 Recht op inzage persoonsgegevens

De medewerker heeft het recht om zijn of haar persoonsgegevens die door OPOO worden verwerkt, in te zien. OPOO zorgt ervoor dat medewerkers via digitale middelen inzage kan krijgen in hun eigen persoonsgegevens.

Indien een medewerker, anders dan via de in lid 2 genoemde digitale weg, inzage wil in zijn of haar dossier, moet hij of zij zich identificeren met een geldig identiteitsbewijs. Er wordt bij de vaststelling van de identiteit geen kopie van het identiteitsbewijs opgenomen in de administratie.



Oegstgeest

10.3 Recht op correctie van persoonsgegevens

De medewerker heeft het recht te verzoeken om verbetering, aanvulling of verwijdering van zijn of haar persoonsgegevens, bijvoorbeeld door een aanvullende verklaring te verstrekken. Feitelijke onjuistheden worden zo snel mogelijk gecorrigeerd.

OPOO is verplicht om elke derde aan wie de persoonsgegevens zijn verstrekt, op de hoogte te stellen van de correctie, tenzij dit onmogelijk is of onevenredig veel inspanning vergt.

10.4 Recht op gegevenswissing ('vergetelheid')

OPOO is verplicht persoonsgegevens van de medewerker zonder onredelijke vertraging te wissen, onder andere in de volgende gevallen:

- De persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor ze zijn verzameld of verwerkt;
- De medewerker trekt zijn toestemming in en er is geen andere rechtsgrond voor de verwerking;
- De medewerker maakt gegrond bezwaar tegen de verwerking;
- De persoonsgegevens zijn onrechtmatig verwerkt.

10.5 Recht op beperking van de verwerking

De medewerker heeft het recht om OPOO te verzoeken de verwerking van zijn of haar persoonsgegevens (tijdelijk) te beperken indien:

- De juistheid van de persoonsgegevens wordt betwist;
- De persoonsgegevens onrechtmatig zijn verwerkt;
- De persoonsgegevens niet langer nodig zijn voor het oorspronkelijke doel, maar nog wel door de medewerker worden gewenst voor bijvoorbeeld een rechtsvordering;
- Bezwaar is gemaakt tegen de verwerking en nog niet is beslist of het belang van OPOO zwaarder weegt dan dat van de medewerker.

De beperking van de verwerking moet duidelijk in de administratie worden aangegeven, zodat ook andere geautoriseerde partijen dit kunnen zien.

Gedurende de beperking mogen de gegevens alleen worden verwerkt met toestemming van de medewerker, of voor een rechtsvordering.

OPOO zal de beperking pas opheffen nadat de medewerker hierover is geïnformeerd.

10.6 Recht van bezwaar

De medewerker heeft het recht om bezwaar te maken tegen de verwerking van zijn of haar persoonsgegevens vanwege omstandigheden die verband houden met de persoonlijke situatie. In het bezwaar wordt toegelicht waarom het privacybelang van de medewerker zwaarder zou moeten wegen.

Bij een gegrond bezwaar zal OPOO de verwerking van de persoonsgegevens staken, tenzij dwingende gerechtvaardigde gronden anders vereisen.

10.7 Recht overdraagbaarheid van gegevens (dataportabiliteit)

De medewerker heeft het recht om de persoonsgegevens die hij of zij aan OPOO heeft verstrekt, te ontvangen in een gestructureerd, gangbaar en digitaal leesbaar formaat.

De medewerker heeft daarnaast het recht om deze gegevens over te dragen aan een andere verwerkingsverantwoordelijke, zonder daarbij te worden gehinderd of beperkt door OPOO.

10.8 Geautomatiseerde besluitvorming

Voor de inzet van AI-toepassingen en algoritmes geldt het AI-beleid. OPOO neemt geen besluiten over medewerkers die uitsluitend zijn gebaseerd op geautomatiseerde verwerking van persoonsgegevens, als deze besluiten rechtsgevolgen hebben of medewerkers in aanmerkelijke mate treffen.

Dat betekent dat er geen besluiten worden genomen zonder menselijke tussenkomst, zoals het automatisch afwijzen van sollicitaties, het automatisch beëindigen van contracten of het automatisch opleggen van disciplinaire maatregelen.

Bij belangrijke beslissingen is altijd een medewerker betrokken en worden persoonlijke omstandigheden meegewogen.

Mocht geautomatiseerde besluitvorming toch worden toegepast, dan wordt de medewerker hierover vooraf geïnformeerd en wordt, indien nodig, expliciete toestemming gevraagd. De medewerker kan altijd om menselijke tussenkomst verzoeken.

10.9 Profilering

OPOO maakt in zeer beperkte mate gebruik van profilering, bijvoorbeeld:

- In HR-systemen voor de analyse van personeelsgegevens;
- Voor het signaleren van opleidings- of ontwikkelbehoeften;
- In planningssoftware of inzetregistratiesystemen;
- Voor rapportages over verzuim of inzet.

Profilering wordt uitsluitend toegepast voor interne bedrijfsvoering of personeelsbeleid, niet voor commerciële of marketingdoeleinden.

Bij het gebruik van profilering gelden de volgende uitgangspunten:

- Menselijke beoordeling: profilering leidt nooit automatisch tot ingrijpende besluiten zonder menselijke toets.
- Transparantie: medewerkers worden geïnformeerd over het gebruik van profilering.
- Doelbeperking: profilering vindt alleen plaats binnen de doelen van personeelsbeleid of bedrijfsvoering.
- Controle en evaluatie: gebruikte algoritmes of modellen worden regelmatig beoordeeld op effectiviteit en betrouwbaarheid.



Medewerkers hebben recht op:

- Informatie over het gebruik van profilering;
- Uitleg over de werking van geautomatiseerde verwerkingen;
- Menselijke tussenkomst bij besluiten die (deels) op profilering zijn gebaseerd;
- Correctie van onjuiste gegevens of conclusies;
- Bezwaar tegen het gebruik van profilering, tenzij dit noodzakelijk is voor de uitvoering van de arbeidsovereenkomst of op basis van wetgeving.

Voor vragen of het uitoefenen van uw rechten kunt u contact opnemen met de Functionaris Gegevensbescherming te vinden in onze privacyverklaring.

10.10 Procedure bij verzoeken

Het indienen en afhandelen van verzoeken verloopt volgens de Procedure Rechten van Betrokkenen.

Voor de uitoefening van de rechten, zoals genoemd in dit hoofdstuk, stuurt de medewerker een schriftelijk verzoek aan **de directeur** van de school. Deze neemt een besluit over het verzoek van de medewerker.

De medewerker wordt zo spoedig mogelijk, maar uiterlijk binnen één maand na ontvangst van het verzoek geïnformeerd over de uitkomst. Indien het verzoek complex is of er meerdere verzoeken zijn ingediend, kan deze termijn worden verlengd met maximaal twee maanden. De medewerker wordt hierover tijdig geïnformeerd.

Indien een medewerker van mening is dat sprake is van een ernstige schending van zijn of haar privacy of van de rechten zoals genoemd in dit privacyreglement, kan hiervan melding worden gedaan bij de functionaris gegevensbescherming.

De medewerker kan zich met vragen of klachten over de verwerking van persoonsgegevens altijd wenden tot:

- **De directeur van de school;**
- **De IBP manager van OPOO;**
- De functionaris gegevensbescherming van OPOO;
- De Autoriteit Persoonsgegevens.