



# PRIVACY HANDBOEK

GEWOON SPECIAAL  
ONDERWIJS

Vastgesteld op:

20 december 2021



Dit privacy handboek is met zorg samengesteld en zal jaarlijks worden herzien. Mochten er vragen of opmerkingen zijn over de inhoud van deze uitgave, of heb je suggesties voor toevoegingen/aanpassingen kun je contact opnemen met de Privacy Officer via:  
[privacy@gewoonspeciaal.com](mailto:privacy@gewoonspeciaal.com).



Arnelieke de Bondt  
Jurist | Consultant  
Functionaris Gegevensbescherming  
Datum: 28 januari 2022

## Privacy handboek

Informatie en ICT zijn noodzakelijk in de ondersteuning van het onderwijs. Omdat we met persoonsgegevens (van leerlingen, ouders, medewerkers en soms van derden) werken, is privacywetgeving daarop van toepassing. Deze wetgeving bepaalt niet alleen onder welke voorwaarden persoonsgegevens gebruikt mogen worden, maar geeft ook aan dat er passende technische en organisatorische maatregelen op het gebied van informatiebeveiliging en privacy (afgekort: IBP) genomen moeten worden om de persoonsgegevens te beschermen.

Dit handboek is bedoeld als informatiebron voor alle medewerkers van Stichting Gewoon Speciaal Onderwijs. Hierin staan de afspraken die we met elkaar gemaakt hebben over informatiebeveiliging en privacy. Niet alleen vanuit de wetgeving, maar ook op basis van de normen en waarden die wij vanuit onze visie op onderwijs met elkaar delen en uitdragen:

*Binnen Stichting Gewoon Speciaal Onderwijs willen we kinderen met extra en/of specifieke onderwijs- en/of ondersteuningsbehoefte de kans geven om hun talenten te ontwikkelen. We werken samen met ouders en professionals aan de ontwikkeling van het kind en er is maximale afstemming met de jeugdhulpverlening. Daarmee dragen wij allen bij aan een gezonde maatschappij, waarin mensen zelfbewust, vanuit vertrouwen in eigen kunnen, handelen als burger.*

Om deze doelstelling waar te maken is het van belang goed te weten wie deze leerling is, wat zijn of haar talenten en uitdagingen zijn en hoe het onderwijs voor deze leerling het beste kan worden verzorgd. Om hier een beeld van te krijgen worden persoonlijke gegevens van die leerling op school verzameld en bewaard. Ook heeft de stichting hierin een wettelijke plicht. De Stichting Gewoon Speciaal gaat zorgvuldig met deze gegevens om en heeft dit handboek opgesteld om regels en afspraken over het gebruik van persoonsgegevens vast te leggen.

Het privacy handboek is een document waarin nauwkeurig en op een begrijpelijke manier beschreven is hoe de Stichting Gewoon Speciaal Onderwijs met persoonsgegevens omgaat. Ook bevat het handboek diverse protocollen en templates om gegevensverwerking goed te organiseren en coördineren. Dit handboek wordt binnen de organisatie gebruikt om medewerkers en andere betrokkenen te informeren over het privacybeleid van de Stichting. Een korte samenvatting van het privacybeleid is vastgelegd in de privacyverklaring. Deze verklaring is gepubliceerd op de website van de stichting en de betrokken scholen.

## Inhoudsopgave

Privacy handboek.....	2
Inhoudsopgave.....	3
Privacyverklaring.....	4
Algemeen.....	7
Toegangsbeleid.....	8
Documentmanagement.....	12
Taken en verantwoordelijkheden.....	13
Controle en toezicht.....	15
Verwerking leerlinggegevens.....	16
Verwerking personeelsgegevens.....	19
Verwerking gegevens externe (medewerkers).....	22
Verwerking van gegevens over derden.....	24
Verwerkersovereenkomsten.....	25
Toestemming voor foto's, video's en online diensten.....	26
Geheimhoudingsverklaring.....	27
Gedragcode.....	28
Protocol Datalekken.....	33
Reglement cameratoezicht.....	34
Archivering: bewaartermijnen.....	36
Checklist in- en uitdiensttreding.....	43
BIJLAGEN.....	45
Bijlage A: Overzicht verwerkers.....	46
Bijlage B: Toestemmingsformulier gebruik beeldmateriaal.....	51
Bijlage C: Gebruikersovereenkomst (mobiele) devices.....	53
Afspraken computergebruik leerlingen PO.....	56
Afspraken gebruik ICT VSO.....	57



## fPrivacyverklaring

Deze privacyverklaring is van toepassing op de verwerking van persoonsgegevens door de Stichting Gewoon Speciaal Onderwijs en de daaronder ressorterende scholen. Om goed onderwijs te kunnen bieden is het noodzakelijk dat bepaalde persoonsgegevens worden verwerkt. Deze gegevens verwerkt de stichting met name voor het uitvoeren van een wettelijke verplichting. Gegevens die niet noodzakelijk zijn voor het onderwijs of het volgen van de wet, verwerken we alleen met uw toestemming. Op elk moment kunt u wijzigen waarvoor u wel of geen toestemming geeft.

### Welke gegevens gebruiken wij?

De Stichting Gewoon Speciaal Onderwijs beschikt over informatie van u en uw kind zoals:

- Naam
- (Email) adres
- Telefoonnummer(s)
- Nationaliteit
- Leerprestaties van uw kind
- en soms ook medische informatie als dat nodig is

Dit zijn persoonsgegevens van u en uw kind. In het privacy protocol van de stichting is nader beschreven hoe de school omgaat met persoonsgegevens. Dit reglement is met instemming van de GMR vastgesteld. U vindt het privacy protocol op de website van de school van uw kind(eren).

### Waarvoor gebruiken wij deze gegevens?

Wij verzamelen en verwerken persoonsgegevens voor het leren en begeleiden van onze leerlingen. Deze gegevens, zoals cijfers en vorderingen, worden door leerkrachten en ondersteunend personeel geregistreerd. Daarnaast hebben wij ook gegevens nodig voor de organisatie van het onderwijs. De meeste van die gegevens ontvangen wij van u als ouder of verzorger van de leerling bij de inschrijving op de school.

Het is soms noodzakelijk dat wij bijzondere persoonsgegevens registreren als dat nodig is voor de juiste begeleiding van een leerling. Het gaat daarbij meestal om medische gegevens, zoals diagnoses van dyslexie of ADHD.

### Waar slaan wij gegevens op?

De leerlinggegevens worden opgeslagen in ons (digitale) leerlingvolgsysteem (LVS). Dit programma is beveiligd en toegang tot leerlinggegevens is beperkt tot de medewerkers die direct betrokken zijn bij de begeleiding van uw kind. Deze gegevens zijn noodzakelijk voor de uitvoering van hun werkzaamheden.

Wij bewaren de gegevens niet langer dan noodzakelijk is. Hoe lang wij gegevens mogen en moeten bewaren staat in de wet als bewaartermijn. De bewaartermijn van het onderwijskundig rapport is uiterlijk 5 jaar na het verlaten van de school.

### Wat delen wij met derden?

Soms zijn wij verplicht om gegevens te delen met andere organisaties zoals de Dienst Uitvoering Onderwijs, de leerplichtambtenaar, de onderwijsinspectie, de GGD/schoolarts, het regionale samenwerkingsverband en de accountant.

Tijdens de lessen maken wij gebruik van digitale leermiddelen. Er wordt een beperkte set persoonsgegevens uitgewisseld met leveranciers om bijvoorbeeld een leerling te identificeren bij het inloggen. Wij hebben met deze leveranciers, afspraken gemaakt over de gegevens die zij voor ons verwerken. De leverancier kan de leerlinggegevens alleen gebruiken als wij daar toestemming voor geven. Een lijst van de leveranciers waar de school afspraken mee heeft gemaakt, is op te vragen bij de school.

### Wat zijn uw rechten?

De wet geeft u een aantal rechten over uw persoonsgegevens. Ouders en leerlingen kunnen op elk moment gebruik maken van deze rechten.

- Recht op inzage

Dit betekent dat u altijd kunt vragen om de gegevens die wij van u en/of uw kind hebben, te bekijken. Wij hebben dan wel tijd nodig om deze gegevens voor u zichtbaar te maken.

- Recht op rectificatie en aanvulling en recht op beperking van de verwerking:

Daarnaast heeft u het recht te vragen om gegevens te verbeteren, te beperken of helemaal te wissen uit de systemen van de school. Wij zorgen dan dat deze gegevens overal worden aangepast. Als ouders ons vragen om gegevens te beperken of te wissen, kijkt de school eerst of dit kan. Wij moeten ons wel aan de wet houden. Soms schrijft de wet ons voor bepaalde informatie te bewaren.

- Recht op dataportabiliteit:

U kunt ook vragen om gegevens, over te dragen aan u of aan een organisatie.

- Recht op een menselijke blik bij besluiten

De Stichting Gewoon Speciaal Onderwijs neemt geen besluiten die alleen gebaseerd zijn op geautomatiseerde verwerking van gegevens over uw kind. Beslissingen worden nooit genomen zonder dat er een mens naar kijkt. Dit kan bijvoorbeeld de leerkracht, Intern begeleider of zorg coördinator zijn.

- Het recht om bezwaar te maken tegen de gegevensverwerking:

Als u vindt dat de school niet goed omgaat met uw informatie, dan kunt u dit bespreken met de directeur of locatieleider van de school. Komt u er niet uit, dan kunt u een bericht sturen naar de Privacy Officer van Stichting Gewoon Speciaal Onderwijs, via [privacy@gewoonspeciaal.com](mailto:privacy@gewoonspeciaal.com). Als u daarna nog vragen heeft, kunt u terecht bij onze Functionaris voor Gegevensbescherming: Mevr. A. de Bondt ([a.debondt@goc-consultants.nl](mailto:a.debondt@goc-consultants.nl)).

### Klachten

Wanneer uw vraag of probleem niet goed wordt opgelost, kunt u dat melden bij [Autoriteit Persoonsgegevens](#).

### Cookies

Als u op de website van Stichting Gewoon Speciaal Onderwijs of de school kijkt, laat Google Analytics cookies achter. We kunnen nooit zien wie bepaalde informatie heeft bekeken. We gebruiken de cookies om statistieken te kunnen zien. De website en het Analytics account zijn echter volledig ingesteld op geanonimiseerd gebruik. Dat betekent dat het bezoek op geen enkele manier kan worden herleid tot u of uw computer.



## Contactgegevens

### Contactgegevens Stichting:

Stichting Gewoon Speciaal Onderwijs

Handboog 4

3994 AD Houten

T: 030-636 1530

E: [info@gsonderwijs.nl](mailto:info@gsonderwijs.nl)

### Contactgegevens Functionaris Gegevensbescherming (extern):

Arnelieke de Bondt

GOC Consultants

[a.debondt@goc-consultants.nl](mailto:a.debondt@goc-consultants.nl)

## Algemeen

Privacy binnen de schoolorganisatie gaat over de bescherming van gegevens over leerlingen, hun ouders en medewerkers. Dit wordt geregeld in de Algemene Verordening Gegevensbescherming (AVG). In deze 5 vuistregels worden de belangrijkste uitgangspunten voor het verantwoord omgaan met persoonsgegevens samengevat (bron: [Kennisset](#)).

Binnen Stichting Gewoon Speciaal Onderwijs spreken we met elkaar af dat we altijd checken of we aan deze vuistregels voldoen bij het verzamelen en verstrekken van persoonsgegevens.

### 5 Vuistregels

#### 1. Doel en doelbinding

Heb ik vooraf een doel voor de verwerking van persoonsgegevens vastgesteld?  
Worden de persoonsgegevens alleen gebruikt voor dat doel dat ik vooraf heb vastgelegd?

#### 2. Grondslag

Is er minimaal een wettelijke grondslag voor de verwerking? Zoals:

- Als er een wettelijke plicht bestaat om deze gegevens te verstrekken. Bijv. voor bekostiging, inspectie, overdrachtdossier, etc.;
- Als er toestemming is van de ouders/verzorgers. Bijv. voor de begeleiding van een leerling door externe onderwijspecialisten, foto's op website, etc.;
- Als de partij een publiekrechtelijke taak heeft. Bijv. de uitwisseling van informatie bij de overstap van PO naar VO;
- Als dit nodig is voor het uitvoeren van een overeenkomst met de ouders/verzorgers. Bijv. voor de TSO van kinderen;
- Als er sprake is van een gerechtvaardigd belang, zoals het gebruik van een pasfoto voor identificatie in het leerlingvolgsysteem.

#### 3. Dataminimalisatie

Gebruik ik alleen die gegevens die noodzakelijk zijn om het vastgestelde doel te verwezenlijken? Kan ik met minder of bijvoorbeeld anonieme gegevens werken?  
Bewaar ik de gegevens niet langer dan nodig?

#### 4. Transparantie

Heb ik de leerling of zijn ouders vooraf helder geïnformeerd over het doel van de gegevensverwerking? Heb ik uitgelegd welke gegevens worden gebruikt en met wie deze worden gedeeld?

#### 5. Data-integriteit

Kloppen de persoonsgegevens die ik gebruik nog steeds? Zijn de gegevens op het juiste moment, op de juiste plaats en voor de juiste mensen beschikbaar? Heb ik onjuiste gegevens gecorrigeerd of verwijderd?





## Toegangsbeleid

Een overzicht van toegangsrechten is zichtbaar in de Excel autorisatiematrix.

Niet alle medewerkers hebben toegang nodig tot leerlinggegevens. De Autoriteit Persoonsgegevens heeft aangegeven dat toegang toegestaan is wanneer dit noodzakelijk is voor het uitvoeren van de werkzaamheden. Per rol is vastgesteld welke gegevens kunnen worden ingezien en gewijzigd, waarbij is gekeken wat die rol nodig heeft aan gegevens om zijn of haar werkzaamheden uit te kunnen voeren. Gegevens die daarbij niet noodzakelijk zijn, kan die rol ook niet inzien. Daar waar medewerkers groepsdoorbrekend werken, danwel een taak hebben die meerdere stamgroepen betreft is de toegang tot de leerlingdossiers breder ingeregeld dan enkel de eigen stamgroep. Dit is noodzakelijk voor de beschikbaarheid van de noodzakelijke gegevens voor de begeleiding van de leerling.

De directeur van de school is verantwoordelijk voor het verstrekken van de juiste toegang (lees: accounts met de juiste rollen en rechten). De directeur ziet er ook op toe dat de accounts worden ingetrokken na het beëindigen van een arbeids- of samenwerkingscontract of het wijzigen van functies. Daarnaast worden de accounts van systemen met persoonsgegevens periodiek gecontroleerd.

Gegevens van leerlingen met betrekking tot administratie, inschrijving, onderwijsbegeleiding en zorg worden in het leerlingvolgsysteem opgeslagen. De afspraken met betrekking tot de toegang tot en het verwerken van leerlinggegevens in het leerlingvolgsysteem zijn hieronder beschreven. Dit beleid wordt jaarlijks gecontroleerd.

- Inloggegevens van het leerlingvolgsysteem worden via het e-mailadres van de organisatie verstrekt aan de medewerker en nooit gedeeld met anderen.
- Inloggegevens worden jaarlijks vernieuwd. De gebruiker ontvangt een geautomatiseerd bericht met het verzoek om het wachtwoord te veranderen.
- Inloggegevens worden nooit gedeeld met anderen en worden nooit opgeschreven.
- Computers waar het leerlingvolgsysteem in de internetbrowser is geopend, worden niet onbeheerd achtergelaten.
- De optie “automatisch wachtwoord onthouden” in de internetbrowser wordt niet aangezet voor het leerlingvolgsysteem.

Inloggen tot het leerlingvolgsysteem is alleen voorbehouden aan medewerkers die in dienst zijn van Stichting Gewoon Speciaal Onderwijs en externe zorgbegeleiders. Met de leverancier van het leerlingvolgsysteem is een zogenaamde verwerkersovereenkomst afgesloten, waarin ook afspraken zijn gemaakt over beveiliging en back-up van de data die in het leerlingvolgsysteem wordt opgeslagen.

De uitwisseling met de overheid en andere scholen gebeurt ook door middel van het leerlingvolgsysteem. Dit systeem voldoet aan de Europese standaarden op het gebied van beveiliging die de overheid heeft bepaald.

### Uitzondering op smalle inregeling van toegangsbeleid

In uitzondering op voorgaand gestelde smalle inregeling van het systeem wordt er bij SBO De Kristal gewerkt met een bredere toegang tot de leerlinggegevens. De werkwijze van deze school laat het niet toe om toegang per klas te beperken. Deze brede toegang is van



toepassing op de autorisaties van het Leerlingvolgsysteem (ParnasSys) en van de dossiers die aanwezig zijn in de Cloud.

De directeur van de school draagt zorg dat de logging van deze twee systemen periodiek worden gecontroleerd om uit te kunnen sluiten dat van deze brede toegang misbruik wordt gemaakt. Deze periodieke controle wordt intern geregistreerd.

Tabel A: Toegangsrechten in ParnasSys voor medewerkers van stichting Gewoon Speciaal Onderwijs<sup>1</sup>

Funcities/rollen	Rol in ParnasSys	Werkzaamheden	Niveau van toegang <sup>1</sup> :
<b>Bovenschools</b>			
Bestuurder	Monitororganisatie beheerder	Sturing en beleid	Stichting
Directie(raad)	Monitororganisatie beheerder	Sturing en beleid	Stichting
<b>School</b>			
Leerkrachten	Leerkracht	Verzorgen onderwijs	School
Invalleerkracht	Leerkracht beperkt	Verzorgen onderwijs	Groep
Lio-stagiaire	Leerkracht beperkt	Verzorgen onderwijs	Groep
Directeur	Applicatiebeheerder	Sturing en beleid	School
Intern begeleider	Intern begeleider	Leerlingzorg	School
Orthopedagoog	Intern begeleider	Leerlingzorg	School
School- maatschappelijk- werker	Intern begeleider	Leerlingzorg	School
Logopedist	Intern begeleider	Leerlingzorg	School
Administratief medewerker	Administratie / leerkracht <sup>2</sup>	Administratietaken	School
<b>Extra rollen op schoolniveau</b>			
Beheerder ParnasSys <sup>3</sup>	Applicatiebeheerder	Beheer	School

<sup>1</sup> De volgende toegangsniveaus worden onderscheiden:

- Alle leerlingen in een specifieke **(sub)groep** of **meerdere (sub)groepen**
- Alle leerlingen per **school**

Behoudens de gegeven uitzondering wordt alleen toegang verschaft tot een specifieke (sub)groep waarbij de medewerker direct is betrokken

<sup>2</sup> om de gegevens van de leerlingen op correcte wijze te kunnen invoeren, is het noodzakelijk dat administratief medewerkers de rol van leerkracht hebben.

<sup>3</sup> Deze rol kan bij Directeur, IB-er of ICT belegd worden, afhankelijk van taakbeleid van de school.

<sup>1</sup> Daar waar medewerkers groepsdoorbrekend werken, danwel een taak hebben die meerdere stamgroepen betreft is de toegang tot de leerlingdossiers breder ingeregeld dan enkel de eigen stamgroep. Dit is noodzakelijk voor de beschikbaarheid van de noodzakelijke gegevens voor de begeleiding van de leerling.

Tabel B: Toegangsrechten in Somtoday voor medewerkers van stichting Gewoon Speciaal Onderwijs

Funcities/rollen	Rol in Somtoday	Werkzaamheden	Niveau van toegang <sup>1</sup> :
<b>Bovenschools</b>			
Bestuurder	Monitororganisatie beheerder	Sturing en beleid	Stichting
Directie(raad)	Monitororganisatie beheerder	Sturing en beleid	Stichting
<b>School</b>			
Leerkrachten	Leerkracht	Verzorgen onderwijs	School
Invalleerkracht	Leerkracht beperkt	Verzorgen onderwijs	Groep
Lio-stagiaire	Leerkracht beperkt	Verzorgen onderwijs	Groep
Directeur	Applicatiebeheerder	Sturing en beleid	School
Intern begeleider	Intern begeleider	Leerlingzorg	School
Orthopedagoog	Intern begeleider	Leerlingzorg	School
School- maatschappelijk- werker	Intern begeleider	Leerlingzorg	School
Logopedist	Intern begeleider	Leerlingzorg	School
Administratief medewerker	Administratie / leerkracht <sup>2</sup>	Administratietaken	School
<b>Extra rollen op schoolniveau</b>			
Beheerder Somtoday	Applicatiebeheerder	Beheer	School

<sup>1</sup> De volgende toegangsniveaus worden onderscheiden:

- Alle leerlingen in een specifieke **(sub)groep** of **meerdere (sub)groepen**
- Alle leerlingen per **school**

Behoudens de gegeven uitzondering wordt alleen toegang verschaft tot een specifieke (sub)groep waarbij de medewerker direct is betrokken

<sup>2</sup> om de gegevens van de leerlingen op correcte wijze te kunnen invoeren, is het noodzakelijk dat administratief medewerkers de rol van leerkracht hebben.

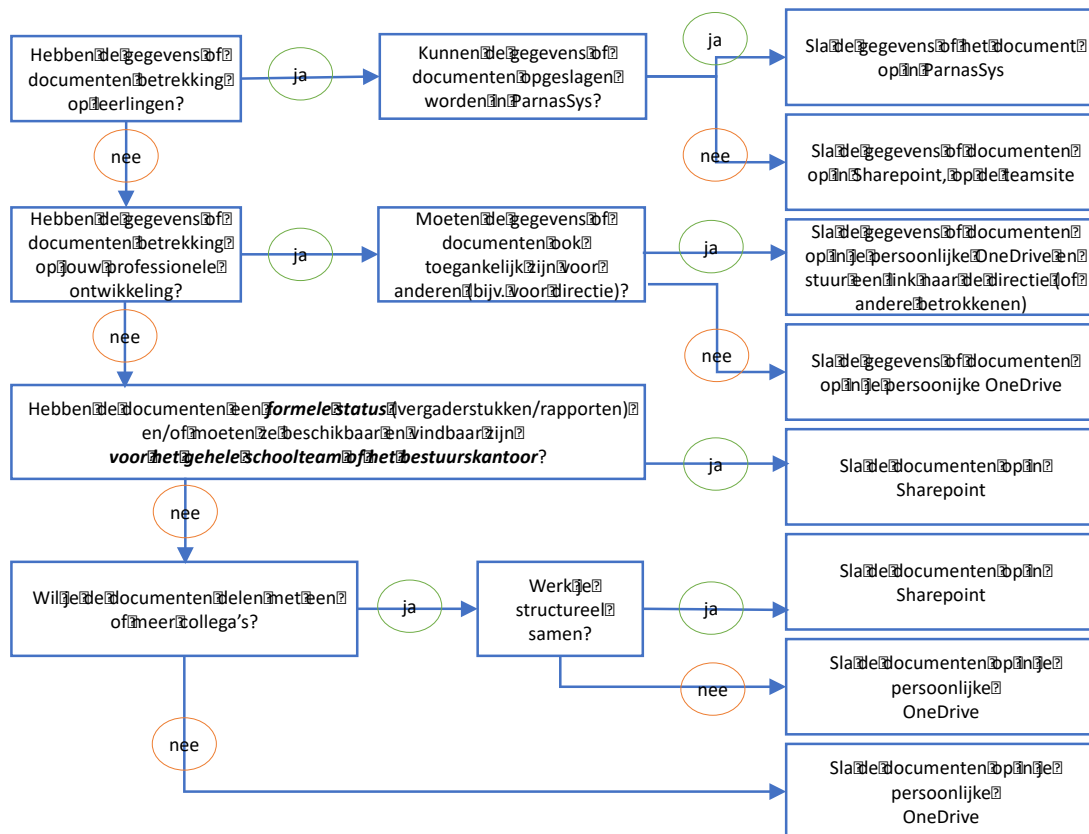
<sup>3</sup> Deze rol kan bij Directeur, IB-er of ICT belegd worden, afhankelijk van taakbeleid van de school.



## Documentmanagement

Om ervoor te zorgen dat we binnen de school onze documenten en gegevens overzichtelijk en veilig opgeslagen hebben, zijn er afspraken over wat we waar bewaren. Op deze manier zijn documenten eenvoudiger terug te vinden, maar kunnen ze ook beter afgeschermd en geback-up't worden.

In het schema hieronder kun je aan de hand van een aantal vragen bepalen op welke plek je digitale gegevens op moet slaan.



Leerlinggegevens worden zo veel mogelijk opgeslagen in het leerlingdossier in het leerlingvolgsysteem. Ouders hebben het recht om deze gegevens in te mogen zien. In uitzonderlijke gevallen kan het voorkomen dat je informatie over een leerling wil bewaren die je niet kwijt kan in het leerlingdossier. Bijvoorbeeld wanneer de betreffende informatie de leerling in gevaar kan brengen. In dat geval kan de informatie opgeslagen worden in een afgeschermd gedeelte van de Cloud omgeving. Daarnaast kan het wenselijk zijn om bijvoorbeeld groepsoverzichten met gegevens die niet afkomstig zijn uit het leerlingvolgsysteem op te slaan op de teamsite van Cloud.

## Taken en verantwoordelijkheden

Binnen het vaststellen en uitvoeren van het IBP-beleid zijn verschillende verantwoordelijkheden belegd binnen Stichting Gewoon Speciaal Onderwijs. Deze verantwoordelijkheden zijn opgenomen in onderstaande matrix.

Onderwerp	Verantwoordelijk voor	Niveau	Rol/functie
<b>Privacy reglement</b>	Vaststellen	Bovenschools	Bestuurder
	Communicatie met ouders	School	Directeur
<b>Gebruik beeldmateriaal en online diensten</b>	Toestemming	School	Directeur
<b>Gedragcode</b>	Vaststellen	Bovenschools	Bestuurder
	Bewustwording	School	Directeur
	Uitvoering	School	Medewerkers
<b>Document management</b>	Inrichten O365	Bovenschools	Bovenschools ICT-er
	Vaststellen bewaarplaatsen	School	Directie/IB
	Vaststellen bewaartermijnen	Bovenschools	Bestuurder
	Vernietiging	School	Directeur
<b>Toegangsbeleid</b>	Toegangsmatrix leerlingvolgsysteem	Bovenschools	Bovenschools ICT-er
	Toegangsmatrix Office365	Bovenschools	Bovenschools ICT-er
<b>Verwerkersovereenkomsten</b>	Contracten met meerder scholen	Bovenschools	Bestuurder
	Individuele contracten per school	School	Directeur
<b>Datalekken</b>	Protocol vaststellen	Bovenschools	Bestuurder
	Meldpunt	School	Directeur / ICT
	Melden en registreren	Bovenschools	FG/privacyfunctionaris
	Technicus	Bovenschools	Bovenschools ICT-er

<b>Devices in bruikleen</b>	Afsluiten overeenkomst	School	Directeur
-----------------------------	---------------------------	--------	-----------

### Klachten

Voor vragen rondom privacy kan men zich wenden tot [privacy@gewoonspeciaal.com](mailto:privacy@gewoonspeciaal.com). Indien men van mening is dat het privacy protocol niet op de juiste wijze wordt nageleefd binnen Stichting Gewoon Speciaal Onderwijs kan er een klacht worden ingediend bij de directeur van de school. Wanneer deze klacht voor de betrokkene niet leidt tot een acceptabele oplossing kan men zich wenden tot het College van Bestuur ([bestuur@gsonderwijs.nl](mailto:bestuur@gsonderwijs.nl)).

Het is ook mogelijk om contact op te nemen met de Autoriteit Persoonsgegevens (Bezuidenhoutseweg 30, 2594 AV Den Haag) via <https://www.autoriteitpersoonsgegevens.nl/>.

## Controle en toezicht

Jaarlijks wordt onderstaande (niet uitputtende) controlelijst ingevuld door alle scholen om na te gaan of het handboek is geïmplementeerd. De resultaten worden gerapporteerd aan de bestuurder.

Aantekeningen	Onderwerp	Toelichting
	<b>Bewustwording:</b>	Is er aandacht besteedt aan bewustwording, hoe is dit vorm gegeven? Waar kunnen zij terecht met vragen en opmerkingen? Doen zij verbetervoorstellen als er processen niet soepel verlopen?
	<b>Privacyverklaring:</b>	Is de privacyverklaring bekend bij de medewerkers? Wordt deze ook transparant gecommuniceerd met de betrokkenen (bijvoorbeeld in de schoolgids of schoolwebsite)
	<b>Verwerkingsoverzicht:</b>	Heeft de school controle op de systemen en tools die persoonsgegevens verwerken namens de school? Is er een centraal aanspreekpunt om dit te registreren?
	<b>Risicoanalyse:</b>	Als er nieuwe processen of programma's worden gebruikt moet er vóóraf een (beknopte) risicoanalyse uitgevoerd worden. Wordt dit gedaan binnen de school?
	<b>Veiligheidsmaatregelen n.a.v. risicoanalyse:</b>	Wat gebeurt er met de risico's die volgen uit de risicoanalyse? Worden er beheersmaatregelen genomen om risico's te beperken of uit te sluiten?
	<b>Delen met derden:</b>	Hoe gaan de medewerkers om met het delen van gegevens met derden (samenwerkingsverband of externe hulpverlening?).
	<b>Datalekregister:</b>	De organisatie is verplicht om alle vormen van datalekken (beveiligingsincidenten) te registreren. Deze hoeven niet altijd bij de AP gemeld te worden, maar registratie is belangrijk om eventuele maatregelen te kunnen nemen. Worden incidenten herkend en ook geregistreerd?
	<b>Opslag van gegevens:</b>	Waar worden alle gegevens opgeslagen? Als deze in de cloud staan, staat dan álles in de cloud of blijven er gegevens achter op het 'eigen device'. Denk hierbij ook aan telefoonnummers en bestanden met mailadressen.
	<b>Toestemming vragen:</b>	Hoe is de procedure omtrent het vragen van toestemming ingebed. Is dit gewaarborgd bij de inschrijving en is hier nog (periodiek) een check op? Hoe is het aanpassen van deze toestemming geregeld? Kan dit eenvoudiger (transparanter) door ouderportaal?



## Verwerking leerlinggegevens

Voor de begeleiding van de leerling tijdens zijn of haar schoolloopbaan worden gegevens verzameld om de leerling optimaal te laten functioneren, zowel wat betreft prestaties als welbevinden. Deze gegevens worden vastgelegd in een leerlingdossier.

### Verzamelen van persoonsgegevens

De gegevens die worden opgeslagen en verzameld zijn:

- Naam, voornamen, geslacht, geboortedatum, geboorteland, nationaliteit, adresgegevens en soortgelijke voor communicatie benodigde gegevens van de leerling/ouders/verzorgers;
- Administratienummer (o.a. BSN);
- Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling;
- Gegevens over de aard en het verloop van het onderwijs, alsmede de behaalde resultaten en gegevens over verlof en verzuim;
- Gegevens over de organisatie van het onderwijs, zoals welke klas, vakken en dergelijke;
- Zorggegevens die nodig zijn voor de organisatie van het onderwijs;
- Gegevens van psychosociale aard, zoals testrapporten, persoonlijkheidsonderzoeken, intelligentieonderzoeken en orthopedagogische onderzoeken;
- Ontwikkelingsperspectiefplannen van de leerling;
- Gespreksverslagen;
- Verslaglegging van het multidisciplinair overleg (MDO);
- Gegevens nodig voor het berekenen, vastleggen en innen van inschrijvingsgelden, school- en leskosten en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten;
- Loggegevens over gebruik van de systemen.

Deze gegevens worden zo veel als mogelijk digitaal opgeslagen, en indien noodzakelijk op papier.

### Doel van de gegevensverwerking

Deze persoonsgegevens worden door de school(organisatie) verzameld om:

- Overzicht te hebben van de leerlingen die onderwijs volgen;
- Overzicht te hebben van de aard, organisatie en verloop van dat onderwijs per leerling en de behaalde studieresultaten;
- Te communiceren met leerlingen en/of hun ouders/ verzorgers;
- Persoonlijke (waaronder medische) omstandigheden van een leerling ende gevolgen daarvan voor het volgen van onderwijs bij te houden;
- Financieel beheer uit te kunnen voeren;
- Aan de wettelijke eisen rond monitoring en verantwoording naar toezichthoudende instanties en zorginstellingen te kunnen voldoen;
- Toegang tot de systemen te krijgen;
- De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het bewaken van de consistentie en betrouwbaarheid van de opgeslagen gegevens te verzorgen;
- De continuïteit en goede werking van de systemen te waarborgen.

### Verstrekken gegevens aan derden

De gegevens mogen in beginsel **niet** aan derden worden doorgegeven of door anderen worden ingezien zonder toestemming van de ouders, tenzij de school verplicht is om bepaalde persoonsgegevens te verstrekken, die noodzakelijk zijn voor de uitvoering van een wettelijke

plicht. Toestemming van ouders vindt schriftelijk plaats en wordt opgeslagen in het leerlingdossier.

Bij het uitwisselen van gegevens wordt altijd gecheckt of aan de [vijf privacy-vuistregels](#) wordt voldaan:

1. Doel en doelbinding
2. Grondslag
3. Dataminimalisatie
4. Transparantie
5. Data-integriteit

De gegevens worden verstrekt aan de volgende externe partijen:

- Externe partijen die in opdracht van de school en met toestemming van de ouders ondersteunen bij het bieden van aanvullende onderwijsbegeleiding voor de leerling.
- Een andere onderwijsinstelling bij verhuizing, overplaatsing of doorstroming naar het V(S)O. Ouders hoeven geen toestemming te verlenen voor het uitwisselen van het Onderwijskundig Rapport (OKR). Zij hebben wel recht op inzage. Eventuele opmerkingen van ouders kunnen toegevoegd worden aan het dossier, maar de school is niet verplicht tot wijziging van de gegevens.
- Het Regionaal Samenwerkingsverband. Ouders hoeven geen toestemming te verlenen voor het uitwisselen van het Onderwijskundig Rapport (OKR). Zij hebben wel recht op inzage. Eventuele opmerkingen van ouders kunnen toegevoegd worden aan het dossier, maar de school is niet verplicht tot wijziging van de gegevens.
- Externe deskundigen uit het MDO (schoolmaatschappelijk werk, schoolarts/ -verpleegkundige, ambulante begeleider, orthopedagoog) op grond van toestemming door de ouders/verzorgers.
- Externe partijen die in opdracht van de school en met toestemming van de ouders ondersteunen bij het bieden van aanvullende zorg voor de leerling.
- Verwerkers in de zin van leveranciers van onderwijsmiddelen die in opdracht van de school zorgen voor toegang en beheer van de digitale systemen die bij de begeleiding en zorg voor leerlingen worden gebruikt en waarmee een verwerkersovereenkomst is afgesloten.
- De Inspectie van het Onderwijs op grond van een wettelijke verplichting inzake onderwijskwaliteit.

### Rechten van leerlingen/ouders

De wet geeft leerlingen/ouders een aantal rechten over uw persoonsgegevens. Ouders en leerlingen kunnen op elk moment gebruik maken van deze rechten.

- Recht op inzage

Dit betekent dat een leerling of ouder altijd kunt vragen om de gegevens die de Stichting heeft, te bekijken. Als een ouder de persoonsgegevens wil inzien of wijzigen, dan kan men hiervoor een afspraak maken met de directeur van de betreffende school. Ouders krijgen het dossier niet mee, maar hebben wel recht op een kopie.

- Recht op rectificatie en aanvulling en recht op beperking van de verwerking:

Daarnaast hebben leerlingen/ouders het recht te vragen om gegevens te verbeteren, te beperken of helemaal te wissen uit de systemen van de school. De organisatie draagt zorg dat deze gegevens overal worden aangepast. Als ouders ons vragen om gegevens te beperken of te wissen, kijkt de school eerst of dit kan. Wij moeten ons wel aan de wet houden. Soms schrijft de wet voor bepaalde informatie te bewaren.

- Recht op dataportabiliteit:

Leerlingen/ouders kunnen vragen om gegevens, over te dragen aan hen of aan een organisatie.

- Recht op een menselijke blik bij besluiten

De Stichting Gewoon Speciaal Onderwijs neemt geen besluiten die alleen gebaseerd zijn op geautomatiseerde verwerking van gegevens over uw kind. Beslissingen worden nooit genomen zonder dat er een mens naar kijkt. Dit kan bijvoorbeeld de leerkracht, Intern begeleider of zorg coördinator zijn.

- Het recht om bezwaar te maken tegen de gegevensverwerking:

Als u vindt dat de school niet goed omgaat met persoonsgegevens, kan dit worden besproken met de directeur of locatieleider van de school. Als men er niet uitkomt met elkaar is het mogelijk contact op te nemen met de Privacy Officer van Stichting Gewoon Speciaal Onderwijs. Als u daarna nog vragen heeft, kunt u terecht bij onze Functionaris voor Gegevensbescherming.

## Verwerking personeelsgegevens

Niet alleen van leerlingen worden persoonsgegevens verwerkt binnen Stichting Gewoon Speciaal Onderwijs, maar ook van onze medewerkers. Soms zijn dat gegevens die direct samenhangen met de arbeidsverhouding tussen Stichting Gewoon Speciaal Onderwijs en medewerkers, maar ook worden persoonsgegevens van onze medewerkers verwerkt in systemen die gebruikt worden bij het geven en begeleiden van onderwijs. De informatie over persoonsgegevens van medewerkers is ook van toepassing op stagiaires.

## Verzamelen van persoonsgegevens

De gegevens die worden verzameld en opgeslagen zijn:

- Naam, voornamen, geslacht, geboortedatum, adresgegevens en soortgelijke voor communicatie benodigde gegevens, bankrekeningnummer van de medewerker;
- Een administratienummer (o.a. BSN);
- Nationaliteit en geboorteplaats;
- Gegevens voor digitale communicatie;
- Gegevens over de groep waar een medewerker aan gekoppeld is;
- Loggegevens over het gebruik van de systemen;
- Gegevens over salaris, belasting, premies en andere vergoedingen;
- Gegevens over gevolgde en te volgen opleidingen, cursussen en stages;
- Verklaring omtrent gedrag (VOG)
- Gegevens voor personeelsbeoordeling en loopbaanbegeleiding, voor zover die gegevens bij de medewerker bekend zijn;
- Gegevens over de (voormalige) functie, alsmede over de aard, inhoud en beëindiging van het dienstverband;
- Gegevens voor de administratie van aan- en afwezigheid, in verband met verlof, arbeidsduurverkorting, bevalling of ziekte, met uitzondering van gegevens over de aard van de ziekte;
- Gegevens die in het belang van de medewerker worden opgenomen met het oog op zijn/haar arbeidsomstandigheden;
- Gegevens, waaronder begrepen gegevens over (voormalige) gezinsleden van de medewerker, die noodzakelijk zijn voor een overeengekomen arbeidsvoorwaarde;

## Doel van de gegevens

Deze gegevens worden verzameld om:

- Onderwijs te geven en leerlingen te begeleiden
  - Opslag van leer- en toetsresultaten;
  - Het terugontvangen van leer- en toetsresultaten om te verwerken in het leerlingvolgsysteem;
  - De beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen aanbieden dat is afgestemd op de specifieke leerbehoefte van een leerling;
  - Analyse en interpretatie van leerresultaten;



- Het kunnen uitwisselen van leer- en toetsresultaten tussen digitale onderwijsmiddelen;
- Gebruik te maken van specifiek docenteninformatie in de digitale onderwijsmiddelen;
- (Digitale) onderwijsmiddelen door leveranciers geleverd te krijgen en in gebruik te nemen;
- Het geven van leiding aan de werkzaamheden van de medewerker;
- De behandeling van personeelszaken;
- Het berekenen, vastleggen en betalen van salarissen, vergoedingen en andere geldsommen en beloningen in natura;
- Het berekenen, vastleggen en betalen van belasting en premies;
- De uitvoering van een voor de medewerker geldende arbeidsvoorwaarde;
- Opleidingen en scholing van de medewerker;
- Bedrijfsmedische zorg en bedrijfsmaatschappelijk werk voor de medewerker;
- Het opstellen van een lijst van data van verjaardagen en andere feestelijkheden en gebeurtenissen;
- De interne controle en de bedrijfsvoering;
- Het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen;
- Het behandelen van geschillen;
- Het doen uitoefenen van accountantscontrole;
- Het verlenen van ontslag;
- Het regelen van aanspraken op uitkeringen in verband met de beëindiging van een dienstverband;
- De uitvoering of toepassing van een andere wet;
- Toegang tot de systemen te krijgen;
- De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het bewaken van de consistentie en betrouwbaarheid van de opgeslagen gegevens te verzorgen;
- De continuïteit en goede werking van de systemen te waarborgen.

### Verstrekken aan derden

De gegevens worden verstrekt aan de volgende externe partijen:

- Verwerkers in de zin van personeelsadministratie voor het berekenen, vastleggen en betalen van salarissen, vergoedingen en andere geldsommen;

### Verwerken personeelsgegevens

- Voor de organisatie van het onderwijs en begeleiding van leerlingen wordt gebruikt gemaakt van digitale systemen, waarin gegevens over hun prestaties en welbevinden worden vastgelegd. In deze systemen worden ook gegevens van onderwijzend personeel vastgelegd, gericht op het kunnen maken van een koppeling tussen leerling en leerkracht en om de opgeslagen gegevens van de leerlingen in te kunnen zien, aan te vullen en te wijzigen.
- Voor het verzorgen van het onderwijs wordt, naast boeken, ook gebruik gemaakt van digitale onderwijsmiddelen. In deze onderwijsmiddelen, die worden afgenomen van externe leveranciers, worden persoonsgegevens verwerkt die nodig zijn voor de toegang tot en het gebruik van deze digitale producten en diensten. Voorbeelden van deze digitale onderwijsmiddelen zijn, digitale (aanvullingen op) lesmethodes, toetssystemen en apps. Ook in deze systemen worden persoonsgegevens van onderwijzend personeel opgeslagen.
- Ook worden onderwijs-ondersteunende ICT-middelen, zoals iPads of andere computer-systemen ingezet. Voor systeembeheer, beveiliging, logging en monitoring wordt software op deze middelen geïnstalleerd die persoonsgegevens verzamelen.

- Verwerkers in de zin van leveranciers van onderwijsmiddelen en of die in opdracht van de school deze middelen ter beschikking stellen;
- Verwerkers die zorgen voor toegang tot de onderwijsmiddelen in opdracht van de school;
- Verwerkers in de zin van leveranciers van onderwijsmiddelen die in opdracht van de school zorgen voor toegang en beheer van de digitale systemen die worden gebruikt bij de begeleiding en zorg voor leerlingen.

### Rechten van medewerkers

Alle medewerkers van Stichting Gewoon Speciaal Onderwijs hebben een eigen inlog voor het digitale personeelsdossier. Wanneer men vragen heeft over de persoonsgegevens of deze wil wijzigen dan kan men terecht bij het Administratiekantoor Groenendijk Onderwijsadministratie van Stichting Gewoon Speciaal Onderwijs, te bereiken via telefoonnummer: 0184 – 412 507.

- **Recht op inzage**

Dit betekent dat een medewerker mag vragen om de gegevens die de Stichting heeft, te bekijken. Als een medewerker de persoonsgegevens wil inzien of wijzigen, dan kan hij hiervoor een afspraak maken met de directeur van de betreffende school.

- **Recht op rectificatie en aanvulling en recht op beperking van de verwerking:**

Medewerkers hebben het recht om gegevens te verbeteren, te beperken of helemaal te wissen uit de systemen van de organisatie. De organisatie draagt zorg dat deze gegevens overal worden aangepast. Als medewerkers vragen om gegevens te beperken of te wissen, kijkt de organisatie eerst of dit kan. Soms schrijft de wet voor bepaalde informatie te bewaren.

- **Recht op dataportabiliteit:**

Medewerkers kunnen vragen om gegevens, over te dragen aan hen of aan een organisatie.

- **Recht op een menselijke blik bij besluiten**

De Stichting Gewoon Speciaal Onderwijs neemt geen besluiten die alleen gebaseerd zijn op geautomatiseerde verwerking van gegevens. Beslissingen worden nooit genomen zonder dat er een mens naar kijkt.

- **Het recht om bezwaar te maken tegen de gegevensverwerking:**

Als u vindt dat de organisatie niet goed omgaat met persoonsgegevens, kan dit worden besproken met de directeur of locatieleider van de school. Als men er niet uitkomt met elkaar is het mogelijk contact op te nemen met de Privacy Officer van Stichting Gewoon Speciaal Onderwijs. Als u daarna nog vragen heeft, kunt u terecht bij onze Functionaris voor Gegevensbescherming.

## Verwerking gegevens externe (medewerkers)

Soms wordt gebruik gemaakt van extern personeel, om kennis aan te vullen of om opgevallen plekken tijdelijk op te vullen. Om de contracten en inzet af te handelen, worden gegevens in diverse systemen opgeslagen

### Verzamelen van persoonsgegevens

De gegevens die worden verzameld en opgeslagen zijn:

- Naam, voornamen, geslacht, geboortedatum, adresgegevens en soortgelijke voor communicatie bedoelde gegevens;
- Bedrijfsgegevens en bankrekeningnummer van de extern ingehuurde medewerker;
- Verstrekte Verklaring Omtrent Gedrag (VOG);
- De gegevens voor de organisatie en begeleiding van onderwijs zoals vermeld bij de verwerking van personeelsgegevens.

### Doel van de gegevens

Deze gegevens worden verzameld om:

- De contractuele en financiële verplichtingen af te handelen die samenhangen met de inhuur;
- De ingehuurde in staat te stellen de ICT-middelen en software in te zetten die nodig zijn bij de uitvoer van de werkzaamheden;
- De correcte uitvoering van een wettelijke verplichting die samenhangt met de inhuur.

### Verstrekken aan derden

Binnen de school hebben de volgende type medewerkers toegang tot de gegevens:

- Medewerkers salarisadministratie en financiën;
- Personeelsadviseurs;
- Opdrachtgever van de betreffende externe medewerker;
- Hoofd P&O, bedrijfsvoering en financiën;
- ICT-ondersteunend personeel.

Deze gegevens worden verstrekt aan uitzendbureaus en detachingsbureaus waarmee door Stichting Gewoon Speciaal Onderwijs wordt samengewerkt.

### Bewaartermijn

De persoonsgegevens worden verwijderd zo snel mogelijk na beëindiging van de contractperiode, maar maximaal na 2 jaar, tenzij een wettelijke bepaling anders voorschrijft. De gegevens worden opgeslagen in het leerlingvolgsysteem.

Wanneer men de persoonsgegevens wil inzien of wijzigen, dan kan men hiervoor terecht bij de afdeling administratie van Stichting Gewoon Speciaal Onderwijs, te bereiken via telefoonnummer: 0184 412507.

### Vrijwilligers

Vrijwilligers, met name ouders van (oud)leerlingen, worden op de verschillende scholen ingezet om te helpen bij schoolactiviteiten zoals sportdagen en excursies. Van de vrijwilligers worden alleen gegevens verzameld en opgeslagen die nodig zijn om contact met hen te onderhouden. Het betreft naam, adres, telefoonnummer en/of e-mailadres. Voor inzage en wijziging kan de betreffende vrijwilliger terecht bij de administratie van de school waar hij of zij vrijwilligerswerk verricht.

## Oud-leerlingen

Voor het onderhouden van contacten met en het verzenden van informatie aan oud-leerlingen worden (evt. na toestemming) de volgende gegevens opgeslagen:

- Naam, voornamen, geslacht, geboortedatum, adresgegevens en soortgelijke voor communicatie bedoelde gegevens;
- Gegevens betreffende de schoolloopbaan van de oud-leerling.

## Verwerking van gegevens over derden

In sommige gevallen worden gegevens van derden opgeslagen, die geen leerling, ouder of medewerker zijn. Denk bijvoorbeeld aan sollicitanten, stagiaires, LIO-ers en extern ingehuurd personeel.

### Verzamelen van persoonsgegevens

De gegevens die worden verzameld en opgeslagen zijn:

- Naam, voornamen, geslacht, geboortedatum, adresgegevens en soortgelijke voor communicatie benodigde gegevens, bankrekeningnummer van de medewerker;
- Een administratienummer (o.a. BSN);
- Nationaliteit en geboorteplaats;
- Gegevens over gevolgd en te volgen opleidingen, cursussen en stages;
- Gegevens over de functie waarnaar gesolliciteerd is;
- Gegevens over de aard, inhoud van huidige en vorige dienstverbanden en beëindiging van vorige dienstverbanden;
- Andere gegevens met het oog op het vervullen van de functie, die door de sollicitant zijn verstrekt of die hem of haar bekend zijn (testen, assessments, etc.);
- Andere dan de hierboven genoemde gegevens waarvan de verwerking wordt vereist vanwege de toepassing van een andere wet.

### Doel van de gegevens

Deze gegevens worden verzameld om:

- De geschiktheid van een sollicitant te beoordelen voor een functie die vacant is of kan komen;
- De veiligheid binnen de organisatie te borgen;
- De door de sollicitant gemaakt onkosten af te handelen;
- De uitvoering of toepassing van een andere wet te borgen.

### Verstrekken aan derden

Binnen Stichting Gewoon Speciaal Onderwijs hebben alleen medewerkers die betrokken zijn bij de sollicitatieprocedure toegang tot de persoonsgegevens van de sollicitanten.

De gegevens worden alleen verstrekt aan externe partijen die namens Stichting Gewoon Speciaal Onderwijs een test of assessment verzorgen. In dat geval worden aan de direct bij de activiteiten betrokken personen slechts die persoonsgegevens verstrekt die noodzakelijk zijn voor de test of assessment.

### Bewaartermijn

De persoonsgegevens worden verwijderd op een daartoe strekkend verzoek van de sollicitant en in ieder geval uiterlijk vier weken nadat de sollicitatieprocedure is beëindigd, tenzij de persoonsgegevens met toestemming van de sollicitant langer worden bewaard.





## Verwerkersovereenkomsten

In de nieuwe privacywet is bepaald dat de school afspraken moet maken met alle leveranciers van de school die leerling gegevens verwerken in zogenaamde Verwerkersovereenkomsten. Het gaat bijvoorbeeld om uitgevers van digitaal lesmateriaal, leveranciers van toetsen, etc.

Het belangrijkste hierbij is dat scholen, als verwerkingsverantwoordelijke, de regie hebben en houden over wat er gebeurt met de persoonsgegevens. Dit mag een organisatie niet overlaten aan de leverancier (verwerker). De school beslist wat de leverancier wél en niet met de gegevens mag doen.

De verwerkersovereenkomsten worden waar mogelijk bovenschools afgesloten. Hiervoor is een inventarisatie gedaan van de lopende contracten van de scholen binnen Stichting Gewoon Speciaal Onderwijs. Wanneer een school een contract afsluit met een nieuwe leverancier zal er een nieuwe verwerkersovereenkomst gesloten moeten worden en vastgelegd in het dataregister. De school is verplicht om nieuwe contracten door te geven aan het bestuur en de privacy officer.

Voor het afsluiten van verwerkersovereenkomsten met dienstverleners voor onderwijsmateriaal wordt gebruik gemaakt van de meest actuele model verwerkersovereenkomst, die te vinden is via <https://www.privacyconvenant.nl>. Voor verwerkersovereenkomsten bij overige diensten aan de onderwijsorganisatie worden passende overeenkomsten opgesteld en afgesloten.

## Software

- Bij het gebruik van online software, app's en digitaal lesmateriaal, wordt gekeken of er persoonsgegevens bij verwerkt worden;
- Een verwerkersovereenkomst wordt afgesloten met elke leverancier van (online)software, die in opdracht van de organisatie persoonsgegevens verwerkt;

## Samenwerkingsverbanden

Een uitzondering hierop is de uitwisseling van gegevens met het samenwerkingsverband in het kader van passend onderwijs. Het samenwerkingsverband is een zelfstandige organisatie die zelf verantwoordelijk is voor de gegevens van leerlingen. De Wet op Passend Onderwijs regelt dat een school gegevens uitwisselt met het samenwerkingsverband. Hiervoor hoeft daarom geen verwerkersovereenkomst afgesloten te worden. Het blijft natuurlijk wel belangrijk om de gegevens op de juiste manier uit te wisselen.

In [bijlage A](#) is een overzicht te vinden van de leveranciers van digitale onderwijsmiddelen, waar de school op dit moment een verwerkersovereenkomst mee heeft en welke gegevens per leverancier worden verwerkt.



## Toestemming voor foto's, video's en online diensten

In de nieuwe privacywetgeving zijn de regels rondom het publiceren van beeldmateriaal van leerlingen aangescherpt. Ouders, leerlingen ouder dan 16 jaar maar ook medewerkers, moeten altijd toestemming geven voor het gebruik van beeldmateriaal en die toestemming moet specifiek zijn. Dat betekent dat het voor ouders en medewerkers duidelijk is voor welk gebruik van het beeldmateriaal ze toestemming geven, bijvoorbeeld voor het gebruik in de website, een nieuwsbrief of de schoolgids. Ouders en medewerkers moeten ook de mogelijkheid hebben deze toestemming weer in te trekken.

In beginsel is de school niet verantwoordelijk voor foto's die ouders maken en op een persoonlijk Social Media platform plaatsen. Zo ver gaat de verantwoordelijkheid van school namelijk niet. Dat betekent niet dat de school het daardoor zomaar 'goed kan vinden'. Er ontstaat een soort 'gedoogconstructie'. Het is daarom goed om aan ouders te vragen om zéér terughoudend te zijn met het publiceren van foto's van andere kinderen en bij voorkeur alleen foto's te maken van eigen kind(eren). Het maakt daarvoor niet uit of een ouder foto's maakt bij het schoolplein bij de aankomst van Sinterklaas of 3 dagen mee gaat met het schoolkamp van groep 8.

Voor het gebruik van online diensten door leerlingen binnen de school moeten ouders ook toestemming verlenen. Dit betekent dat wanneer leerlingen in de klas gebruik willen maken van een eigen (privé) account (bijvoorbeeld Whatsapp of Pinterest), ouders hier vooraf toestemming voor moeten geven. Het uitgangspunt is dat toestemming van de ouders voor elk persoonlijk account vereist is wat niet automatisch eindigt bij het verlaten van de school.

In de koppeling op deze pagina is het toestemmingsformulier opgenomen dat door alle scholen van Stichting Gewoon Speciaal Onderwijs gebruikt wordt voor het vragen van toestemming. Hierop geven ouders aan of zij toestemming geven voor het gebruik van beeldmateriaal en de online diensten. Ouders worden er jaarlijks aan herinnerd dat deze toestemming verlengd wordt tenzij de toestemming door ouders wordt gewijzigd. Dit informeren kan door middel van de schoolgids of een nieuwsbrief.

Bij gebruikmaking van beeldmateriaal van medewerkers is eveneens een toestemming benodigd. Wanneer niet alleen de naam maar ook foto's van directie, decaan, mentoren en/of leerkrachten op de website van de school worden geplaatst gelden er andere regels dan bij leerlingen. Met het publiceren van foto's van medewerkers worden leerlingen en ouders geïnformeerd wie er op school werkt. Zo is contact met medewerkers persoonlijker en leerlingen kunnen hun leraar sneller herkennen. Medewerkers worden wel geïnformeerd voor publicatie van foto's. Zij worden op die manier in de gelegenheid gesteld om eventueel – onderbouwd – bezwaar maken tegen de publicatie.



## Geheimhoudingsverklaring

Medewerkers beschikken uit hoofde van hun functie over informatie over leerlingen die niet bedoeld is voor derden. De school (het bevoegd gezag) wil voorkomen dat deze informatie zomaar op straat komt te liggen. Daarom wordt in een arbeidsovereenkomst vaak een geheimhoudingsverklaring opgenomen waarin de werknemer tot geheimhouding verplicht wordt.

Maar ook vrijwilligers, externe medewerkers, ouders of anderen betrokken bij de school krijgen vaak informatie te zien waarvan het niet de bedoeling is dat dit openlijk wordt gedeeld. Zij hebben geen arbeidsovereenkomst die geheimhouding kan bedingen en daarom is er voor Gewoon Speciaal Onderwijs een geheimhoudingsverklaring opgesteld. Deze kan gebruikt worden om de integriteit van deze vrijwilligers, externe medewerkers, ouders of andere betrokkenen te waarborgen.

In de koppeling op deze pagina is een template voor deze geheimhoudingsverklaring opgenomen.



## Gedragcode

Het gebruik van internet, netwerk, Cloud-omgeving en e-mail is voor alle medewerkers noodzakelijk om hun werkzaamheden goed te kunnen verrichten. Bij deze werkzaamheden wordt gebruik gemaakt van de (ICT)faciliteiten van de organisatie.

### Bijvoorbeeld

- Hardware: pc, laptop, tablet, telefoon;
- Software (of -systemen): alle applicaties voor het uitvoeren van de werkzaamheden;
- Informatie en (persoons)gegevens: rapportages, dossiers, gegevens in e-mails;
- Internetgebruik.

Aan het gebruik hiervan zijn risico's verbonden, waardoor het noodzakelijk is om hierover afspraken te maken. Van medewerkers wordt verwacht dat zij verantwoord omgaan met de beschikbaar gestelde bedrijfsmiddelen. Dit wordt ook verwacht als medewerkers hun eigen middelen inzetten om werkzaamheden uit te voeren.

De afspraken in dit document gelden voor alle devices waarmee het werk wordt uitgevoerd. Ze gelden voor iedereen die werkzaam is de Stichting Gewoon Speciaal Onderwijs, ook voor tijdelijke werknemers.

Voor een veilig schoolklimaat is het belangrijk dat de afspraken rondom informatiebeveiliging en privacy door alle werknemers worden nageleefd en uitgedragen. Daarom is er een gedragscode opgesteld waaraan alle medewerkers van Stichting Gewoon Speciaal Onderwijs zich dienen te houden.

## REGELS TEN AANZIEN VAN GEBRUIK APPARATUUR

### Algemene normen

Iedere medewerker voldoet aan de volgende algemene normen voor 'zorgvuldigheid' (niet uitputtend):

- Ga zorgvuldig om met persoonsgegevens, waarbij de basisregels voor het omgaan met persoonsgegevens als bekend worden geacht;
- Voorkom het lekken van interne en vertrouwelijke informatie;
- Zorg voor goede beveiligingsmaatregelen ter bescherming van bedrijfsmiddelen;
- Meld diefstal of verlies van bedrijfsmiddelen onmiddellijk na constatering via de [website](#) van Stichting Gewoon Speciaal Onderwijs en bij je leidinggevende (zie hiervoor het [protocol beveiligingsincidenten en datalekken](#)).

### Computergebruik

- Het gebruik van de ICT-bedrijfsmiddelen is verbonden aan de werkzaamheden en gaat uit van de volgende afspraken:
- Zorg dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden;
- Weet welke gegevens er mogen worden gebruikt (mag iedereen het zien?) en welke ICT-voorzieningen kunnen worden ingezet (is het veilig genoeg?) bij het verrichten van de verschillende werkzaamheden;
- Sla (persoons)gegevens alleen op de daarvoor aangewezen systemen op.;
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk;
- Sluit na gebruik de computer af of log uit.

## Werkplek

Voorkom dat anderen (onbedoeld) toegang kunnen krijgen tot bedrijfsmiddelen waartoe zij geen rechten hebben en/of laat gegevens niet (onbedoeld) lekken. Als aanvullende regels op computergebruik gelden voor de werkplek de volgende clean desk en clear screen regels:

- Vergrendel bij het tijdelijk verlaten van de werkplek de pc;
- Verwijder interne en vertrouwelijke documenten van het bureau bij het voor langere tijd verlaten van de werkplek;
- Voorkom dat gevoelige en vertrouwelijke informatie zichtbaar is wanneer iemand anders op het beeldscherm (of via een digibord) mee kan kijken. Sluit het e-mail programma af en zorg voor een opgeruimd digitaal bureaublad;
- Laat geen afdrukken bij de printer liggen;
- Haal overbodig geworden papieren documenten met persoonsgegevens erop altijd door de papierversnipperaar.

## Gebruik van e-mail

De Stichting Gewoon Speciaal Onderwijs stelt een e-mailsysteem en een bijbehorende mailbox aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik van e-mailfaciliteiten is verbonden aan deze werkzaamheden en gaan uit van de volgende afspraken:

- Gebruik het mailadres alleén voor communicatie voor uitvoering van de werkzaamheden;
- Gebruik voor privé e-mail een eigen privé e-mailadres;
- Het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie;
- Het is niet toegestaan e-mail te gebruiken voor berichten met pornografische, racistische, discriminerende, beledigende, (seksueel) intimiderende of aanstootgevende inhoud of voor berichten die kunnen aanzetten tot haat en geweld;
- Synchroniseert een medewerker de zakelijke e-mail met eigen devices (tablet, telefoon) dan kan de organisatie, bij verlies of diefstal van het device, gebruik maken van de mogelijkheid om de e-mail op afstand te wissen, ook als daarmee alle (privé)gegevens van het device gewist worden.

## Gebruik eigen devices (BYOD)

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden worden uitgevoerd. De organisatie is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen van de organisatie.

Voor 'Own Devices' ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:

- Beveilig het device met een wachtwoord, of met een pincode die langer is dan 4 tekens;
- Vergrendel het device bij het verlaten van de werkplek;
- Sla persoonsgegevens van de organisatie niet op het eigen device op;
- Houd software up-to-date door het uitvoeren van periodieke updates (minimaal maandelijks);
- Neem adequate maatregelen tegen virussen of malware door het up-to-date houden van de virusscanner en door het periodiek (minimaal maandelijks) scannen van het device.



## REGELS TEN AANZIEN VAN GEBRUIK VAN GEGEVENS EN INFORMATIE

### Leerlinggegevens

**1. Verwerk leerling gegevens zoveel mogelijk digitaal.**

Leerlinggegevens worden zoveel mogelijk digitaal opgeslagen, geraadpleegd en bewerkt in het leerlingvolgsysteem. Dit geldt ook voor gegevens die via ouders/verzorgers en/of externen worden ontvangen. Bewaar geen gegevens op een USB-stick.

Gegevens die op papier aangeleverd worden, worden gescand en aan het leerlingvolgsysteem toegevoegd. Vergeet niet om de scan van je eigen computer te verwijderen.

**2. Formuleer gegevens die je vastlegt over een persoon zorgvuldig en professioneel.**

Ouders hebben het recht om het dossier in te zien. Zorg ervoor dat de gegevens zodanig zijn geformuleerd dat dit kan. Het past ook bij je houding als onderwijsprofessional.

**3. Gebruik voor de verwerking van leerlinggegevens bij voorkeur een computer van school.**

Moet je leerlinggegevens downloaden en bewerken op je computer? Doe dit alleen op een beveiligde computer (die voorzien is van encryptie of versleuteling), bij voorkeur een computer van school. Verwijder de bestanden na gebruik van je computer. Zorg ervoor dat anderen (bijv. familieleden) niet bij jouw werkbestanden kunnen komen.

**4. Ga na welke afspraken er binnen de school gemaakt zijn voordat je gegevens uitwisselt met derden.**

Wanneer je gegevens uit wil wisselen met externen, zoals bijvoorbeeld de logopedist, een arts, jeugdzorg of een schoolbegeleidingsdienst dan is het nodig om toestemming te vragen van ouders. Zorg dat je de toestemming registreert en hou daarbij ook rekening met de verdeling van het ouderlijk gezag. Voor de uitwisseling van gegevens met het samenwerkingsverband of een andere school gelden aparte afspraken. Hiervoor kun je terecht bij je IB-er.

**5. Informeer derden (ouders, hulpverleners etc.) wanneer je door hen aangeleverde informatie (zowel geschreven als mondeling) opslaat in het leerlingdossier.**

Wanneer je bijvoorbeeld telefonisch contact hebt over een leerling met een hulpverlener en je wilt die informatie opslaan in het leerlingdossier. Informeer dan zowel de hulpverlener als de ouders welke informatie je aan het dossier toevoegt.

### Hoe en wat communiceer ik online?

**1. Maak gebruik van een link naar het leerlingvolgsysteem om leerlinggegevens uit te wisselen met collega's.**

Verstuur leerlinggegevens liever niet per mail, maar verstuur een link met de vindplaats van de benodigde gegevens in het leerlingvolgsysteem.

**2. Vraag ouders om toestemming om een (privé)account aan te maken voor online diensten.**

Leerlingen moeten toestemming hebben van hun ouders/verzorgers om een

(privé)account aan te maken voor online diensten zoals Pinterest, Canva, Google etc.

- 3. Deel over individuele leerlingen nooit informatie via Social media.**  
Doe dit vooral in persoon of desnoods via de telefoon. Wat je communiceert via Social media kan makkelijk anders worden geïnterpreteerd door de lezer als je hier niet alert op bent.
- 4. Deel alleen kennis en informatie over de school als het geen vertrouwelijke of persoonlijke informatie betreft en andere betrokkenen en de naam van de school niet schaadt.**  
Wees voorzichtig met het online uiten standpunten. Privé-meningen van medewerkers kunnen eenvoudig verward worden met de officiële standpunten van de school en/of het bestuur. Je blijft altijd persoonlijk verantwoordelijk voor wat je deelt of publiceert. Wees je ervan bewust dat gepubliceerde uitlatingen voor onbepaalde tijd openbaar zullen zijn, ook na het verwijderen van het bericht.
- 5. Ga voordat je foto's of video's publiceert waar leerlingen op te zien zijn na of ouders hiervoor toestemming hebben gegeven.**  
Meer informatie hierover is te vinden in hoofdstuk 2.
- 6. Gebruik de accounts die door de school worden beheerd als je met ouders of leerlingen wil communiceren via e-mail of Social media.**  
Formuleer je boodschap ook hier professioneel en zorgvuldig, in correcte taal.
- 7. Word geen vrienden met ouders op sociale media met je privé-account.**
- 8. Zet e-mailadressen altijd in de BCC-regel als je naar (grote) groepen mensen een bericht verstuurt.**  
Zo blijven de e-mailadressen van de groepsleden afgeschermd.
- 9. Stuur nooit een e-mailbericht door naar derden zonder de degene van wie je het bericht ontvangen hebt hierover te informeren.**
- 10. Wanneer je een bericht stuurt met belangrijke en/of gevoelige informatie naar (een groep) ouders/verzorgers laat dit dan nalezen door een collega.**  
Een foutje is snel gemaakt en bovendien kan een ander kan je boodschap anders interpreteren dan jij hem bedoeld hebt. Het is dan fijn als er iemand met je meeleeft voordat je hem verstuurt.

### Hoe houd ik indringers op afstand?

- 1. Zorg er bij vertrouwelijke (telefonische) gesprekken voor dat er niet kan worden meegeluisterd.**  
Trek je je even terug als een gesprek een vertrouwelijk karakter heeft of krijgt.
- 2. Bewaar laptops of tablets altijd op een veilige plek, zeker tijdens vakantieperiodes.**  
Het is een open deur, maar toch gebeurt het heel erg makkelijk. Maak elkaar er dus op attent als je een laptop of tablet onbeheerd ziet liggen. Als je computer gestolen wordt, heeft dat gevolgen voor de school en de leerling.
- 3. Klik alleen op linkjes en open alleen bijlagen in e-mails van betrouwbare afzenders en pas op met het downloaden van bestanden.**  
Virussen kunnen makkelijk worden binnengehaald via (phishing)mails. In het criminele

circuit is dit een veelgebruikte methode om aan jouw gegevens te komen. Ook kunnen de gegevens op je computer versleuteld worden (ransomware).

- 4. Meld je altijd af als je de computer onbeheerd achterlaat. En zorg ervoor dat er op je werkplek geen gevoelige informatie zichtbaar of voor het grijpen ligt, ook bij de printer.**

Met de combinatie van de Windows- en L-toets kun je je makkelijk afmelden. Maak er een gewoonte van om papieren op je bureau om te draaien. Zo voorkom je dat anderen informatie zien die niet voor hen is bedoeld.

- 5. Zet je digibord op freeze als je wachtwoorden intoetst of persoonsgegevens in je scherm ziet staan. En zorg dat niemand meekijkt als jij je wachtwoord intoetst.**

Voordat je het weet zien leerlingen gevoelige gegevens of kunnen ze aan de hand van je afgekeken gebruikersnaam en wachtwoord proberen in te loggen. Zet ook de notificatie-functie van je e-mail uit, zodat er tijdens je les geen meldingen op het bord binnen komen die leerlingen kunnen zien, maar niet voor hun ogen bestemd zijn.

- 6. Laat je wachtwoorden van het leerling administratiesysteem of andere systemen met persoonsgegevens niet onthouden door je internetbrowser. En schrijf je logingegevens nooit op.**

Zonder dat je er erg in hebt, klik je de optie 'wachtwoord onthouden' in je browser aan. Heel makkelijk als je vaak moet inloggen, maar iemand anders kan dan dus ook inloggen. Kijk [hier](#) voor een tip om een sterk wachtwoord te kiezen die je makkelijk kunt onthouden.

- 7. Hou je logingegevens altijd voor jezelf, ook al vragen anderen aan je om ze te delen.**

Je login is in feite een sleutel om toegang te krijgen tot de informatie die voor jou toegankelijk moet zijn. Daarnaast herkent het systeem jou door je login, zodat het kan bijhouden wie welke gegevens heeft toegevoegd of gewijzigd.



## Protocol Datalekken

Organisaties zijn verplicht om een datalek te melden aan de Autoriteit Persoonsgegevens (AP), tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de personen waarvan de gegevens zijn gelekt. Organisaties moeten het datalek daarnaast melden aan de betrokken personen wanneer het lek kan leiden tot fysieke, materiële of immateriële schade voor deze betrokkenen. Het gaat dan om een situatie waarbij het lek waarschijnlijk een hoog risico voor de betrokkenen oplevert. Bij het niet melden van een datalek kan de Autoriteit Persoonsgegevens achteraf een boete opleggen.

Zijn er leerlinggegevens verloren gegaan? Is je laptop gestolen? Heb je last van een virus waardoor je niet meer bij je bestanden kunt? Of vertrouw je iets niet? Dan ben je verplicht dit zo snel mogelijk te melden via de [website](#) van Stichting Gewoon Speciaal Onderwijs en bij je leidinggevende. Als er persoonsgegevens beschadigd of verloren zijn, dan moet er mogelijk binnen 3 dagen een melding gedaan worden bij de Autoriteit Persoonsgegevens in het kader van meldplicht datalekken.

We spreken van een datalek wanneer er mogelijk persoonsgegevens (van leerlingen, hun ouders of medewerkers) in handen kunnen vallen van derden die geen toegang tot die gegevens zouden mogen hebben of wanneer er persoonsgegevens onbedoeld verloren zijn gegaan of onbedoeld zijn gewijzigd.

Voorbeelden van datalekken zijn de volgende incidenten, waarbij persoonsgegevens betrokken zijn:

- een e-mail die aan een verkeerd persoon geadresseerd is
- een kwijtgeraakte USB-stick
- inloggegevens die openbaar zijn geworden
- een gestolen iPad
- een gehackte computer
- gestolen of zoekgeraakte documenten
- onbedoeld gewijzigde gegevens

Het bevoegd gezag van de school is verantwoordelijk voor de bescherming van persoonsgegevens van leerlingen en personeel en moet bepalen of er een melding gedaan moet worden bij de Autoriteit Persoonsgegevens. Wanneer er een datalek ten onrechte niet wordt gemeld, kan een hoge boete opgelegd worden.

Ben je dus (een device met) persoonsgegevens kwijtgeraakt of heb je onrechtmatigheden geconstateerd met betrekking tot de toegang tot persoonsgegevens? Meld dit dan direct via de [website](#) en bij je leidinggevende, deze informeert de Privacy Officer en de Functionaris Gegevensbescherming.

In de koppeling op deze pagina is het protocol melden datalekken opgenomen.



## Reglement cameratoezicht

In het belang van de veiligheid, de gezondheid en het welzijn van leerlingen en medewerkers zijn kunnen scholen ervoor kiezen om camera's op te hangen. Met het cameratoezicht worden de volgende doelen nagestreefd:

- Bewaking in verband met toegang, schade door vandalisme en diefstal
- Herkenning of identificatie van personen die bij gebeurtenissen betrokken zijn geweest
- Bevorderen van het gevoel van veiligheid
- Preventief, ter voorkoming van onwenselijk gedrag
- Ondersteuning bij opsporing van strafbare feiten

## Informatievoorziening

De camera's zijn zichtbaar opgehangen, er wordt in principe geen gebruik gemaakt van verborgen camera's. In bijzondere gevallen, bij vermoeden van onrechtmatig handelen van leerlingen of personeel, kan tijdelijk een verborgen camera worden geplaatst.

Bij het betreden van de school wordt gewaarschuwd dat er cameratoezicht wordt uitgevoerd.

## Bewaartermijn beelden

- De camerabeelden worden maximaal 4 weken bewaard behoudens voor de beelden van de incidenten die in behandeling zijn. Indien er in de periode geen incidenten hebben plaatsgevonden of zijn gemeld bij de schoolleiding worden de beelden verwijderd.
- Bij geconstateerde incidenten worden de daaraan te relateren camerabeelden pas verwijderd nadat het incident is afgehandeld. Camerabeelden die gebruikt worden in het kader van onderzoek, waarvan aangifte is gedaan bij de politie, worden pas vernietigd na overleg met de politie. De termijn van vier weken is in deze gevallen niet van toepassing.
- Incidenten die het bewaren van beelden noodzakelijk maken, worden geregistreerd en gedocumenteerd in een logboek. Als beelden van een incident worden bekeken, wordt daarvan melding gemaakt in een logboek. Het logboek wordt beheerd door de systeembeheerder.

## Meekijken van beelden

Toestemming voor het bekijken van opgeslagen en/of actuele camerabeelden kan alleen gegevens worden door een lid van het managementteam.

## Beheer systeem

Systeembeheerders zijn alleen gerechtigd benodigde software te installeren en te controleren op het functioneren van het systeem.

## Informatie aan ouders

- Ouders van een leerling die een incident meldt dat het bekijken van camerabeelden noodzakelijk maakt, worden hiervan door de schoolleiding op de hoogte gesteld.



- Indien een leerling – in het belang van het oplossen van een incident – wordt verzocht camerabeelden te bekijken, worden ouders hiervan op de hoogte gesteld. Ouders kunnen het bekijken van de beelden desgewenst bijwonen.
- Ouders van een leerling die na het bekijken van de camerabeelden als “dader” wordt geïdentificeerd, worden hiervan door de schoolleiding op de hoogte gesteld en hebben het recht de beelden binnen de bewaartermijn uit dit protocol te bekijken.

Camerabeelden die een incident registreren, dat aangifte bij de politie noodzakelijk maakt, kunnen desgevraagd door de politie worden bekeken. Betrokken leerlingen en ouders worden hierover geïnformeerd.

## Archivering: bewaartermijnen

Vanuit de privacywetgeving zijn er geen concrete bewaartermijnen voor persoonsgegevens vastgesteld. Wel dient iedere organisatie hiervoor richtlijnen te hebben. Hierbij is het van belang om na te gaan hoe lang de gegevens nodig zijn voor het doel waarvoor deze zijn verzameld. In andere wetten zijn in sommige gevallen wel bewaartermijnen opgenomen waaraan organisaties zich moeten houden.

Naast de in dit document genoemde termijnen kan bij de praktische uitvoering uitgegaan worden van de volgende, door Kennisnet opgestelde, algemene richtlijnen voor bewaartermijnen:

- Gegevens die zijn vastgelegd in het leerling administratiesysteem - 5 jaar;
- Gegevens die betrekking hebben op financiën - 7 jaar;
- Overige gegevens - 2 jaar en in het passend onderwijs 3 jaar;
- Let op: Getuigschriften (diploma's en cijferlijsten) en besluiten tot het verlenen van vrijstelling op grond van de Leerplichtwet dienen bewaard te blijven. Op deze stukken is de Archiefwet van toepassing. Op dit moment is nog niet duidelijk of deze gegevens vernietigd mogen worden.

**Als de bewaartermijn verstreken is moeten de gegevens vernietigd worden.**

### Leerlingen (onderwijskundig)

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Het onderwijskundig rapport	2 jaar (vuistregel volgens AP voor leerlingdossier)	Na datum van uitschrijving
Gegevens over leerprestaties van de leerling (o.a. schoolexamens)	2 jaar (vuistregel AP voor leerlingdossier)	Na datum van uitschrijving
Verslagen van gesprekken met de ouders	2 jaar (vuistregel AP voor leerlingdossier)	Na datum van uitschrijving
Adres- en communicatiegegevens	2 jaar (vuistregel AP voor leerlingdossier)	Na datum van uitschrijving
Gegevens betreffende de godsdienst of levensovertuiging	2 jaar (vuistregel AP voor leerlingdossier)	Na datum van uitschrijving
Gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen en	3 jaar Art. 18a lid 13 Wet PO	Na afloop van: (a.) de beoordeling van de toelaatbaarheid van de leerling tot het onderwijs aan

of de doorverwijzing naar speciaal onderwijs		<p>een speciale school voor basisonderwijs of tot het speciaal onderwijs,</p> <p>(b.) de advisering over de ondersteuningsbehoefte van de leerling aan het bevoegd gezag van de school waar de leerling is aangemeld of ingeschreven,</p> <p>(c.) de toewijzing van ondersteuningsmiddelen of ondersteuningsvoorzieningen aan de school.</p>
Psychologisch rapport	<p>2 jaar</p> <p>(aanvulling: bewaartermijn voor medisch dossier is 15 jaar. Deze bewaartermijn geldt voor de psycholoog en niet voor de school)</p>	Na datum van uitschrijving
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk	6 maanden	Na moment van opname

### Leerlingen/oud-leerlingen (administratief)

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Gegevens die nodig zijn om te berekenen hoeveel bekostiging de school ontvangt	<p>7 jaar</p> <p>(art. 172 lid 3 WPO)</p>	Na afloop van het schooljaar waarop de bekostiging betrekking heeft
Gegevens over in- en uitschrijving	<p>5 jaar</p> <p>(art. 6 lid 1 bekostigingsbesluit WPO)</p>	Na datum van uitschrijving
Kopie identiteitsbewijs	Er mag gevraagd worden naar het identiteitsbewijs van de leerling. Het is niet toegestaan om die kopie in het dossier te bewaren. Volgens de wet moet de school de identiteit controleren, en dat betekent	

	niet dat een kopie mag worden bewaard na inschrijving.	
Gegevens over verzuim en afwezigheid	5 jaar (art. 6 lid 1 Besluit bekostiging WPO)	Na datum van uitschrijving
Gegevens met betrekking tot de vergoeding van de kosten verbonden aan leerlingvervoer	2 jaar (norm: art 21 lid 5 vrijstellingsbesluit WBP)	Na afloop van het schooljaar waarop de verstrekking van de vergoeding betrekking heeft
Communicatiegegevens oud-leerlingen (o.b.v. toestemming, bv. t.b.v. reünies)	Verwijderen op verzoek van de leerling of bij diens overlijden	Na datum van uitschrijving

### Personeel/oud-medewerkers/leden toezichthoudend orgaan

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Akte van aanstelling/ arbeidsovereenkomst	2 jaar (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	Na einde dienstverband
Wijzigingen arbeidsovereenkomst	2 jaar (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	Na einde dienstverband
Correspondentie inzake benoemingen, promotie, demotie	2 jaar (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	Na einde dienstverband
Gegevens sollicitatie (Sollicitatiebrief, -formulier, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek)	2 jaar (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	Na einde dienstverband
Aanspraken in verband met de beëindiging van het dienstverband	2 jaar (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	Datum waarop aanspraken zijn geëindigd

Afspraken inzake werk MR	2 jaar  (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	Na einde lidmaatschap
Kopie getuigschrift	2 jaar  (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	Na einde dienstverband
Afspraken inzake opleidingen	2 jaar  (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	Na einde dienstverband
Aanvraag opleiding door werknemer	2 jaar  (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	Na einde dienstverband
Afspraken omtrent loopbaan	2 jaar  (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	Na einde dienstverband
Verlagen functionerings- en beoordelingsgesprekken	2 jaar  (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	Na einde dienstverband
Correspondentie UWV en bedrijfsarts	2 jaar  (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	Na einde dienstverband
Verslaglegging inzake Wet Verbetering Poortwachter	2 jaar  (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	Na einde dienstverband

Verzuimregistratie als werkgever eigenrisicodragers Ziektewet is.	5 jaar (art. 3 lid 2 Regeling wkzh, administratieve voorschriften, en kosten eigenrisicodragers ZW)	
Gegevens m.b.t. eigenrisicodragerschap i.v.m. WW	Tot einde wettelijke verplichting	
Verslaglegging van correspondentie met betrekking tot problematische (financiële) privé-situatie	2 jaar (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	Na einde dienstverband
Loonbeslagen	Tot opheffen loonbeslag	Bij opheffen loonbeslag
Correspondentie met betrekking tot jubilea	tot einde dienstverband	
Correspondentie directie/PZ/direct leidinggevende	2 jaar (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	
Identiteitspapieren van derden ingeleende vreemdelingen waarvoor een tewerkstellingsvergunning is verleend	5 jaar (art. 15 lid 4 Wet arbeid vreemdelingen)	Einde dienstverband
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk	2 jaar (art. 53 lid 2 WPO, i.i.g. gedurende dienstverband, algemene norm 2 jaar)	Einde dienstverband
Loonadministratie	7 jaar (art. 52 lid 4 Algemene wet inzake rijksbelastingen)	Na afloop boekjaar
Burgerlijke staat werknemer	7 jaar (art. 52 lid 4 Algemene wet inzake Rijksbelastingen)	Na einde dienstverband



Loonbelastingverklaringen en kopie identiteitsbewijs uit loonadministratie	5 jaar (art. 7.5 lid 4 en art. 7.9 lid 2 Uitvoeringsregeling loonbelasting)	Na einde kalenderjaar waarin dienstverband is geëindigd
Communicatiegegevens oud-personeelsleden	7 jaar (art. 52 lid 4 Algemene wet inzake Rijksbelastingen Bewaren toegestaan op basis van toestemming	Einde dienstverband

### Sollicitanten

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Sollicitatiebrief, -formulier, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek	4 weken zonder toestemming, maximaal 1 jaar met toestemming van de sollicitant (vuistregel AP)	Na beëindiging sollicitatieprocedure

### Leveranciers

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Persoonsgegevens van (vertegenwoordigers van) leveranciers	2 jaar	Nadat de desbetreffende transactie is afgewikkeld of samenwerking is beëindigd.

### Huurders

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Persoonsgegevens van huurders	2 jaar	Nadat de huur is beëindigd

### Alle bovengenoemde categorieën en bezoekers

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Camera en videobeelden	maximaal 4 weken, of na afhandeling van incidenten	Na moment van opname

Gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de video-opnamen zijn gemaakt (logboek)	Gedurende het lopende schooljaar(eigen norm)	Na moment van opname
Registratielijsten bezoekers	niet langer dan nodig, 1 week, of na afhandeling van incidenten.  (art. 5 lid 1e AVG)	Na moment van registratie

### Disclaimer

Deze richtlijn is door Privacy op School B.V. met zorg en aandacht samengesteld. Het betreft een algemene richtlijn en houdt geen individueel advies in. Er kunnen dan ook geen rechten aan de richtlijn worden ontleend. Privacy op School is niet aansprakelijk voor schade of kosten die direct en/of indirect ontstaan door het gebruik van deze richtlijn, zoals schade veroorzaakt door mogelijke schrijffouten, onjuistheid, onvolledigheid of gedateerdheid. Privacy op School behoudt zich het recht voor om eventuele wijzigingen met onmiddellijke ingang en zonder informatie vooraf door te voeren. Het gebruik van deze richtlijn is voor risico van de gebruiker.

## Checklist in- en uitdiensttreding

### Actielijst nieuwe medewerkers

Actie:	Actie door:
Muteren in Groenendijk Personeels Beheer(GPB) n.a.v. aanmeldingsformulier.	Secretariaat/administratie
Verzoek aan ICT'er aanmaken email adres en laten opnemen in de verschillende verzendlijsten en Cloud mappen	Secretariaat/administratie
Aanmaken email adres en laten opnemen in de verschillende verzendlijsten en Cloud mappen	ICT-coördinator
Doorgeven inloggegevens van nieuwe medewerkers aan Secretariaat	ICT-coördinator
Aanmelden medewerker bij diverse software (oa Gynzy)	ICT-coördinator
Doorgeven mutaties (nieuw en uit dienst) voor IPPON aan bestuursbureau.	Secretariaat/administratie
Aanmaken inlogaccount in het leerlingvolgsysteem en koppelen aan de juiste groepen	Secretariaat/administratie
Uitnodigen voor de agenda's en uitleg jaarplanner	Secretariaat/administratie
Wijzigen naamkaartjes /groepsafbeelding / aanwezigheidsbord /postvakjes	Secretariaat/administratie
Aanpassen personeelslijst / lijst noodnummers	Secretariaat/administratie
Uitreiken sleutel en sleutelverklaring laten tekenen	Secretariaat/administratie
Alarmcode doorgeven en uitleg werking alarm geven	Secretariaat/administratie
Uitleg geven nieuwe medewerkers ontruimingsoefening.	Secretariaat/administratie
Verjaardagen vermelden	Secretariaat/administratie
Verzoek tot voorstellen t.b.v. de nieuwsbrief ouders	Secretariaat/administratie
Foto nieuwe medewerker maken	Secretariaat/administratie
Naam vermelden op lijst dienstjaren	Secretariaat/administratie
Naam toevoegen in SoftwareTaakbeleid	Secretariaat/administratie

## Actielijst medewerkers uit dienst

Actie:	Actie door:
Muteren in GPB.	Secretariaat/administratie
Verzoek aan ICT'er email adres op te heffen uit de verschillende verzendlijsten te halen en Cloud omgeving af te sluiten.	Secretariaat/administratie
ICT'er verwijdert medewerker na laatste werkdag uit de verschillende verzendlijsten en Cloud omgeving.	ICT-coördinator
ICT'er heft O365 account op 1 week na laatste werkdag.	ICT-coördinator
Afmelden medewerker bij diverse software (o.a. Gynzy)	ICT-coördinator
Doorgeven mutaties voor IPPON aan bestuursbureau.	Secretariaat/administratie
Afsluiten account in het leerlingvolgsysteem een dag na laatste werkdag	Secretariaat/administratie
Afsluiten inzage in de agenda jaarplanner.	Secretariaat/administratie
Wijzigen naamkaartjes / groepsafbeelding /aanwezigheidsbord / postvakjes	Secretariaat/administratie
Aanpassen personeelslijst/lijst noodnummers	Secretariaat/administratie
Innemen van sleutel, ontbinding sleutelverklaring tekenen.	Secretariaat/administratie
Alarmcode inactief maken	Secretariaat/administratie
Mail sturen met de mededeling, dat ze 1 week na hun laatste werkdag de tijd hebben om hun mail/ OneDrive op te schonen, voordat het O365 account wordt gesloten en dat na hun laatste werkdag, deze persoon op de eerst volgende werkdag door de administratie wordt gedeactiveerd in het leerlingvolgsysteem en het verzoek om sleutels in te leveren.	Secretariaat/administratie
Verjaardag verwijderen uit de jaarplanner	Secretariaat/administratie
Foto personeelslid uit het leerlingvolgsysteem halen?	Secretariaat/administratie
Naam verwijderen van lijst dienstjaren	Secretariaat/administratie
Naam verwijderden uit software Taakbeleid	Secretariaat/administratie





# BIJLAGEN

PRIVACY HANDBOEK



## Bijlage A: Overzicht verwerkers

Voor digitale leermiddelen en toetsen worden systemen van diverse leveranciers of uitgeverijen gebruikt. Met deze partijen worden of zijn verwerkersovereenkomsten afgesloten. Onderdeel hiervan is dat zij ook voldoen aan de Europese standaarden en voorzieningen met betrekking tot de veilige uitwisseling van persoonsgegevens.

Verwerkers die deelnemer zijn van het Privacy Convenant kunnen gebruik maken van het [template](#) van voornoemd convenant. Voor verwerkers die geen deelnemer zijn van het convenant zal een separate overeenkomst opgesteld worden die voldoet aan de eisen van de AVG.

- |  |   |
|--|---|
| <input type="checkbox"/> 678 Onderwijsadvisering       | <input type="checkbox"/> DataCare                       |
| <input type="checkbox"/> Apply                         | <input type="checkbox"/> Dedicon                        |
| <input type="checkbox"/> Ars Scribendi Uitgeverij B.V. | <input type="checkbox"/> Driestar Educatief             |
| <input type="checkbox"/> Avision (onderzoek)           | <input type="checkbox"/> Eigenwijs                      |
| <input type="checkbox"/> Bareka Online Rekentoetsen    | <input type="checkbox"/> Emjee ICT diensten             |
| <input type="checkbox"/> BasisOnline                   | <input type="checkbox"/> Groenendijk                    |
| <input type="checkbox"/> Bazalt Educatieve Uitgaven    | <input type="checkbox"/> Google                         |
| <input type="checkbox"/> Benny Vreden                  | <input type="checkbox"/> Gynzy                          |
| <input type="checkbox"/> BHV BHV,112                   | <input type="checkbox"/> Heutink ICT                    |
| <input type="checkbox"/> Blink                         | <input type="checkbox"/> Heutink Primair Onderwijs BV   |
| <input type="checkbox"/> Bloon                         | <input type="checkbox"/> Iddink Voortgezet Onderwijs bv |
| <input type="checkbox"/> Bomberbot                     | <input type="checkbox"/> ISO Groep Automatisering B.V.  |
| <input type="checkbox"/> Boom uitgevers Amsterdam      | <input type="checkbox"/> Jamf School                    |
| <input type="checkbox"/> Bosos                         | <input type="checkbox"/> Junior Einstein                |
| <input type="checkbox"/> Bureau ICE                    | <input type="checkbox"/> Kennisnet                      |
| <input type="checkbox"/> CED-Groep                     | <input type="checkbox"/> Koninklijke Van Gorcum         |
| <input type="checkbox"/> Cito                          | <input type="checkbox"/> Kurzweil                       |
| <input type="checkbox"/> Cloudwise B.V.                | <input type="checkbox"/> LessonUp                       |
| <input type="checkbox"/> Concapps                      | <input type="checkbox"/> Lexima                         |
| <input type="checkbox"/> Cupella                       | <input type="checkbox"/> LinkedIn                       |



- Mailchimp
- Malmberg
- Memelink
- Mollie
- Noordhoff
- Oefenweb.nl
- Onlineklas
- Parentcom
- ParnasSys
- Parnassys Parro
- Parnassys Schoolkassa
- Pearson
- Prowise B.V.
- Raet
- Rolf groep (licentie groove.me)
- Rovict B.V.
- Rutgers
- Schoolmaster BV
- Social Schools
- SOMToday
- Semenarium voor Orthopedagogiek  
( Memelink)
- Snappet
- Squla
- Stichting Basispoort
- Taalbos
- TimeTell
- Tumult
- Uitgever Essener
- Uitgever Zwijsen
- Van Dijk Educatie bv
- Veilig Verkeer Nederland
- Veolia
- Xando
- Zermelo Software B.V.
- Zivver
- Zoom
- Zorg van de zaak
- ZuluDesk/ JAMF
- Zwijsen

## Bijlage B: Toestemmingsformulier gebruik beeldmateriaal

### Toelichting in het kader van privacy wetgeving

De gegevens die u heeft ingevuld op het inschrijfformulier, worden opgeslagen in de leerling administratie van onze school. Uiteraard worden deze gegevens vertrouwelijk behandeld. Op onze verwerkingen is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Dit betekent onder andere dat de gegevens door ons worden beveiligd, en dat de toegang tot de gegevens is beperkt tot alleen personeel die de gegevens strikt noodzakelijk nodig heeft. U heeft als ouder het recht om de door ons geregistreerde gegevens in te zien (voor zover die informatie betrekking heeft op uw kind). Als de gegevens niet kloppen, dan mag u van ons verwachten dat wij – op uw verzoek - de informatie verbeteren of aanvullen.

Voor meer informatie over de omgang met de privacy van uw kind(eren), verwijzen wij u naar onze privacyverklaring onderaan op [onze website](#).

### Toestemming

In het kader van privacywetgeving, willen wij u toestemming vragen voor het delen van de volgende persoonsgegevens. U mag natuurlijk altijd terugkomen op de door u gegeven toestemming. Ook mag u op een later moment alsnog toestemming geven.

### Foto- en videomateriaal

Op onze school laten wij u met foto's en video's zien waar we mee bezig zijn. Opnames worden gemaakt tijdens verschillende gelegenheden. Ook uw zoon/dochter kan op deze foto's (en soms in video's) te zien zijn. Graag willen we daarom uw toestemming voor het gebruik van beeldmateriaal van uw zoon/dochter. Uw toestemming geldt alleen voor foto's en video's die door ons, of in onze opdracht worden gemaakt. Het maken van foto's door ouders is binnen de school niet toegestaan. Het kan voorkomen dat andere ouders foto's maken tijdens schoolactiviteiten die buiten de school plaatsvinden. De school heeft daar geen invloed op. Wij vragen daarom aan ouders om terughoudend te zijn met het maken van foto's en video's en deze niet te delen via sociale media.

### Adressenlijst

Op onze school wordt er, per klas, een lijst gemaakt met de adressen van leerlingen. Deze lijst met contactgegevens is erg praktisch om te overleggen met andere ouders, als de kinderen (buiten schooltijd) willen afspreken of als er vragen zijn rondom school, overblijf, etc. Wij vragen hierbij uw toestemming om de naam van uw kind, diens adres en uw telefoonnummer te mogen delen met de andere ouders van de school. Als u er bezwaar tegen heeft, wordt de naam van uw kind niet gedeeld (en moet u daar zelf voor zorgen). Deze informatie op de klassenlijst mag uitsluitend gebruikt worden voor persoonlijk gebruik onderling.

### Sociale media

Sociale media spelen een belangrijke rol in het leven van leerlingen en onderwijzend personeel. Het gebruik van sociale media is onderdeel van het gedrag van leerlingen binnen de school. Sociale media kunnen helpen om het onderwijs te verbeteren en de lessen leuker te maken en om contact te onderhouden met vrienden of klasgenoten. Maar sociale media brengen ook risico's met zich mee, zoals pesten en het ongewild delen van foto's of andere gegevens. Op school besteden we in ons lesprogramma hier aandacht aan. Voor het gebruik van sociale media door uw kind(eren), vragen wij uw toestemming.

Hierbij verklaart ondergetekende, ouder/verzorger van  
....., dat:

foto's en video's **WEL** gebruikt mogen worden:

- op het ouderportaal van de school
- in de (digitale) nieuwsbrief
- in de schoolkalender
- in de schoolgids
- op de website van de school
- in folders en flyers ter promotie van de school
- op sociale-media accounts van de school (Whatsapp, Twitter, Facebook)

*(kruis aan waar u toestemming voor geeft)*

haar/zijn naam, adres en telefoonnummer **WEL / NIET** \* gedeeld mag worden met andere ouders

hij/zij **WEL / NIET** \* getoond mag worden op de klassenfoto die periodiek gemaakt wordt

hij/zij onder schooltijd **WEL / NIET**\* gebruik mag maken van sociale media t.b.v. onderwijsdoeleinden

(\* streep door wat niet van toepassing is)

N.B. De toestemming kan op elk moment ingetrokken worden. Neem hiervoor contact op met **naam directeur**, via **mailadres directeur**.

## Bijlage C: Gebruikersovereenkomst (mobiele) devices

### Gebruikersovereenkomst Stichting Gewoon Speciaal Onderwijs

Stichting Gewoon Speciaal te Houten, in deze vertegenwoordigt door **Naam**, **functie**, hierna te noemen werkgever

en

[Naam medewerk(st)er], werkzaam als [functie] bij [Onderwijsinstelling], hierna te noemen werknemer:

Nemen in aanmerking dat:

- dat werkgever heeft vastgesteld dat voor een goede uitoefening van de dienstbetrekking het noodzakelijk is dat de werknemer een communicatiemiddel<sup>2</sup> en bijbehorende apparatuur in bruikleen ter beschikking wordt gesteld;
- Werkgever verstrekt aan werknemer de apparatuur ten behoeve van de uitoefening van de werkzaamheden ten tijde van de dienstbetrekking;
- De apparatuur is eigendom van werkgever en wordt in bruikleen gegeven aan werknemer;
- Deze overeenkomst bepaalt de nadere gebruiksvoorwaarden waaronder werknemer de apparatuur kan gebruiken;
- Door ondertekening aanvaardt werknemer alle voorwaarden van deze overeenkomst.

#### 1. Aard en uitvoering

Het type apparatuur en/of het abonnement wordt door werkgever vastgesteld en aangeschaft.

#### 2. Rechten en plichten werknemer

- a. Werknemer verklaart de apparatuur in goede staat te hebben ontvangen en zal deze niet aan derden ter beschikking stellen, verpanden of op enigerlei andere wijze vervreemden.
- b. Werknemer is verantwoordelijk voor het in goede en representatieve staat houden van de apparatuur.
- c. Tijdens een ziekteperiode van de werknemer van 6 weken of langer, moet de apparatuur ingeleverd worden bij werkgever.
- d. Het is werknemer niet toegestaan zonder toestemming van de direct leidinggevende de apparatuur tijdens verlof mee te nemen naar het buitenland. Ook is bellen naar en vanuit het buitenland niet toegestaan.
- e. Het is werknemer niet toegestaan zonder toestemming van de werkgever wijzigingen in de configuratie van de apparatuur aan te brengen.
- f. Het is werknemer verboden de apparatuur te gebruiken voor activiteiten die in strijd zijn met de bedrijfsdoelstellingen of het aanzien van de werkgever schade (kunnen) berokkenen, dan wel de grenzen van betamelijkheid en fatsoen overschrijden.
- g. Werknemer is op de hoogte dat werkgever het gebruik van de apparatuur door de werknemer controleert op het zakelijk gebruik van de apparatuur. Door ondertekening van deze overeenkomst stemt de werknemer in met deze controle. Tevens verklaart werknemer zicht bereid alle medewerking te verlenen die noodzakelijk is om het zakelijk gebruik te kunnen onderbouwen.

---

<sup>2</sup> Specificatie van communicatiemiddel is opgenomen in de bijlage van de overeenkomst.

- h. Werknemer verklaart zich akkoord dat indien werknemer heeft gehandeld in strijd met de bepalingen van deze gebruikersovereenkomst, eventueel daaruit voortvloeiende kosten zullen worden verhaald op werknemer.

### 3. Gebruik apparatuur

De werknemer wordt voor de uitoefening van zijn dienstbetrekking de apparatuur ter beschikking gesteld die werknemer voor minder dan € [bedrag] per jaar voor privé doeleinden gebruikt. Bij het belastbare loon van de werknemer wordt maandelijks een bedrag van € [bedrag] geteld voor het privégebruik van de mobiele telefoon.

De werknemer wordt voor de uitoefening van de dienstbetrekking een mobiele telefoon ter beschikking gesteld die werknemer uitsluitend voor zakelijke doeleinden dient te gebruiken.

### 4. Niet toegestaan gebruik

Het is werknemer niet toegestaan:

- Sms-berichten te sturen naar of te ontvangen van commerciële nummers die niet werkgerelateerd zijn en tot (extra) kosten kunnen leiden, zoals reageren op radio- of tv-acties.
- De verstrekte simkaart te gebruiken in een ander dan het verstrekte toestel.
- Een andere simkaart in het verstrekte toestel te gebruiken dan de bij het verstrekte toestel behorende simkaart.
- Gebruik te maken van bluetooth anders dan voor het verbinden met een headset of carkit. Bij gebruik van bluetooth moet de keuze 'verborgen' worden ingesteld.
- Het toestel uit handen te geven of uit te lenen aan personen van buiten de organisatie.

### 5. Diefstal en beschadiging

- Werknemer dient afdoende beschermingsmaatregelen te treffen, zoals periodiek wijzigen van wachtwoorden en dergelijke, ter bescherming van gegevens op de apparatuur.
- Werknemer dient alle zorgvuldigheid in acht te nemen ter voorkoming van beschadiging, diefstal of verlies van de apparatuur.
- In geval van schade of diefstal van de apparatuur is werknemer verplicht dit zo spoedig mogelijk, doch uiterlijk binnen 24 uur bij werkgever te melden. Als contractant draagt werkgever het risico voor misbruik na diefstal, mits aan het hiervoor gestelde is voldaan.
- Werknemer kan aansprakelijk worden gesteld voor verlies van of schade aan de apparatuur ontstaan door verwijtbare nalatigheid of onachtzaamheid. Kosten voor herstel of vervanging kunnen in dat geval worden ingehouden op het salaris van medewerker.

### 6. Termijn van gebruik

- Werknemer dient de apparatuur binnen de afgesproken bruikleentermijn dan wel bij beëindiging van het dienstverband of functieverandering op eerste verzoek in volledige staat te retourneren. Bij verzuim hiertoe, verbindt werknemer zich tot betaling van de rest(boek)waarde van de apparatuur aan werkgever.
- Indien werknemer na het einde van de bruikleenovereenkomst of na opzegging hiervan door werkgever niet onmiddellijk voldoet aan een verzoek van werkgever tot teruggave van de apparatuur, verbeurt werknemer een boete van €250,00 voor iedere dag, dat

werknemer, na bij aangetekende brief door werkgever vermaand te zijn, aan zijn verplichtingen niet voldoet.

- c. Indien één van de genoemde gevallen in deze gebruikersovereenkomst zich voordoet, is werkgever bevoegd een geschil betreffende de teruggave van de apparatuur aan het oordeel van de President van de arrondissementsrechtbank te Utrecht, rechtsprekende in kort geding, te onderwerpen.
- d. Door ondertekening van deze overeenkomst verklaart werknemer dat hij gevolgen van deze overeenkomst heeft begrepen en zich daarmee akkoord verklaart.

Aldus verklaard, opgemaakt in tweevoud en ondertekend te **Plaats**,

**Naam school**

	Werkgever	Werknemer
<b>Naam:</b>		
<b>Datum:</b>	vrijdag 28 januari 2022	
<b>Plaats:</b>		
<b>Handtekening:</b>		





## Afspraken over computergebruik

1. Je mag **alleen** op de computers in opdracht van de meester of juf
2. Bij een storing altijd de meester of juf waarschuwen
3. Er worden aan, op, naast of in de nabijheid van de computers niet gegeten of gedronken.
4. Je mag **alleen** op internet met toestemming én als de meester of juf erbij is
5. Nooit van jezelf, van anderen of van de school de naam, adres, telefoonnummer of andere persoonlijke zaken doorgeven
6. Nooit op internet naar pagina's gaan met seks, geweld, discriminatie of andere "minder geschikte pagina's".
7. Als je per ongeluk op zo'n site komt of andere schokkende beelden ziet, dit direct melden aan de juf of meester
8. Alleen met toestemming van de juf of meester programma's of bestanden downloaden.
9. Printen mag alleen door de groepsleerkrachten
10. Downloaden moet bedoeld zijn voor een opdracht die voor school wordt uitgevoerd en niet voor eigen gebruik
11. Je mag niet chatten
12. Je mag geen spelletjes tegen anderen spelen via het internet
13. Wie zich niet aan deze regels houdt, mag minimaal een maand geen gebruik meer maken van de computer.



## Afspraken gebruik ICT VSO

**Regels met betrekking tot gebruik van ICT-middelen en internet op de Berg en Boschschool voor leerlingen die gebruik maken van het WIFI-netwerk en daarop inloggen met school- of eigen apparatuur.**

Deze regels zijn speciaal opgesteld voor leerlingen die **met toestemming** van de school gebruik maken van het leerlingnetwerk. Daarnaast blijven de algemene “regels tot gebruik van ICT middelen en internet voor leerlingen” van kracht.

### Algemeen:

De kwaliteit en betrouwbaarheid van de ICT- infrastructuur op school moet gewaarborgd zijn om optimaal onderwijs te bieden aan leerlingen en de organisatie goed te laten functioneren. Het E-mailverkeer en internetgebruik moet aan regels en afspraken gebonden zijn om misbruik te voorkomen.

De school wil daarom regels hanteren en bij misbruik van de schoolsystemen en de mogelijkheden die deze bieden m.b.t. E-mail en internetverkeer de misbruiker kunnen aanspreken op zijn of haar verantwoordelijkheid. Daarnaast wil de school eventuele veroorzaakte schade kunnen verhalen op de veroorzaker.

Leerlingen die gebruik maken van het **leerlingnetwerk** worden daarvoor geautoriseerd middels het MAC-adres van het laptop of tablet.

**Door het ondertekenen van dit formulier verklaren zij kennis te hebben genomen van de regels en zich daaraan te zullen houden. De betrokkene ontvangt (indien gewenst) een kopie van dit ondertekende reglement.**

## 2. Algemene uitgangspunten computergebruik (Hard en Software)

Iedere leerling is verantwoordelijk voor de hard-/software waarmee hij of zij op school werkt. De leerlingen moeten zorgvuldig met de beschikbaar gestelde materialen omgaan. Wat mag is:

- de in gebruik zijnde (school)hardware op dezelfde plaats achterlaten, en zorgen dat die onbeschadigd blijft.
- de standaardinstellingen daarvan ongewijzigd houden.
- de standaardinstellingen van je profiel, gebruikte (school) pc of beeldscherm en overige apparatuur ongewijzigd houden.
- een gestarte internetsessie alleen zelf gebruiken.
- een door andere gestarte internetsessie ongebruikt laten/niet overnemen.
- een internetsessie afsluiten als je er niet actief gebruik van maakt.
- je persoonlijke user-id, wachtwoord, en overige inlogcode e.d. alleen voor jezelf houden.
- Indien het vermoeden bestaat dat anderen op de hoogte zijn van je wachtwoord dan moet je dit direct wijzigen.
- indien door anderen onder jouw netwerk-account wordt ingelogd (spoofing) dien je dit direct te melden aan de ICT-medewerkers.
- op schoolapparatuur alleen software die door school is gedownload en geïnstalleerd gebruiken.
- virusvrije software/virusscanner gebruiken.
- geen andere (rand)apparatuur aansluiten/inschakelen zoals wifi-accesspoints, hotspots e.d

### 3. E-mailgebruik en overige sociale media

Regels en afspraken met betrekking tot het e-mail- en internetverkeer zijn erop gericht berichten die op enige wijze aanstootgevend kunnen zijn tegen te gaan.

Het is toegestaan om e-mails te versturen waarvan de inhoud in principe door iedereen gelezen mag worden. Dus:

- alleen berichten zonder dreigende, beledigende, seksueel getinte of discriminerende aard.
- alleen berichten die niet verplicht doorgestuurd moeten worden. (z.g. kettingbrieven)
- alleen berichten zonder kwetsend of grof taalgebruik.
- alleen berichten zonder commerciële boodschappen.

### 4. Internetgebruik

Internetgebruik op school is vooral bedoeld om bij te dragen aan het leerproces. Alles dat behoort tot het vervullen van opdrachten vanuit de school is dus toegestaan.

De volgende regels zijn van kracht:

- je werkt stil zodat niemand last van je heeft.
- je respecteert de auteursrechten van derden.
- je blijft weg van sites die pornografisch, racistisch, discriminerend, beledigend, gewelddadig of aanstootgevend materiaal bevatten.
- je houdt je aan de “*netiquette*”. (De netiquette omvat de ongeschreven richtlijnen en gedragsregels voor het gebruik van internet.) Meer informatie op <http://nl.wikipedia.org/wiki/Netiquette>

### 5. Gebruik van eigen apparatuur

De eigen apparatuur waarmee leerlingen gebruik maken van het netwerk dient van goede kwaliteit te zijn. Technische ondersteuning (hard én/of software) kan niet gegeven worden. Mocht er een storing optreden dan zal aanvankelijk getracht worden het probleem op te lossen. Mocht een probleem zich vaker voordoen dan zal de leerling het advies krijgen andere apparatuur aan te schaffen.

### 6. Controle

Controle op alles wat in deze regeling is omschreven vindt plaats door:

- vastlegging van het computergebruik.
- het blokkeren van verboden sites.
- bij het vermoeden van misbruik kan de systeembeheerder (na overleg met de schoolleiding) je vragen de computer / telefoon / tablet beschikbaar te stellen voor controle. Hieraan dient gevolg gegeven te worden.

### 7. Wat gebeurt er als je je niet aan regels/afspraken houdt?

- je wordt aangesproken op je gedrag.
- de mogelijkheid tot computergebruik wordt je voor bepaalde tijd ontnomen.
- als de overtreding ernstig is kun je een officiële waarschuwing krijgen.
- je ouders/verzorgers worden aansprakelijk gesteld voor de schade en de daaruit voortvloeiende kosten van herstel.
- in het geval van strafbare feiten wordt aangifte gedaan bij de politie.

### 8. Rechten en plichten

De school houdt zich aan de bepalingen in de Wet Bescherming Persoonsgegevens (zie voor de tekst van de wet op <http://www.rijksoverheid.nl/onderwerpen/persoonsgegevens>).

### 9. Slotbepaling

Als zich situaties voordoen waarin deze regeling niet voorziet zal de schoolleiding in overleg met de medezeggenschapsraad handelen.

Handtekening leerling	Handtekening ouders