passenderwijs
samenwerkingsverband primair onderwijs

Bijlage E

Algemene verordening gegevensbescherming (AVG)

Passenderwijs, 2020-2021

Professionals zijn zich steeds meer bewust van de ruimte in de wet voor het uitwisselen van persoonsgegevens in noodzakelijke situaties. Het doel van de uitwisseling is altijd in het belang van het kind. Van belang is dat professionals een bewuste, gewogen afweging maken. Naast wetgeving rondom privacy zijn tevens diverse beroepscodes van toepassing.

Stichting Passenderwijs dient te voldoen aan de Algemene Verordening Gegevensbescherming (AVG) die per 25 mei 2018 van toepassing is in de gehele Europese Unie (EU). Deze verordening stelt strengere eisen en voorwaarden dan de Wet bescherming persoonsgegevens (Wpb)die hiermee is komen te vervallen.

Passenderwijs dient passende technische en organisatorische maatregelen uit te voeren om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen in redelijkheid een passend beveiligingsniveau gelet op de risico's die verwerking van te beschermen gegevens met zich meebrengt. De maatregelen zijn ook gericht op het voorkomen van onnodige verzameling en verdere verwerking van persoonsgegevens.

Stichting Passenderwijs heeft dit document vanuit de volgende voorwaarden opgesteld:

- Passenderwijs dient in 2018 te voldoen aan Europese privacyregels
- Passenderwijs gaat bewust om met verwerking van leerling gegevens
- Het gebruik van leerling gegevens is noodzakelijk voor het uitvoeren van onze taken
- Voor gebruik van digitale diensten onder de 16 jaar is toestemming nodig
- Passenderwijs heeft een Functionaris Gegevensbescherming (FG) aangesteld.

Dit document begint met het privacyreglement. Hierin zijn uniforme afspraken vastgelegd rondom het uitwisselen en registreren van persoonsgegevens. Daarnaast heeft het reglement tot doel de rechten van betrokkenen te waarborgen. Als bijlage is een toelichting op het privacyreglement toegevoegd en veel gestelde vragen in het kader van privacy.
Vervolgens de bewustwording bij het gebruik van data en gegevens, dit is een praktische omschrijving welke regels/attitude minimaal van medewerkers verwacht wordt.
Daarna volgt de regeling ICT en informatiegebruik met bijlagen. Hierin zijn de kaders geschetst voor verwerking van privacygevoelige informatie en de bescherming van en omgang met deze gegevens. Ook hierbij het reglement met de taken en bevoegdheden van de Functionaris Gegevensbescherming (FG). Tot slot de toekomstige ontwikkeling van de AVG.

Het reglement is verbindend voor alle professionals, werkend in dienst of in opdracht van of op vrijwillige basis voor Passenderwijs. Hierbij wordt concreet gedacht aan het Loket, het Meerpartijenoverleg (MPO), de Centrale Toekenningscommissie (CTC) en het uitvoerende Regioteam van de Stichting Passenderwijs.

1 Privacyreglement Stichting Passenderwijs

Artikel 1 Begripsbepalingen

Dit reglement verstaat onder:	
Verwerker	de natuurlijke persoon of rechtspersoon, overheidsinstantie, dienst of nader orgaan dat persoonsgegevens verwerkt ten behoeve van de verwerkingsverantwoordelijke.
Betrokkene	de persoon op wie een persoonsgegeven betrekking heeft.
Regioteam	alle uitvoerende professionals, werkzaam voor het SWV Passenderwijs.
Meerpartijen overleg (MPO)	overleg waaraan de intern begeleider en Passenderwijs deelnemen. Op verzoek van de school kunnen aanvullende partijen worden uitgenodigd (schoolbegeleider, jeugdverpleegkundige, etc.).
Centrale Toekenningscommissie (CTC)	commissie die toelaatbaarheidsverklaringen en arrangementen extra ondersteuning toekent in opdracht van het SWV.
Persoonsgegevens	gegevens, herleidbaar tot een natuurlijk persoon.
Registratie	het geautomatiseerde systeem dat door het Regioteam wordt aangehouden, waarin persoonsgegevens zijn opgenomen van de personen genoemd in art. 4.
SWV	samenwerkingsverband Passenderwijs, verantwoordelijk bestuur van Stichting Passenderwijs.
Verwerkingsverantwoordelijke	het samenwerkingsverband, dat wil zeggen de rechtspersoon die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Artikel 2 Reikwijdte en doelstelling van het reglement

1. Dit reglement is van toepassing op alle persoonsgegevens van een betrokkene die door of namens Stichting Passenderwijs te Woerden worden verwerkt.
2. Dit reglement heeft tot doel:
   a) vast te stellen van welke personen het SWV persoonsgegevens verwerkt;
   b) te voorkomen dat persoonsgegevens worden verwerkt voor een ander doel dan het doel waarvoor ze zijn verzameld;
   c) de rechten van een betrokkene te waarborgen.
3. Binnen het SWV heeft de verwerking van persoonsgegevens specifiek ten doel als bron van informatie te dienen ten behoeve van beantwoording van en/of advisering ten aanzien van de hulpvraag neergelegd door de school, met toestemming van een wettelijk vertegenwoordiger/gezagdragend ouder bij het SWV.
4. In de CTC heeft de verwerking van persoonsgegevens de volgende doelen:
   a) als bron van informatie bij de toekenning van extra ondersteuning;
   b) als informatiebron bij behandeling van bezwaarschriftprocedures door de CTC, ten behoeve van adviseurs die daarbij betrokken worden;
   c) voor het voeren van procedures in geval van bezwaar tegen een besluit van de CTC op een bezwaarschrift en in geval van beroep.

Artikel 3 Toestemming

1. Een wettelijk vertegenwoordiger/gezagdragend ouder dient schriftelijk toestemming te verlenen om gegevens op te vragen bij derden, indien nodig.
2. Voor het bespreken van de onderwijsbehoefte van een kind met kernpartners (GGD, Jeugdhulp, Speciaal (Basis) Onderwijs, Schoolbegeleidingsdienst, Leerplicht etc.) is toestemming nodig van een wettelijke vertegenwoordiger/gezagdragend ouder.
3. Wanneer de bespreking van het kind niet binnen redelijke termijn na aanmelding bij het SWV plaatsvindt, dient het SWV opnieuw (schriftelijk) toestemming te vragen om het kind te bespreken.
4. In geval van diagnostisch of psychologisch onderzoek wordt, indien daartoe nog geen toestemming is verleend door de betrokkene(n), een aanvullende toestemmingsverklaring naar ouder(s)/verzorger(s) gestuurd.
5. Het SWV is bevoegd zonder toestemming van het kind dan wel diens wettelijk vertegenwoordiger persoonsgegevens betreffende de gezondheid van het kind te verwerken, ten behoeve van:
   a) het verdelen en toewijzen van ondersteuningsmiddelen en voorzieningen aan de scholen;
   b) het beoordelen of kinderen toelaatbaar zijn tot het speciaal (basis) onderwijs op verzoek van het bevoegd gezag van een school waar het kind is aangemeld of ingeschreven;
   c) het adviseren over de ondersteuningsbehoefte van een kind op verzoek van het bevoegd gezag van de school waar het kind is aangemeld of ingeschreven.

Artikel 4 Niet-anonieme casuïstiekbesprekingen

1. Persoonsgegevens worden alleen uitgewisseld als er een gerechtvaardigd doel aanwezig is, gelegen in het belang van het kind. Uitwisseling vindt alleen plaats onder deelnemers die de gegevens nodig hebben voor hun taakuitoefening.
2. Aan het casusoverleg nemen alleen die beroepskrachten deel die een directe behandelrelatie of adviesfunctie hebben met het kind dan wel uit hoofde van een specifieke taak of functie een vast teamlid zijn van het overleg.
3. Deelnemers bespreken de kindgegevens niet met anderen van buiten het SWV zonder toestemming van wettelijk vertegenwoordiger/gezagdragend ouder.
4. Indien de wettelijk vertegenwoordiger/gezagdragend ouder bezwaar maakt tegen bespreking van hun kind, worden hun bezwaren gewogen ten opzichte van het belang van het kind. Indien de conclusie is dat de belangen van het kind zwaarder wegen dan de bezwaren van de wettelijk vertegenwoordiger/gezagdragend ouder, dan worden de bezwaren van laatstgenoemden terzijde geschoven.
   Maar niet dan nadat de professional zijn voornemen om de bezwaren terzijde te schuiven heeft getoetst aan de hand van het ‘juridisch Zwitsers zakmes’ (zie bijlage voor toelichting). De professional motiveert en documenteert deze beslissing in het dossier van het kind.

Artikel 5 Verantwoordelijkheid van de bewerker

De bewerker van de registratie is verantwoordelijk voor de verwerking van de registratie overeenkomstig de bepalingen van de AVG. De Verwerkingsverantwoordelijke treft daartoe de nodige voorzieningen, waaronder in elk geval zodanige opslag van gegevens dat deze niet voor onbevoegden toegankelijk zijn.

Artikel 6 Categorieën van personen in de verwerking

In de registratie worden uitsluitend persoonsgegevens opgenomen over:

a) kinderen die voor advisering of ondersteuning door de school worden aangemeld bij het Loket van het SWV.
b) familieleden of andere personen uit de omgeving van deze kinderen, voor zover de gegevens in redelijkheid relevant zijn te achten, voor het beantwoorden van de hulpvraag en/of toekennen van het arrangement.

Artikel 7 Opnemen van gegevens

1. In alle gevallen worden in de registratie uitsluitend persoonsgegevens opgenomen die dienstig zijn ter verwezenlijking van het doel van de verwerking.
2. De Verwerkingsverantwoordelijke doet een mededeling aan de betrokkene(n) dat persoonsgegevens over de aanmelding en ten behoeve van de onderwijszorg worden geregistreerd.

Artikel 8 Soorten van gegevens

De volgende persoonsgegevens kunnen worden verwerkt:

a) NAW-gegevens (van kind en wettelijk vertegenwoordiger), nationaliteit en persoonsgebonden nummer;
b) gegevens betreffende gezondheid of welzijn van het kind voor zover die noodzakelijk zijn voor de ondersteuning;
c) gegevens betreffende de godsdienst of levensovertuiging van het kind voor zover die noodzakelijk zijn voor de ondersteuning;
d) gegevens betreffende de aard en het verloop van het onderwijs en ondersteuning, alsmede de behaalde resultaten;
e) gegevens ten dienste van het toekennen van ondersteuningsmiddelen of voorzieningen;
f) gegevens die de aanleiding voor aanmelding bij het SWV weergeven;
g) gegevens die de aard van de onderwijsbehoefte inzichtelijk maken;
h) gegevens die reeds ondernomen activiteiten van de school ten aanzien van het kind inzichtelijk maken;
i) opgestelde onderwijskundige rapporten en/of ontwikkelingsperspectief van het kind;
j) gegevens die door externe partijen wordt verstrekt en betrekking hebben op de ondersteuningsbehoefte waarmee het kind is aangemeld bij het SWV;
k) andere dan de onder a) t/m j) bedoelde gegevens waarvan de verwerking wordt vereist met het oog op de toepassing van een wettelijke regeling.

Artikel 9 Toegang tot gegevens

1. De Verwerkingsverantwoordelijke kan rechtstreekse toegang verlenen tot de in de verwerking opgenomen persoonsgegevens danwel persoonsgegevens verstrekken aan partijen die recht hebben op informatie m.b.t. het ondersteuningsproces van het kind.
2. De volgende functionarissen hebben rechtstreeks toegang tot de in de verwerking opgenomen persoonsgegevens
   a) de secretariële ondersteuning van het loket en de CTC (de bewerker);
   b) de begeleiders passend onderwijs om ondersteuning te kunnen uitvoeren;
   c) de coördinatoren van het Loket om ondersteuning te kunnen toekennen;
   d) de CTC om extra ondersteuning te kunnen toekennen.
3. De Verwerkingsverantwoordelijke kan eveneens rechtstreekse toegang verlenen tot de in de verwerking opgenomen persoonsgegevens danwel persoonsgegevens verstrekken aan diegene aan wie krachtens wettelijk voorschrift deze toegang dient te worden verleend, echter niet dan na deugdelijke legitimatie door diegene.

Artikel 10 Verstrekking van gegevens

1. De verantwoordelijke voor verwerking verstrekt persoonsgegevens uit de verwerking slechts aan anderen dan de in artikel 9 genoemde personen uitsluitend en voor zover:
   a) de verantwoordelijke daartoe op grond van enige wettelijke bepaling verplicht is;
   b) de betrokkene op wie de te verstrekken persoonsgegevens betrekking heeft of diens wettelijk vertegenwoordiger daarin heeft toegestemd.
2. De verantwoordelijke verstrekt persoonsgegevens, bedoeld in artikel 3 van dit reglement, niet aan derden, met uitzondering van het bevoegd gezag van de school waar het desbetreffende kind is aangemeld of ingeschreven.

Artikel 11 Beveiliging van gegevens

1. De Verwerkingsverantwoordelijke draagt zorg voor passende technische en organisatorische maatregelen ter voorkoming van verlies of onrechtmatige verwerking van persoonsgegevens. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau, gelet op de risico's die de verwerking en de aard van de te beschermen persoonsgegevens met zich meebrengen.
2. Bij elektronische verwerking van gegevens (groeidocument) wordt toegang verleend op basis van wachtwoordbeveiliging.
3. Een ieder die betrokken is bij de uitvoering van dit reglement en daarbij de beschikking krijgt over persoonsgegevens is verplicht tot geheimhouding daarvan. Dit geldt niet indien een wettelijk voorschrift tot bekendmaking verplicht.

Artikel 12 Inzagerecht betrokkene

1. Indien een betrokkene of diens wettelijk vertegenwoordiger(s) schriftelijk inzage verzoekt, stelt de coördinator de verzoeker binnen een maand na ontvangst van het schriftelijk verzoek, in de gelegenheid de registratie van de hem betreffende persoonsgegevens in te zien.
2. De coördinator kan weigeren aan het verzoek, bedoeld in het eerste lid, te voldoen, voor zover dit noodzakelijk is op grond van een wettelijk voorschrift of op grond van aanwijzingen gegeven door een daartoe bevoegd overheidsorgaan.

Artikel 13 Correctie van onvolledige of onjuiste gegevens

1. Verzoeken om verbetering, verwijdering of aanvulling van de in de verwerking opgenomen persoonsgegevens, worden schriftelijk ingediend door degene op wie de gegevens betrekking hebben of door zijn gemachtigde.
2. Gemachtigden dienen een schriftelijke machtiging over te leggen.
3. Aan de indiener van het in het eerste lid bedoelde verzoek wordt, na een besluit daartoe door of namens de werkgever van degene die de registratie heeft verricht, binnen een maand na de datum van indiening schriftelijk medegedeeld, of, en zo ja, welke verbetering, verwijdering of aanvulling heeft plaatsgevonden.

Artikel 14 Verzet tegen verwerking van gegevens

1. Wanneer de verwerking van persoonsgegevens plaatsvindt op basis van:
   a) noodzakelijkheid voor een goede vervulling van een door de verantwoordelijke verrichte publiekrechtelijke taak, of
   b) noodzakelijkheid voor een gerechtvaardigd belang van de verantwoordelijke of een derde

   kan betrokkene dan wel diens wettelijk vertegenwoordiger schriftelijk verzet aantekenen tegen de verwerking van de persoonsgegevens, op basis van zijn bijzonder persoonlijke omstandigheden.
2. De verantwoordelijke dient binnen een maand na ontvangst van het verzet te beoordelen of het verzet terecht is. Is dat het geval, dan dient de verwerking van persoonsgegevens onmiddellijk te worden beëindigd.

Artikel 15 Bewaartermijnen

1. De bewaartermijnen zijn van toepassing op verschillende groepen van persoonsgegevens binnen Passenderwijs: personeelsgegevens, leerlinggegevens in monitorinstrument, leerlinggegevens in groeidocument, gegevens leerlingbespreking, ruwe gegevens diagnostiek. De bewaartermijn wordt bepaald volgens wettelijke bepalingen en het principe 'niet langer dan nodig'.

2. De volgende bewaartermijnen zijn vastgesteld:
   a) bewaartermijn van personeelsgegevens in het personeelsdossier van medewerkers bedraagt 2 jaar na het moment van uitdiensttreding;
   b) bewaartermijn gegevens sollicitanten: vernietiging na vervulling vacature
   c) bewaartermijn van gegevens in het monitorinstrument bedraagt 1 volledig schooljaar na het schooljaar van vertrek uit het samenwerkingsverband, de monitor van de voorgaande ondersteuningsplanperiode* zal geanonimiseerd worden en voor analyses gebruikt worden, per planperiode komt er een nieuwe monitor;
   d) bewaartermijn van gegevens in het groeidocument (Parantion) bedraagt 1 volledig schooljaar na het schooljaar van vertrek uit het samenwerkingsverband;
   e) bewaartermijn van gegevens uit leerlingbesprekingen bedraagt 1 volledig schooljaar na het schooljaar van bespreking;
   f) bewaartermijn van ruwe testgegevens bedraagt 2 volledige schooljaren na het schooljaar van afname;
   g) bewaartermijn van IQ-verslagen bedraagt 3 jaar.
   h) bewaartermijn van een toelaatbaarheidsverklaring bedraagt 1 schooljaar na afloop van de TLV.
3. Voor medewerkers die gebonden zijn aan een beroepscode gelden de bepalingen die zijn opgenomen in deze code.
4. Het besluit en de uitvoering van verwijdering vindt jaarlijks in september plaats en heeft betrekking op het voorgaande schooljaar.

Artikel 16 Slotbepalingen

1. Dit reglement kan aangehaald worden als *'Privacyreglement Stichting Passenderwijs'* en treedt in werking op 1 april 2017.
2. Het samenwerkingsverband maakt het reglement (digitaal) openbaar.

* Ondersteuningsplanperiode is de periode van 4 jaar van het ondersteuningsplan. Het wettelijk verplichte Ondersteuningsplan geeft richting aan de wijze waarop Passenderwijs haar opdracht binnen de wet Passend Onderwijs invulling geeft. Deze beleidsdocumenten zijn de basis voor al het handelen van het samenwerkingsverband. De documenten zijn bestuurlijk vastgesteld voor 4 jaar. Binnen het Op Overeenstemming Gericht Overleg (OOGO) hebben de bevoegde wethouders van de betrokken gemeenten akkoord gegeven en heeft ook de Ondersteuningsplanraad (OPR) instemming verleend. Aan het eind van het schooljaar worden alle tussentijdse wijzigingen uit de voortgangsparagraaf gewijzigd in het Ondersteuningsplan. Een update wordt aan het begin van het schooljaar op de website geplaatst.

Bijlage Relevante toelichting op het privacyreglement

Gegevensdeling zonder vooraf informatie te verstrekken aan wettelijke vertegenwoordiger(s)

Er kunnen zich omstandigheden voordoen die het noodzakelijk maken, gezien het belang van het kind, dat zijn situatie wordt besproken zonder dat de wettelijk vertegenwoordiger/ gezagdragend ouder daarover van te voren is geïnformeerd. Dit geschiedt conform de zorgvuldigheidseisen van 'Afweging 3' uit het 'Instrument samenwerken in de Jeugdketen. Een instrument voor gegevensuitwisseling van het Ministerie van VWS.
Dit betekent dat de professional een gerechtvaardigd doel moet hebben om niet de wettelijk vertegenwoordiger/gezagdragend ouder van te voren te informeren. Dat doel moet vervolgens worden getoetst aan het 'juridisch Zwitsers zakmes'

Uitgelicht: **Juridisch Zwitsers zakmes**

Bij het 'juridisch Zwitserszakmes' gaat het om toepassing van eisen van subsidiariteit, proportionaliteit en doelmatigheid:

Subsidiariteit	:	het gaat er om dat het minst ingrijpende actie wordt genomen
Proportionaliteit	:	het gaat er om dat de actie in verhouding staat tot het doel
Doelmatigheid	:	het gaat er om dat de gekozen actie de meest geschikte handelwijze is

Belangrijke regels:

- Vertel welke gegevens u met wie wilt delen. De AVG bepaalt dat iedereen het recht heeft om te weten wat er waar over hem/haar vast ligt en wat er tussen wie wordt uitgewisseld. Iemand dient altijd geïnformeerd te worden.
- Vraag alleen toestemming wanneer je 'nee' kunt accepteren.
- Weeg de bezwaren van ouders af tegen het belang van het kind.
  De principes van subsidiariteit, proportionaliteit en doelmatigheid spelen hierbij een rol.

Welke onderzoeksgegevens over de leerling mogen scholen delen met het SWV met en zonder toestemming van de ouders? (bron: www.passendonderwijs.nl, website ministerie)

Om te beoordelen welke plek voor een kind het meest passend is, heeft het SWV een aantal gegevens over de leerling nodig. Deze gegevens worden (onder andere) verzameld via onderzoek.

Resultaten van onderzoek welke de school ZONDER TOESTEMMING van ouders mag delen met het samenwerkingsverband
Onderzoek dat door de leraren en intern begeleiders zelf wordt uitgevoerd, zoals lesobservaties en informatie uit het leerlingvolgsysteem.

Resultaten van onderzoek welke de school NIET ZONDER TOESTEMMING van ouders mag delen met het samenwerkingsverband
Onderzoek dat door gedrags- en opvoeddeskundigen (al dan niet in dienst van de school) wordt uitgevoerd, zoals een orthopedagoog of psycholoog. Denk bijvoorbeeld aan het afnemen van een IQ-test bij de leerling.

Aanvullende informatie uitwisseling gegevens (bron: handreiking gegevensuitwisseling, Nederlands Jeugdinstituut, 2016)

- ✓ Voor schriftelijke of mondelinge uitwisseling van gegevens gelden dezelfde regels
- ✓ Anoniem advies vragen is mogelijk indien casus niet tot de persoon herleidbaar is
- ✓ Als toestemming voor uitwisseling van gegevens wordt geweigerd, dan alleen uitwisselen op basis van publiekrechtelijke taak school of gerechtvaardigd belang van school of derde, hierbij hebben ouders het recht bezwaar aan te tekenen
- ✓ Levensbedreigende situatie? Gegevensuitwisseling op grond van vitaal belang kind
- ✓ Gegevensuitwisseling alleen met die partijen die nodig zijn om het doel van de gegevensuitwisseling te bereiken
- ✓ Persoonsgegevens van geheimhouders verkrijgen is alleen mogelijk met toestemming of indien sprake is van 'conflict van plichten' of 'goed hulpverlenerschap'.

2. Bewustwording bij bewerking en gebruik van data en gegevens

Passenderwijs heeft inhoudelijke afspraken gemaakt over:

- Procedure meldplicht datalekken
- Verwerkersovereenkomsten leveranciers
- Toestemming voor gebruik foto's en video's
- Beveiligingsvoorschriften bij het bewust handelen inzake gebruik en bewerking van gegevens
- Waar data van de organisatie mag staan
- Risico-situaties waarin de medewerker verantwoordelijkheid draagt

Wanneer u hier meer informatie over wenst kunt u contact opnemen via info@passenderwijs.nl.

3. Regeling ICT, informatiegebruik en protocol datalekken St. Passenderwijs

In het onderwijs wordt steeds vaker locatie onafhankelijk gewerkt. Medewerkers werken steeds vaker op een laptop of ander flexibel device. Dit brengt voor Passenderwijs nieuwe mogelijkheden maar ook risico's en verplichtingen met zich mee. Passenderwijs is ervoor verantwoordelijk dat de apparaten waarop medewerkers werken professioneel beveiligd zijn. Dit komt onder andere doordat de AVG van organisaties eist dat persoonsgegevens adequaat beveiligd worden. Concreet betekent dit dat ieder apparaat waarop gewerkt wordt voor de organisatie beheerd en beveiligd moet worden. Passenderwijs realiseert dit middels het gebruik van Microsoft Intune, een clouddienst voor het beheren van bedrijfsmobiliteit (Enterprise Mobility Management, EMM) die werknemers in staat stelt om productief te zijn terwijl zakelijke gegevens veilig blijven.

Artikel 1 Begripsbepalingen

In deze regeling wordt verstaan onder:	
organisatie	het geheel van de organisatie, waaronder ook begrepen het bestuur en de medezeggenschapsraad;
bestuurder	het bestuur van Stichting Passenderwijs;
directeur	degene belast met de dagelijkse leiding van de organisatie;
medewerker	personeelslid of medewerker die op arbeidsovereenkomst of anderszins betaalde of niet betaalde werkzaamheden voor de organisatie verricht;
ICT-middelen	alle elektronische informatie- en communicatie faciliteiten en ICT-apparatuur, door of namens de organisatie aan medewerkers beschikbaar gesteld, alsmede de privé ICT-middelen indien en voor zover zij gebruikt worden op de werkplek en of voor de uitvoering van de door of namens de directeur opgedragen taken;
ICT-apparatuur	elektronische informatie- en communicatiemiddelen, inclusief alle bijbehorende hard- en software en bestanden;
functionaris gegevensverwerking	door het bestuur aangewezen aanspreekpunt voor gegevensverwerking;
Informatie van de organisatie	alle bestanden en informatie van de organisatie door of namens de directie aan medewerkers beschikbaar gesteld, hieronder begrepen informatie van ketenpartners;
beveiligingsincident	gebeurtenis die een bedreiging vormt of kan vormen voor de vertrouwelijkheid, integriteit of beschikbaarheid van gegevens;
beveiligingsclassificatie	overzicht van de risicoklassen van bestandsgegevens;
privé-bestand	bestand met een geheel of overwegend persoonlijke inhoud;
privé ICT-middelen	ICT apparatuur in eigendom van medewerker zelf of anderszins verkregen, zonder dat deze door of namens de algemeen directeur beschikbaar is gesteld;
persoonsgegeven	elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van de Wet bescherming persoonsgegevens;

verwerken van persoonsgegevens	elke handeling of geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
verkeersgegevens	gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan;
bestand	elk gestructureerd geheel van organisatie- of persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen of eenheden.

Artikel 2 Reikwijdte

1. Deze regeling is voor alle medewerkers van toepassing op het gebruik van ICT-middelen en informatie van de organisatie, ongeacht de plaats waar dit plaatsvindt en ongeacht het eigendom van de middelen waarmee informatie wordt benaderd.
2. Tevens is deze regeling van toepassing op de wijze waarop controle op dit gebruik plaatsvindt en op het verwerken van persoonsgegevens in dit kader.

Artikel 3 Gebruik van ICT-middelen en informatie van de organisatie

1. Medewerkers gebruiken de ICT-middelen en informatie van de organisatie primair en hoofdzakelijk voor het uitvoeren van de aan hen door de directeur opgedragen taken, in overeenstemming met wet- en regelgeving en het doel waarvoor de middelen en informatie zijn verstrekt.
2. Het is medewerkers verboden om ICT-middelen van de organisatie aan een ander ter beschikking te stellen. Informatie van de organisatie mag slechts verstrekt worden aan daartoe geautoriseerde anderen.
3. De ICT-middelen en informatie van de organisatie worden beschikbaar gesteld voor zakelijk gebruik. Privégebruik van informatie van de organisatie en bestanden is niet toegestaan.
4. Gebruik van de ICT-middelen of informatie van de organisatie voor commerciële doeleinden is niet toegestaan.
5. Het is medewerkers toegestaan gebruik te maken van privé ICT-middelen voor de uitvoering van de hen opgedragen taken, mits de medewerkers zich hierbij houden aan de bepalingen van deze regeling en bevoegd zijn tot de voor de uitvoering van deze regeling noodzakelijke maatregelen.
6. Het is medewerkers niet toegestaan om de ICT-middelen of informatie van de organisatie te gebruiken voor illegale doeleinden danwel het opvragen, versturen, vastleggen of anderszins verwerken van materiaal of informatie die naar algemeen maatschappelijke opvattingen als lasterlijk, beledigend, aanstootgevend of oneervol wordt beschouwd.
7. Medewerkers dienen de gestelde beveiligingseisen ten aanzien van ICT-middelen en informatie van de organisatie in acht te nemen.
8. Medewerkers dienen schade aan, verlies of diefstal van ICT-middelen of informatie van de organisatie onverwijld bij de leidinggevende te melden.

Artikel 4 Toegang tot en beveiliging van informatie van de organisatie

1. De medewerker verschaft zich uitsluitend toegang tot die gegevens waartoe hij geautoriseerd is.
2. Het is de medewerker verboden om anderen dan daartoe geautoriseerde medewerkers toegang tot informatie van de organisatie te verlenen.
3. De medewerker neemt passende technische en organisatorische maatregelen om informatie van de organisatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. De medewerker houdt hierbij in ieder geval rekening met:
    a. de beveiligingsclassificatie (zie bijlage A)van de informatie;
    b. de door de organisatie gestelde beveiligingsvoorschriften;
    c. aan de werkplek verbonden risico's;
    d. het risico door het benaderen van informatie van de organisatie met andere dan door de organisatie verstrekte of goedgekeurde ICT-apparatuur.
4. De medewerker dient geconstateerde of vermoede beveiligingslekken en beveiligingsincidenten onverwijld te melden bij de functionaris gegevensverwerking.
5. In geval van dringende redenen kan de directeur, of bij diens afwezigheid de functionaris gegevensverwerking, dan wel de voorzitter van het bestuur besluiten tot het nemen van noodmaatregelen voor de gegevensverwerking.
6. De medewerker is verplicht advies of ondersteuning van de leidinggevende of de functionaris gegevensverwerking te vragen indien de medewerker onvoldoende in staat is de beveiligingsvoorschriften uit te voeren of te beoordelen.

Artikel 5 Controle

1. Controle door of in opdracht van de algemeen directeur op het gebruik van de ICT-middelen en informatie van de organisatie vindt slechts plaats in het kader van de in artikel 7, eerste lid, genoemde doeleinden.
2. Controle ter verkrijging van inzicht in de mate van gebruik van de ICT-middelen en informatie van de organisatie wordt beperkt:
    a) tot de verkeersgegevens, die betrekking hebben op tijd, hoeveelheid, omvang en dergelijke.
    b) zodat deze in redelijke verhouding staat tot het doel waarvoor deze wordt aangewend.
3. De controle vindt in beginsel geanonimiseerd en slechts steekproefsgewijs plaats.
4. Controle in het kader van het beheer van de toegang tot de systemen en het beveiligen van het systeem en het netwerk voor het tegengaan van virussen en andere schadelijke programma's vindt op geautomatiseerde wijze plaats.
5. Onrechtmatig gebruik dan wel misbruik van de ICT-middelen en informatie van de organisatie wordt zo veel mogelijk softwarematig onmogelijk gemaakt.
6. Controle beperkt zich tot autorisatie- en verkeersgegevens van het gebruik van de ICT-middelen of informatie van de organisatie, alleen bij zwaarwegende redenen kan er controle op de inhoud plaatsvinden. Privé-bestanden worden hierbij zoveel mogelijk ontzien.
7. De medewerker die voor de uitvoering van de door de algemeen directeur opgedragen taken gebruik maakt van privé ICT-middelen is verplicht mee te werken aan eventuele controles volgens dit artikel. Hierbij worden de regels van dit artikel in acht genomen.
8. Indien een medewerker wordt verdacht van het overtreden van deze regeling, kan gedurende een vastgestelde periode gerichte controle plaatsvinden. Deze gerichte controle wordt slechts uitgevoerd nadat de medewerker is ingelicht dat signalen hierover zijn ontvangen en om zijn reactie is gevraagd.
9. Indien geconstateerd wordt dat een medewerker zich niet houdt aan de bepalingen van deze regeling, wordt de betrokken medewerker zo spoedig mogelijk hierop aangesproken door zijn leidinggevende.

10. Het gebruik van ICT-middelen en informatie van de organisatie door bestuursleden, de Medezeggenschapsraad en andere medewerkers met een vertrouwensfunctie, is in beginsel uitgesloten van controle. Dit geldt niet voor de controle op de veiligheid van het elektronische verkeer, voor de overzichten als genoemd in het achtste lid en voor informatie die geen verband houdt met genoemde functies of lidmaatschappen.

Artikel 6 Sancties

1. Medewerkers kunnen disciplinair worden bestraft volgens de regels die vastgelegd zijn in de CAO.
2. Vrijwilligers en andere medewerkers die niet onder de CAO vallen, en deze regeling niet naleven, mogen, al dan niet tijdelijk, geen ICT-middelen en informatie van de organisatie gebruiken, onverminderd de bevoegdheid van de algemeen directeur de contractuele relatie te beëindigen.

Artikel 7 De verwerking van persoonsgegevens van medewerkers

1. De verwerking van persoonsgegevens inzake het gebruik van ICT-middelen en informatie van de organisatie heeft de volgende doeleinden:
    a) het verkrijgen van inzicht in de aard en mate van het gebruik van de ICT-middelen en informatie van de organisatie;
    b) het voorkomen van onrechtmatig gebruik dan wel misbruik van de ICT-middelen en informatie van de organisatie;
    c) het beveiligen van het systeem en het netwerk;
    d) het beschermen van de privacy van de medewerkers op de werkplek;
    e) het beschermen van de integriteit en goede naam van de organisatie;
    f) het beheer van ICT-middelen en toegang tot informatie van de organisatie;
    g) kostenbeheersing van het gebruik van ICT-middelen.
2. Van medewerkers kunnen de navolgende persoonsgegevens worden verwerkt inzake het gebruik van informatie van de organisatie of ICT-middelen:
    a) geautomatiseerd verkregen logging-gegevens;
    b) naam en zakelijke persoonsgegevens bij incidentmeldingen;
    c) adresgegevens van de externe of mobiele werkplek;
    d) autorisatiegegevens;
    e) informatie over ter beschikking gestelde ICT-middelen en informatie van de organisatie;
    f) informatie over het gebruik van ICT-middelen en informatie van de organisatie;
    g) kosten van het gebruik van ICT-middelen.
3. Het bestuur treft maatregelen zodat verwerking van persoonsgegevens juist en nauwkeurig plaatsvindt.
4. Wat betreft bewaartermijnen wordt verwezen naar artikel 15 van het privacy document van Stichting Passenderwijs.
5. Indien de functionaris die belast is met het beheer van de bestanden delen niet kan verwijderen, wordt onder verwijderen verstaan het niet meer verstrekken van deze gegevens voor de in het eerste lid geformuleerde doeleinden.

Artikel 8 Rechten van de medewerker

1. De medewerker heeft het recht om een kopie van een overzicht te ontvangen van de hem betreffende persoonsgegevens die worden verwerkt. De medewerker kan daartoe een schriftelijk verzoek indienen bij de algemeen directeur.
2. Indien de betreffende persoonsgegevens feitelijk onjuist, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt, kan de medewerker de algemeen directeur schriftelijk verzoeken deze te verbeteren, aan te vullen, te verwijderen of af te schermen. Het verzoek bevat de aan te brengen wijzigingen.

3. Het bestuur bericht de medewerker binnen vier weken na ontvangst van het in het tweede lid genoemde verzoek schriftelijk of, dan wel in hoeverre, hij daaraan voldoet. Een weigering is met redenen omkleed.
4. De algemeen directeur draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.

Artikel 9 Onvoorziene omstandigheden

In gevallen waarin deze regeling niet voorziet of bij twijfel over de toepasselijkheid van deze regeling, beslist de algemeen directeur.

Artikel 10 Openbaarmaking

De algemeen directeur stelt de medewerkers die gebruik maken van de ICT- middelen en informatie van de organisatie op de hoogte van deze regeling.

Artikel 11 Citeertitel en inwerkingtreding

1. Deze regeling wordt aangehaald als: *regeling ICT en informatiegebruik en protocol datalekken Stichting Passenderwijs.*
2. Deze regeling treedt na bestuurlijke vaststelling in oktober 2017 in werking.

Bijlage A Uitwerking classificatieniveau data

Classificatieniveau	Vertrouwelijkheid	Waar	Voorbeelden
Geen	Openbaar	Geen restrictie	ondersteuningsplan, nieuwsbrief, website etc.
Laag	Bedrijfsvertrouwelijk	Werk PC, werkarchief, privé PC	algemene vergaderstukken, personeelsbeleid, diverse formats etc.
Midden	Vertrouwelijk	Werk PC, Office 365, Parantion, beveiligde USB-stick verstrekt door de organisatie	algemene registratiegegevens, casuistiekbespreking etc.
Hoog	Geheim	Werk PC, Office 365, Parantion, beveiligde USB-stick verstrekt door de organisatie	dossiergegevens personeelsleden, persoonlijke gegevens ondersteuningstrajecten, loketbesprekingen, groeidocumenten etc.

Bijlage B Beveiligd e-mailen van bijlagen met persoonlijke content

Ter bevordering van het veilig e-mailen van bestanden naar externen is een richtlijn geformuleerd. Intern is de veiligheid geborgd middels het delen van bestanden binnen Outlook 365 en het gebruik van de share-point omgeving.

Bijlage C Verwerkersovereenkomst inzake geheimhouding en verwerking van persoonsgegevens

Ondergetekenden

Stichting Passenderwijs, statutair gevestigd te Woerden, in deze vertegenwoordigd door ……. in zijn hoedanigheid van algemeen directeur

Hierna te noemen: Opdrachtgever

en

……., statutair gevestigd te ……., in deze vertegenwoordigd door ……. ……..in zijn hoedanigheid van ……;

Hierna te noemen: Opdrachtnemer

Overwegende dat:

- opdrachtnemer voor opdrachtgever werkzaamheden en/of diensten verricht
- opdrachtgever daartoe aan opdrachtnemer gegevens gaat verstrekken
- deze gegevens vertrouwelijk zijn, althans vertrouwelijk behandeld dienen te worden
- deze gegevens persoonsgegevens kunnen bevatten
- deze gegevens voor opdrachtnemer noodzakelijk zijn om overeengekomen werkzaamheden of diensten uit te voeren

Komen het volgende overeen:

Artikel 1 Onderwerp van de overeenkomst

a) de levering van gegevens door opdrachtgever aan opdrachtnemer
b) het maken van geheimhoudingsafspraken daaromtrent en
c) het maken van verdere afspraken als deze gegevens ook persoonsgegevens bevatten.

Artikel 2 Geheimhouding

1. De van opdrachtgever verkregen gegevens zullen door opdrachtnemer niet aan derden worden verstrekt, tenzij door de opdrachtgever schriftelijk toestemming is verleend, of het voor de uitvoering van de werkzaamheden noodzakelijk is.
2. Opdrachtnemer draagt er zorg voor dat de gegevens aan personeel van betrokken partijen alleen op ‘need-to-know’ basis worden verstrekt, en dat de gegevens alleen worden verstrekt aan personeel dat belast is met het uitvoeren van de overeengekomen werkzaamheden of diensten.
3. Gedurende de periode dat opdrachtnemer de hiervoor bedoelde gegevens onder zich heeft, dient zij de opslag van de gegevens adequaat te beveiligen. In ieder geval zodanig dat derden die niet belast zijn met de uitvoering van overeengekomen werkzaamheden of diensten, geen toegang hebben tot de gegevens. Deze opslag dient daarnaast te voldoen aan relevante regelgeving zoals de Wet bescherming persoonsgegevens indien er persoonsgegevens worden uitgewisseld.

Artikel 3 Persoonsgegevens

1. Indien de gegevens ook persoonsgegevens betreffen, gelden de hierna volgende bepalingen van dit artikel. Opdrachtnemer wordt door partijen beschouwd als de ‘verwerker’, en opdrachtgever als de ‘Verwerkingsverantwoordelijke’, als bedoeld in de AVG.

2. Opdrachtnemer zal in het kader van de uitvoering van de overeengekomen werkzaamheden en diensten de gegevens ten behoeve van opdrachtgever verwerken, waarbij het opdrachtnemer niet is toegestaan de van opdrachtgever verkregen gegevens voor eigen doeleinden, anders dan overeengekomen, te verwerken en/of aan derden te verstrekken.
3. Partijen zullen zorgdragen voor de naleving van de toepasselijke wet- en regelgeving, waaronder in ieder geval begrepen wet- en regelgeving op het gebied van de bescherming van persoonsgegevens, zoals de Wet bescherming persoonsgegevens.
4. Opdrachtnemer legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.
5. Opdrachtgever is te allen tijde gerechtigd om gedurende de uitvoering van de overeenkomst de hiervoor genoemde maatregelen door een onafhankelijke deskundige te laten toetsen door middel van een audit. De kosten voor deze audit zijn voor opdrachtgever.
6. Opdrachtnemer mag in het kader van deze overeenkomst gebruik maken van een derde, zonder voorafgaande toestemming van opdrachtgever, op de voorwaarde dat opdrachtnemer met de derde gelijksoortige afspraken als in deze overeenkomst vervat, schriftelijk vastlegt.
7. Indien Opdrachtnemer vermoedt, of te weten is gekomen, dat de persoonsgegevens van opdrachtgever gecompromitteerd zijn (datalek), of zijn geweest, meldt opdrachtnemer dit onmiddellijk aan opdrachtgever.
8. In het geval dat een betrokkene een verzoek omtrent inzake, correctie of verwijdering richt aan opdrachtnemer, zal opdrachtnemer het verzoek doorsturen aan opdrachtgever, en zal opdrachtgever het verzoek verder afhandelen. Opdrachtnemer mag de betrokkenen daarvan op de hoogte stellen.

Artikel 4 Overige bepalingen

1. Deze overeenkomst duurt voort zolang opdrachtnemer werkzaamheden en/of diensten voor opdrachtgever levert.
2. Op deze overeenkomst is Nederlands recht van toepassing. Geschillen voortvloeiende uit deze overeenkomst worden voorgelegd aan de bevoegde rechter in het arrondissement waar Opdrachtgever gevestigd is.

Voor akkoord,

Naam en handtekening verantwoordelijk voor de opdrachtgever

Naam en functie : ……., algemeen directeur Stichting Passenderwijs
Plaats en datum : Woerden, ……

Ondertekening :

Naam en handtekening verantwoordelijk voor de opdrachtnemer

Naam en functie : ……., …….
Plaats en datum : ……., …….

Ondertekening :

Bijlage D Functieomschrijving Functionaris Gegevensbescherming (FG)

Passenderwijs heeft een interne toezichthouder op de verwerking van persoonsgegevens aangesteld. Deze functie is als taak opgenomen in de normjaartaak van één van de medewerkers van Stichting Passenderwijs. De FG houdt toezicht op de uitvoering van de dataregeling van Stichting Passenderwijs.

Taken functionaris gegevensverwerking

- meldingen van gegevensverwerkingen bijhouden;
- vragen en klachten van mensen binnen en buiten de organisatie afhandelen;
- interne regelingen ontwikkelen;
- adviseren over technologie en beveiliging (*privacy by design*);
- input leveren bij het opstellen of aanpassen van een gedragscode.

Eisen die de wet aan de FG stelt

- De functionaris moet een natuurlijk persoon zijn.
- De functionaris moet voldoende kennis hebben van de organisatie en de privacywetgeving.
- De functionaris moet betrouwbaar zijn (geheimhoudingsplicht)

Bevoegdheden FG

- De functionaris heeft geen formele sanctiebevoegdheden maar wel bevoegdheden tot controle. Zo moet een FG bevoegd zijn om ruimtes te betreden, zaken te onderzoeken en inlichtingen en inzage te vragen.
- De functionaris moet in onafhankelijkheid zijn werkzaamheden kunnen verrichten binnen een organisatie.

Aanstellen FG

De functionaris dient door Passenderwijs aangemeld te worden bij de Autoriteit Persoonsgegevens. Pas dan kan de functionaris aan de slag.
De aanmelding vindt plaats middels aanmelding via de site van de Autoriteit Persoonsgegevens.

Beroepsvereniging FG

De functionaris kan lid worden van het Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG).

Bijlage E Reglement met taken en bevoegdheden Functionaris Gegevensbescherming

Begripsbepaling

Begrip	*Definitie*
AVG	Algemene Verordening Gegevensbescherming
FG	functionaris voor gegevensbescherming artikel 37 AVG
Verwerkingsverantwoordelijke	het bestuur van Stichting Passenderwijs
Verwerker	een natuurlijke persoon of rechtspersoon, overheidsinstantie, bedrijf, organisatie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt
Persoonsgegevens	alle informatie over een identificeerbare natuurlijke

	persoon (betrokkene) waarbij als identificeerbaar wordt beschouwd een natuurlijk persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals naam, identificatienummer, online identificator of van elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon
Verwerking van persoons gegevens	bewerking van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedures, zoals het verzamelen, vastleggen, ordenen, bijwerken of wijzigen, opvragen, raadplegen, verspreiden, verstrekken door middel van doorzending of op andere wijze ter beschikking stellen, afschermen, wissen of vernietigen van gegevens
Personeel	medewerkers in loondienst en/of extern ingehuurd die in opdracht van de Verwerkingsverantwoordelijke werkzaamheden verrichten

Artikel 1 Taken

1. De FG heeft de volgende taken:
    a) het houden van toezicht op verwerkingen van persoonsgegevens;
    b) toezicht op wijzigingen in bestaande verwerkingen en/of het aanleggen van nieuwe verwerkingen met persoonsgegevens binnen Stichting Passenderwijs;
    c) geven van (ongevraagd) advies en doen van aanbevelingen over privacy in het algemeen en de toepassing van de AVG;
    d) overleg met (de contactpersoon van) de Autoriteit Persoonsgegevens;
    e) organiseren, inrichten en/of onderhouden van het verwerkingsregister (dataregister) met alle verwerkingen persoonsgegevens binnen Stichting Passenderwijs;
    f) het (laten) afhandelen van klachten inzake privacy;
    g) overige door het bestuur of directie van Stichting Passenderwijs aan de FG opgedragen werkzaamheden aangaande privacy.
2. Het personeel meldt bij de FG alle (nieuwe) verwerkingen van persoonsgegevens alsmede eventuele incidenten met betrekking tot privacy.

Artikel 2 Bevoegdheden

1. De FG is bevoegd, zo nodig met medeneming van de benodigde apparatuur, elke plaats in de gebouwen op de terreinen die bij Stichting Passenderwijs in gebruik zijn en waar persoonsgegevens worden verwerkt, te betreden.
2. De FG is bevoegd inlichtingen te vorderen van een ieder die onder gezag of in opdracht van Stichting Passenderwijs werkzaam is of overeenkomstig voor of namens Stichting Passenderwijs persoonsgegevens verwerkt.
3. De FG is bevoegd inzage te vorderen van zakelijke gegevens en bescheiden waarin persoonsgegevens zijn verwerkt.
4. De FG is bevoegd van de gegevens en bescheiden kopieën te maken.
5. Indien het maken van kopieën niet ter plekke kan gebeuren, is hij bevoegd de gegevens en bescheiden voor de duur van maximaal één werkdag mee te nemen.
6. De FG is bevoegd tot het geven van een opdracht tot
    a) het aanmaken van een registratie van persoonsgegevens in overeenstemming met de AVG;
    b) vernietiging van persoonsgegevens, waarvan de bewaartermijn is overschreden of indien de gegevensverwerking onrechtmatig is;

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

Artikel 3 Weigering

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

Artikel 4 Geheimhouding

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

Artikel 5 Vaststelling

1. Deze regeling wordt vastgesteld en gewijzigd bij besluit van de Verwerkingsverantwoordelijke.
2. Deze regeling treedt in werking op 8 mei 2018 en zal intern aan het personeel bekend worden gemaakt door publicatie in het ‘handboek personeel’.

Namens het bestuur van Stichting Passenderwijs,

Dhr. E. Blankestijn
Voorzitter bestuur

4. Toekomstige ontwikkeling ten behoeve van AVG

Bovenliggend document is in schooljaar 2018-2019 beoordeeld door de heer B. Dasselaar, juridisch adviseur bij Groenendijk Consultancy. Het document is op een paar punten aangepast en ontwikkelpunten zijn doorgenomen. Het geheel voldoet aan de Algemene Verordening Gegevensbescherming.
Een certificering ontvangen dat men aan de AVG voldoet is nog niet mogelijk, mocht de Raad voor accreditatie (RvA) instellingen hiervoor accrediteren wordt dit gepubliceerd op de website www.autoriteitpersoonsgegevens.nl.

Blijvende ontwikkeling

Organisaties die persoonsgegevens verwerken moeten altijd in de gaten houden of de gegevensverwerking verandert en wat dat betekent voor de mensen van wie de persoonsgegevens zijn. Ook kan het zijn dat de stand van de techniek verandert, waardoor bijvoorbeeld beveiligingsinstellingen aangepast moeten worden aan de nieuwste ontwikkelingen.