stichting invitare openbaar onderwijs nodigt uit...

Privacy-beleid

Opgesteld door	: werkgroep veiligheid (versie 4)
Ingestemming GMR met 4e concept	: 27 juni 2019, aangevuld 26 januari 2022 en 13 april 2022
Vastgesteld door CvB op	: 13 april 2022
Te evalueren in	: schooljaar 2023/24

Inhoudsopgave

1. Inleiding

Privacy is een thema dat al veel langer speelt, maar door de digitalisering en de sociale media is de aandacht de laatste jaren geïntensiveerd. Privacy is geregeld in onze wetgeving. Belangrijker is het om te realiseren dat privacy per definitie een aspect is van de sociale veiligheid. Leerlingen en medewerkers hebben recht op een veilige (digitale) leer- dan wel (digitale) werkomgeving. Stichting Invitare en haar scholen gaan zorgvuldig om met de persoonsgegevens van leerlingen en medewerkers. Zij zijn open naar ouders / verzorgers en medewerkers welke persoonsgegevens ze op welke wijze verwerken en welke rechten de ouders / verzorgers en medewerkers daarbij hebben.

Privacy gaat niet alleen over gedigitaliseerde systemen zoals de leerlingenadministratie of het leerlingvolgsysteem, het gaat ook over gedrag van medewerkers, vrijwilligers en studenten en tevens de experts en ondersteuners waar we mee samenwerken. Invitare realiseert zich dat ook ouders/verzorgers een rol spelen in het beschermen van de privacy van leerlingen. Hoe gaan zij bijvoorbeeld om met beeldmateriaal die zij in en om de school maken? Privacy, sociale veiligheid en dus ook veiligheid is een gezamenlijke verantwoordelijkheid van alle medewerkers èn alle mensen waar wij mee communiceren en samenwerken.

2. Wetgeving en Beleid Invitare

Op 25 mei 2018 is de (Europese) Algemene Verordening Gegevensbescherming van kracht geworden. Vanaf deze datum is de Wet Bescherming Persoonsgegevens niet meer van kracht.

In het voorliggende beleidsdocument gaan we in op de rechten van medewerkers en leerlingen en als afgeleide die van hun ouders / verzorgers. Het beleid heeft tot doel:

- De persoonlijke levenssfeer van de leerlingen en medewerkers te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens;
- Vast te stellen welke persoonsgegevens de scholen en de stichting als geheel verwerken en met welk doel zij dit doen;
- De zorgvuldige verwerking van persoonsgegevens te waarborgen;
- De rechten van ouders / verzorgen, leerlingen en medewerkers inzake privacy te waarborgen.

3. Privacyreglement

VOS ABB heeft Wille Donker advocaten opdracht gegevens een model 'Privacyreglement" op te stellen rekening houdend met de nieuwe wetgeving. Het betreffende reglement hebben wij op een paar beperkte punten passend gemaakt voor Invitare. Het door ons aangepaste reglement is opgenomen als *bijlage 1*. Het document behandelt de registratie van personeel en leerling gerelateerde gegevens en -correspondentie zoals geïnventariseerd in *bijlage 2*.

4. Beveiliging van Persoonsgegevens.

Invitare gaat zorgvuldig om met de persoonsgegevens van leerlingen, hun ouders / verzorgers en medewerkers. Ze beveiligen de gegevens tegen risico's zoals verlies, onbevoegde toegang, vernietiging, gebruik, wijziging of openbaarmaking van gegevens. Via de bewerkersovereenkomsten legt Invitare deze eis ook op aan uitgevers en leveranciers.

4.1. Privacy Impact Assessment

In de wet- en regelgeving wordt het Privacy Impact Assessment (PIA) genoemd. Een PIA is echter niet verplicht gesteld. Wij gaan ervanuit dat bij de opstelling van dit beleidsdocument dermate zorgvuldig is gewerkt en dat bij voorgenomen maatregelen afbreukrisico's zodanig zijn meegewogen dat een PIA voor Invitare niet noodzakelijk is.

4.2. Functionaris Gegevensbescherming (FG-ers)

Verder geeft de wet aan dat elke organisatie een Functionaris Gegevensbescherming moet aanwijzen. Omdat de schooldirecteuren integraal verantwoordelijk zijn voor het reilen en zeilen op school, is besloten de taken van een FG-er bij twee directeuren neer te leggen. Er is voor twee functionarissen gekozen zodat zij hun eigen school niet hoeven te controleren.

Tabel 4.2.1: verdeling scholen over de FG-ers

FG-er 1: José Martens	FG-er 2: Rob Lamers
SBO de Wingerd	Hartenaas
Harlekijn	Elckerlyc
De Bonckert	De Nienekes
't Startblok	De Klimop
Stafbureau	De Kameleon

In *bijlage 11* zijn de taken en verantwoordelijkheden van de Functionarissen Gegevensbescherming vastgelegd.

Binnen de Mosa-groep wordt een afzonderlijke FG-er aangewezen.

4.3. Verwerkingsovereenkomsten

Om de privacy van leerlingen beter te beschermen hebben 130 partijen begin 2017 een privacy-convenant afgesloten. Voor allerlei onderwijskundige software moeten scholen relatief veel persoonsgegevens delen met de leverende partijen. Met de invoering van een pseudoniem of code wordt het risico van hacken of datalekken voorkomen. Daarnaast is in het convenant een model verwerkersovereenkomst opgenomen. Vanaf 2018 moeten voor de stichting als geheel en (wanneer relevant) voor de scholen afzonderlijk verwerkingsovereenkomsten worden afgesloten met de leveranciers van (onderwijs)software. Via een register verwerkingsovereenkomsten houden wij bij met welke partijen Invitare en haar scholen dergelijke overeenkomsten hebben afgesloten. Zie als voorbeeld *bijlage 4.*

4.4. Datalek en meldplicht

Een datalek is het toegang geven tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen – lekken - van gegevens, maar ook onrechtmatige verwerking van gegevens. Er is sprake van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens zoals bedoeld in de wet. Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden. Voorbeelden datalekken zijn:

- een kwijtgeraakte USB-stick met persoonsgegevens of map met leerlinggegevens;
- een gestolen laptop;
- een inbraak in een databestand door een hacker;

- een leerling-dossier in de klas laten liggen terwijl je ergens anders in het gebouw naar een overleg gaat;
- een printopdracht is gegeven van een gespreksverslag. Terwijl je richting de printer loopt word je afgeleid. Collega's van een andere school pakken per ongeluk het verslag als ze hun eigen documenten ophalen;
- leerlingen van eenzelfde gezin worden tijdens de pauze in de teamkamer besproken door hun leerkrachten terwijl er verschillende vrijwilligers een kopje koffie komen halen;
- een gespreksverslag wordt per ongeluk naar een verkeerde ouder verzonden.

Met betrekking tot datalekken geldt de meldplicht datalekken. Deze meldplicht houdt in dat Invitare, binnen 24-uur, een melding moet doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek heeft geconstateerd. In overleg met de Autoriteit Persoonsgegevens bepaalt Invitare per melding of zij het datalek ook melden aan de mensen van wie de persoonsgegevens zijn gelekt.

Medewerkers van Invitare moeten onmiddellijk nadat zij constateren dat een datalek al dan niet door eigen toedoen is ontstaan, hun directeur hierover informeren. Deze geeft de melding onmiddellijk door aan het bestuur. Bij het geval van een datalek wordt het betreffende protocol (*bijlage 5*) gehanteerd.

4.5 Beveiliging systemen en apparatuur

De in deze paragraaf genoemde bijlagen hebben tot doel de veiligheid te bevorderen rond het gebruik van systemen en apparatuur. In *bijlage 13* (Verwijderen hardware…) staat hoe wij omgaan het afvoeren van afgeschreven apparatuur. In *bijlage 14* (Uitdiensttreding: wat moet ik doorgeven) staat beschreven wat de acties zijn bij de uitdiensttreding van personeel. Devices moeten immers worden ingeleverd en autorisaties moeten worden ingetrokken. Tot slot hebben wij in *bijlage* 16 (Wachtwoordenbeleid) de uitgangspunten beschreven hoe medewerkers om moeten gaan met hun wachtwoorden. Deze vormen immers de sleutels tot de systemen die wij gebruiken.

5. Afspraken privacy in het kader van in- en externe communicatie

Het reglement (*bijlage*1) gaat niet in op hoe scholen omgaan met de positie (dat wil zeggen de wensen en rechten) van ouders/verzorgers in het licht van meer openbare communicatieve uitingen. In deze paragraaf gaan we hier wat verder op in.

5.1. Communicatiemiddelen

In *bijlage 2* zijn een aantal communicatiemiddelen genoemd waarin berichten van school verschijnen waarbij gebruik gemaakt wordt van beeldmateriaal of teksten waar leerlingen in voorkomen. Het doel van de inzet van deze communicatiemiddelen is drieledig:

- het zijn middelen om ouders/verzorgers te informeren over allerlei gebeurtenissen in school;
- het zijn middelen om leerlingen te informeren over allerlei gebeurtenissen in school;
- het zijn middelen om ouders/verzorgers van potentiële leerlingen te wijzen op de school.

De scholen van Invitare proberen te allen tijde te voorkomen dat leerlingen in verlegenheid gebracht worden door deze communicatie-uitingen. Ouders/verzorgers kunnen

schriftelijk aangegeven of ze bezwaar hebben tegen deze uitingen. We hopen dat hier beperkt gebruik van gemaakt wordt omdat het over het algemeen uitingen zijn van zaken waar de scholen trots op zijn.

Op verzoek verstrekken een aantal scholen klassenlijsten met gegevens van leerlingen (naam, adres en telefoonnummer) aan de ouders/verzorgers van een bepaalde groep. Ouders/verzorgers kunnen te allen tijde bezwaar maken tegen vermelding van gegevens van hun kinderen. Jaarlijks vragen de scholen aan de ouders / verzorgers toestemming voor een aantal zaken (zie *bijlage 6*).

5.2 Gebruik van e-mail

Zonder extra maatregelen zijn mailtjes die vanuit outlook, google of parnassys verzonden worden beperkt beveiligd. In *bijlage* 15 "Mailen of delen" staat beschreven hoe mails met privacygevoelige data beter beveiligd verzonden kunnen worden vanuit Office 365 dan wel de Google-omgeving. Daarnaast komen vanuit de samenwerkingsverbanden de volgende systemen beschikbaar:

- Samenwerkingsverband Stromenland heeft het programma KindKans aangeschaft. Met dit programma kunnen documenten veilig verzonden worden van school naar medewerkers van Plato;
- Samenwerkingsverband Noord-Limburg heeft het programma Grippa aangeschaft. Met dit programma kunnen documenten veilig verzonden van school naar de BOC-er worden verzonden.

Uitgaande dat beide samenwerkingsverbanden een veilige omgeving hebben gecreëerd waarbinnen privacygevoelige documenten kunnen worden gedeeld en verzonden, verwachten wij dat er nog in mindere mate gevoelige mails onbeschermd verzonden zullen worden. Naast *bijlage* 15 "Mailen of delen" zijn de verwachtingen met betrekking tot het gebruik van e-mail, ICT en sociale media vastgelegd in een protocol (zie *bijlage 7*).

Het mailverkeer van het stafbureau en de Mosagroep wordt ondersteund door Computron. Computron voert een startTLS uit bij elk e-mailverkeer. Het mailverkeer vanuit de scholen vindt plaats via Office 365 en in een enkel geval via google. Beide mailboxen maken gebruik van een SSL. StartTLS en SSL zijn cryptografische versleutelde verbindingen tussen computers.

5.3 Pseudonimisering

Landelijk is vastgelegd dat er zo veel als mogelijk gewerkt moet worden met gepseudonimiseerde gegevens van de leerlingen. Een ECK-versleuteling (Educatieve Content Keten) is gegarandeerd door basispoort, Parnassys, Cito en Route 8. Voor IEP geldt dat zij tot 2020/21 gebruik maken van een Edu-koppeling en daarna van de ECK-versleuteling.

5.4 Websites en het ouderportal

Alle scholen beschikken over een website, zoals ook Invitare als geheel. De sites worden beheerd door verschillende bedrijven. In *bijlage 8* is een overzicht opgenomen waarin is aangegeven welk bedrijf welke website beheert en of er sprake is van het plaatsen van cookies. Een cookie is een klein tekstbestand dat tijdens een bezoek aan een website op de computer, tablet of smartphone van de bezoeker wordt geplaatst. In dit tekstbestand wordt informatie opgeslagen. Deze informatie kan bij een later bezoek weer worden herkend door deze website. Soms kan ook een andere website de cookie lezen en er infor-

matie in opslaan. In principe moet er bij het eerste bezoek aan een site toestemming gevraagd worden voor het plaatsen van Cookies. In de google-omgeving waarbinnen de leerlingen van zeven van onze scholen werken, beheren wijzelf de cookies. In principe wordt na elke internetsessie de zoekgeschiedenis en cookies gewist. Bij twee van onze scholen werken de leerlingen in een Apple-omgeving. Hier wordt de zoekgeschiedenis en de cookies niet automatische verwijderd. Via het programma Zulu stellen we dit echter zelf in.

6. **Informatieplicht**

6.1. Inleiding

Iedere ouder heeft in principe recht op informatie van school over zijn of haar kind. De ene ouder heeft recht op meer informatie dan de andere. Een enkeling heeft zelfs helemaal geen recht op informatie. Dat heeft te maken met de wettelijke hoedanigheid waarin de ouders verkeren.

Voor ouders die met elkaar getrouwd zijn of samenwonen en die gezamenlijk het gezag over hun kinderen hebben, is de situatie het eenvoudigst. Zij krijgen steeds gezamenlijk alle informatie over hun kind. Voor ouders die gescheiden zijn, die niet meer bij elkaar wonen en die wel het gezag hebben, ligt het niet anders. Zij hebben allebei recht op alle informatie over hun kind. De ouder die belast is met het ouderlijke gezag, heeft de verplichting om de andere ouder (die niet belast is met het ouderlijke gezag) op de hoogte te houden van gewichtige aangelegenheden die het kind betreffen. Gegevens over schoolresultaten zouden dus ook via de met het gezag belaste ouder verstrekt moeten worden. Als echter in de communicatie tussen ouders storingen ontstaan, kan dat voor school problemen opleveren.

Ouders die geen gezag (meer) hebben over het kind, hebben ook recht op informatie over hun kind. De ouder zal daar echter zelf om moeten vragen. De school hoeft uit zichzelf geen informatie te geven aan deze ouders. Als het gaat om de vader, moet deze bovendien het kind hebben erkend, anders heeft hij helemaal geen recht op informatie, ook niet als hij erom vraagt. Ouder die het gezag niet (meer) hebben, hebben beperkt recht op informatie over hun kind. Het betreft alleen belangrijke feiten en omstandigheden. Dus informatie over schoolvorderingen en eventueel sociaalpedagogische ontwikkelingen op school. Als het belang van het kind zich tegen informatieverstrekking verzet, dan hebben de ouders ook geen recht op informatie. Dit kan het geval zijn indien een rechter of psycholoog heeft geoordeeld dat het geven van informatie aan een ouder het kind zal schaden. In de volgende tabel is een schema weergegeven waarin de soorten verbintenissen tussen ouders zijn omschreven plus informatierecht.

Voor wie	Alle informatie	Beperkte informatie	Geen informatie
Ouders die met elkaar zijn getrouwd. Voor beiden geldt:	x		
Ouders die zijn gescheiden. Voor beiden geldt:	x (er mag geen informatie worden verstrekt die mogelijk gebruikt kan worden om voordeel ten koste van de andere ouder te behalen).		
Ouders die hun partnerschap hebben laten registreren.	x		
Ouders die niet met elkaar zijn getrouwd, maar via goedkeuring van de rechtbank gezag uitoefenen.	x		
Ouder die niet met het gezag is belast.		X (art 1:377c BW)	
In geval van samenwonen, vader heeft kind erkend maar is niet ingeschreven in gezagsregister. Voor vader geldt:		X (art 1:377c BW)	
In het geval van samenwonen, vader heeft kind erkend en is ingeschreven in gezagsregister. Voor beiden geldt:	x		
Stel heeft samengewoond en is nu uit elkaar. Het kind is erkend en is ingeschreven in het gezagsregister. Voor beiden geldt:	x (er mag geen informatie worden verstrekt die mogelijk gebruikt kan worden om voordeel ten koste van de andere ouder te behalen).		
Stel heeft samengewoond en is nu uit elkaar. Het kind is erkend, maar niet ingeschreven in gezagsregister. Voor vader geldt:		X (art 1:377.c BW)	
Ouders zijn beide uit de ouderlijke macht gezet. Kind is onder voogdij geplaats. Voor beiden geldt:		X (art 1:377.c BW)	
Voogd	x		
Biologische vader die zijn kind niet heeft erkend.			x
Grotouders die de verzorging van het kind op zich nemen, omdat ouders spoorloos zijn.			x

N.b. ten aanzien van de positie van pleegouders wordt opgemerkt dat de rechten door de voogd is geregeld in een standaardovereenkomst.

Indien er dus sprake is van een ouder die niet met het gezag is belast maar die wel informatie wil, geldt artikel 1:377c van het Burgerlijk Wetboek. In dit artikel staat:

- Lid 1 De niet met het gezag belaste ouder wordt desgevraagd door derden die beroepshalve beschikken over informatie inzake belangrijke feiten en omstandigheden die de persoon van het kind of diens verzorging en opvoeding betreffen, daarvan op de hoogte gesteld, tenzij die derde de informatie niet op gelijke wijze zou verschaffen aan degene die met het gezag over het kind is belast dan wel bij wie het kind zijn gewone verblijfplaats heeft, of het belang van het kind zich tegen het verschaffen van de informatie verzet.

- Lid 2: Indien de informatie is geweigerd, kan de rechter op verzoek van de in het eerste lid van dit artikel bedoelde ouder bepalen dat de informatie op de door hem aan te geven wijze moet worden verstrekt. De rechter wijst het verzoek in ieder geval af, indien het belang van het kind zich tegen het verschaffen van de informatie verzet.

6.2. **Informatieverstrekking aan niet-samenwonende ouders**

In principe vinden wij het belangrijk om beide ouders van een leerling goed te informeren over de ontwikkeling van hun kind of kinderen. Maar zoals in paragraaf 6.1 vermeld, is de ouder die is belast met het ouderlijke gezag, verplicht om de andere ouder (die niet belast is met het ouderlijke gezag) op de hoogte te houden. Dit betekent dat school de volgende informatie verstrekt aan alleen de gezaghebbende ouder:

- de schoolgids;
- het rapport;
- de uitnodiging voor de ouderavonden.

Het streven van onze scholen is om gescheiden ouders van een leerling in gezamenlijkheid te informeren of spreken. Dit doen de scholen om aan beide ouders identieke informatie te verstrekken en om zo te voorkomen dat er misverstanden ontstaan. Voor een ouderavond zijn dus beide ouders welkom voor een gezamenlijk gesprek. Alleen in bijzondere gevallen kan hiervan worden afgeweken.

6.3. **Informatieverstrekking gegevens aan derden**

Vele instanties doen een beroep op scholen met het verzoek om nadere informatie te verstrekken. Uitgangspunt is dat het bestuur c.q. de school deze gegevens niet zonder toestemming kan verlenen. Zo vragen gemeenten bijvoorbeeld gegevens op voor het verstrekken van subsidie. Leerling-gegevens worden in deze gevallen alleen maar geanonimiseerd verstrekt.

Ook verzekeringsmaatschappijen, charitatieve instellingen en andere organisaties doen graag een beroep op scholen voor leerling-gegevens. Zonder toestemming van de ouders/verzorgers worden deze niet verstrekt.

Anders is het als de Belastingdienst gegevens opvraagt. Besturen en scholen zijn dan wel verplicht de gegevens te verstrekken, mits het verzoek gebaseerd is op wet- en regelgeving.

In het kader van onderzoeken kunnen scholen benaderd worden voor medewerking. Als voorbeeld kunnen genoemd worden Jeugdzorg, politie en justitie. Formeel is het zo geregeld dat er zonder meer medewerking moet worden verleend bij een justitieel onderzoek. Voor het voorkomen of opsporen van strafbare feiten, is het bestuur alleen verplicht deze gegevens te verstrekken indien de politie hier uitdrukkelijk en gericht om vraagt en aangeeft op grond van welke wettelijke regeling het bestuur de gegevens moet verstrekken. Dit kan bijvoorbeeld op bevel van de rechter-commissaris in strafzaken. Advocaten behoeven niet toegelaten te worden.

7. **Camera- en videobeelden**

Een aantal scholen beschikken over cameratoezicht. Daarnaast komt het ook voor dat vanwege professionaliseringsdoeleinden opnamen in de klas worden gemaakt. *Bijlage 9* gaat hier nader op in.

8. Checklist en voorbeeldbrieven

Ten behoeve van de scholen hebben we een checklijst opgesteld waarmee gecontroleerd kan worden of voldoende zorgvuldig met de privacy van leerlingen en hun ouders / verzorgers wordt omgaan. Tevens is er een geheimhoudingsverklaring opgenomen waarmee de scholen nieuwe medewerkers, studenten en vrijwilligers erop kunnen wijzen dat zij de privacy van leerlingen en hun ouders/verzorgers dienen te respecteren. Deze documenten zijn als *bijlage* 10 en 13 opgenomen

9. Communicatie en evaluatie

Dit document wordt met de directieraad en de GMR besproken. Nadat het document is vastgesteld wordt het onderwerp Privacy met de verschillende teams besproken.

Op dit moment pretenderen wij nog niet dat het beleidsdocument volledig is. Dit betekent dat het komende jaar een aantal amendementen en aanvullingen zullen volgen. Omdat met name de technologische ontwikkelingen snel gaat, zal nadat het document volledig is, het om de twee jaar tegen het licht gehouden worden.

Bijlage 1: Privacyreglement Stichting Invitare Openbaar Onderwijs

Inhoudsopgave

Artikelsgewijze toelichting ten behoeve van implementatie van het reglement

Begripsbepalingen

Voor de toepassing van dit reglement en de daarbij behorende bijlagen wordt verstaan onder:

a. *Algemene Verordening Gegevensbescherming (AVG)*: de Verordening;
b. *Autoriteit Persoonsgegevens*: toezichthoudende autoriteit, als bedoeld in artikel 51 van de AVG;
c. *Bestand*: elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;
d. *Betrokkene*: degene op wie een persoonsgegeven betrekking heeft (een sollicitant, een medewerker werkzaam/werkzaam geweest bij Stichting Invitare Openbaar Onderwijs, een leerling ingeschreven/ingeschreven geweest aan een school behorende tot Stichting Invitare of een ouder/verzorger van wie gegevens in de persoonsregistratie zijn opgenomen, alle overige personen werkzaam bij of ten dienste van de Stichting, waaronder de leden van het toezichthoudend orgaan, leveranciers en dienstverleners, huurders en tenslotte de bezoekers van één van de schoolgebouwen van de Stichting;
e. *Derde*: degene, niet zijnde de verwerker of degene die onder gezag van de verwerkingsverantwoordelijke werkzaam zijn, die door de verwerker gemachtigd is om persoonsgegevens te verwerken;
f. *Dienst van de informatiemaatschappij*: dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht;
g. *Gegevensbeschermingseffectbeoordeling*: een beoordeling van het effect van de beoogde verwerking op de bescherming van persoonsgegevens;
h. *Groep*: een economische eenheid waarin rechtspersonen organisatorisch verbonden zijn (artikel 2:24 BW);
i. *Leerling*: persoon die onderwijs volgt of gaat volgen op een school van de Stichting
j. *Leerling- of personeelsnummer*: eenduidig nummer dat wordt gebruikt ten behoeve van efficiënte verwerking van persoonsgegevens;

k. *Personeel*:
   a. de bij de Stichting werkzame directeur, (adjunct-)directeur of leraar, en overige medewerkers benoemd in een andere functie dan het geven van onderwijs, waaronder begrepen de leden van het bestuur van die scholen die zijn benoemd door een raad van toezicht als bedoeld in artikel 17c, vierde lid van de Wpo respectievelijk artikel 28i vierde lid van de Wec, voor zover die leden mede zijn benoemd op basis van een akte;
   b. de onder a bedoelde medewerker die zonder benoeming is tewerkgesteld bij of ingeleend door de Stichting;

m. *Persoonsgegevens*: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene');
   Pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan de specifieke persoon kunnen worden gekoppeld, zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;

n. *School*: een school als bedoeld in artikel 1 van de Wpo respectievelijk artikel 1 van de Wec en die in stand wordt gehouden door de Stichting;

o. *Schoolbegeleiding*: activiteiten ten behoeve van de schoolorganisatie of het onderwijs aan een school die dienen tot begeleiding, ontwikkeling, advisering, informatieverstrekking en evaluatie, alsmede activiteiten tot bevordering van een optimale schoolloopbaan van leerlingen;

p. *Stichting:* Stichting Invitare Openbaar Onderwijs;

q. *Toestemming van betrokkene*: elke vrije, specifieke, geïnformeerde ondubbelzinnige wilsuiting door middel van een verklaring of een ondubbelzinnig actieve handeling, waarmee betrokkene hem betreffende verwerking van persoonsgegevens aanvaardt;

r. *Het toezichthoudend orgaan*: de Raad van Toezicht;

s. *Verordening:* Verordening EU 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG;

t. *Verwerking van persoonsgegevens*: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen of vernietigen van gegevens;

u. *Verwerkingsverantwoordelijke*: de Stichting;

v. *Verwerker*: degene die op basis van een overeenkomst ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;

w. *Wec*: Wet op de expertisecentra;

x. *Wpo*: Wet op het primair onderwijs.

Artikel 2. Verantwoordelijkheden

2.1. Stichting Invitare Openbaar Onderwijs is verantwoordelijk voor:

a. Een rechtmatige, behoorlijke en transparante gegevensverwerking;
b. Het vaststellen van welbepaalde duidelijk omschreven en gerechtvaardigde doeleinden alsmede een verwerking conform de vastgestelde doeleinden;
c. Een minimale gegevensverwerking, dat wil zeggen dat het gebruik van gegevens wordt beperkt tot hetgeen noodzakelijk is voor de doeleinden waarvoor deze worden verwerkt;
d. Het gebruik van juiste en geactualiseerde gegevens en het wissen respectievelijk corrigeren van gegevens die onjuist zijn;
e. Opslagbeperking van gegevens, dat wil zeggen dat deze niet langer worden bewaard dan nodig voor de vastgestelde doeleinden;
f. Het nemen van passende technische en organisatorische maatregelen.

2.2. De Stichting laat zich bij bovengenoemde taken adviseren door de Functionaris Gegevensbescherming.

Artikel 3. De Functionaris Gegevensbescherming (FG)

3.1. De FG vervult zijn taken en verplichtingen onafhankelijk van het bestuur.
3.2. De FG houdt intern toezicht op de naleving van de wet- en regelgeving, de in de onderwijssector vastgestelde gedragscodes, het beleid van de Stichting of de verwerker met betrekking tot de bescherming van persoonsgegevens.
3.3. De FG adviseert over verwerkingsprocessen en ziet toe op de uitvoering en evaluatie ervan.
3.4. De FG adviseert over het passende niveau van beveiliging van de informatiehuishouding in de organisatie en over maatregelen die zijn gericht op het beperken van de verwerking van persoonsgegevens.
3.5. De FG werkt samen met de toezichthoudende autoriteit (Autoriteit Persoonsgegevens).
3.6. Betrokkenen kunnen met de FG contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten op grond van dit reglement en uit hoofde van de Verordening.
3.7. De FG brengt jaarlijks verslag uit aan de verwerkingsverantwoordelijke van zijn werkzaamheden en bevindingen.
3.8. De FG is met betrekking tot zijn taken tot geheimhouding en vertrouwelijkheid gehouden.

Artikel 4. Informatie en toegang tot de persoonsgegevens

4.1. Indien de gegevens van de betrokkene zelf worden verkregen, informeert de Stichting betrokkene bij de verkrijging van de persoonsgegevens over:
a. de volledige naam en de contactgegevens van Stichting alsmede van de Functionaris Gegevensbescherming;
b. de doeleinden waarvoor de persoonsgegevens worden verwerkt;
c. de wettelijke grondslag voor de verwerking, en indien de verwerking is gebaseerd op de grondslag gerechtvaardigd belang (artikel 6 lid 1f AVG), het gerechtvaardigd belang van de Stichting;
d. de ontvangers of categorieën van ontvangers;
e. in voorkomend geval, dat de Stichting het voornemen heeft om de persoonsgegevens door te geven aan een derde land of internationale organisatie, om

welk derde land het gaat en of het niveau van gegevensbescherming in dit land adequaat is, dan wel of er passende waarborgen zijn genomen;
f. hoelang de persoonsgegevens worden bewaard;
g. het recht van betrokkene om te verzoeken om inzage, rectificatie, beperking van de verwerking en wissing van de persoonsgegevens, alsmede het recht om bezwaar te maken tegen de verwerking;
h. het recht van betrokkene om te allen tijde eerder gegeven toestemming in te trekken;
i. het recht van betrokkene om een klacht in te dienen bij de AP;
j. het bestaan van automatische besluitvorming en de onderliggende logica hiervan, alsmede het belang en de verwachte gevolgen van de verwerking voor betrokkene; en
k. of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten, of de betrokkene verplicht is om de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn als de betrokkene de gegevens niet verstrekt.

4.2. Indien de gegevens *niet* van betrokkene afkomstig zijn verstrekt de Stichting aan de betrokkene de informatie als genoemd onder 4.1. a.t/m j. en in aanvulling daarop informatie over:
- de betrokken categorieën van persoonsgegevens; en
- de bron waar de persoonsgegevens vandaan komen, en in voorkomend geval, of zij afkomstig zijn van openbare bronnen.

De Stichting verstrekt deze informatie binnen een redelijke termijn, doch uiterlijk binnen één maand na de verkrijging van de persoonsgegevens. Indien de gegevens worden gebruikt voor communicatie met de betrokkene, uiterlijk op het moment van het eerste contact met de betrokkene. Indien de verstrekking van de gegevens aan een andere ontvanger wordt overwogen, uiterlijk op het tijdstip waarop de persoonsgegevens voor het eerst worden verstrekt.

4.3. Alle nieuwe medewerkers, stagiairs en vrijwilligers die betrokken zijn bij de uitvoering van dit reglement en daarbij de toegang krijgt tot persoonsgegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs kan vermoeden en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift ter zake van de persoonsgegevens een geheimhoudingsplicht geldt, is verplicht tot geheimhouding daarvan en tekent de geheimhoudingsverklaring. Dit geldt niet indien enig wettelijk voorschrift hem tot bekendmaking verplicht of uit zijn taak bij de uitvoering van dit reglement de noodzaak tot bekendmaking voortvloeit.

4.4. Zittend personeel verplichten wij niet tot tekening van de geheimhoudingsverklaring omdat wij ervanuit gaan dat zij op basis van hun ervaring al bekend zijn met de geheimhoudingsverplichting. Desondanks worden de medewerker hier tijdens een voorlichting AVG in schooljaar 2018/19 voor de zekerheid nog een keer op gewezen.

Artikel 5. Categorieën van betrokkenen, doeleinden en persoonsgegevens

5.1. Leerlingen

5.1.1. De verwerking van persoonsgegevens van leerlingen heeft ten doel:

a. de toelating en inschrijving van de leerling bij de school (artikel 6 lid 1b (lid 1e voor het openbaar onderwijs));
b. de organisatie of het geven van het onderwijs, de (individuele) schoolbegeleiding van leerlingen, het opstellen van een onderwijskundig rapport en het geven van schooladviezen (artikel 6 lid 1c AVG);
c. het bij uitschrijving van een leerplichtige leerling informeren van de vervolgschool over het gevolgde onderwijs en de behaalde leerresultaten (artikel 6 lid 1c AVG);
d. het gebruik van een leerlingvolgsysteem dat de school inzicht verschaft in de cognitieve en sociaal-emotionele ontwikkeling en mogelijkheid biedt tot beheer en delen van deze gegevens met de docenten van de leerlingen en de ouders/verzorgers en leerlingen (artikel 6 lid 1c AVG);
e. het uitvoeren van de op de Stichting rustende verplichtingen en bevoegdheden op grond van de wet en daarop gebaseerde uitvoeringsregelgeving, waaronder (doch niet uitsluitend) de Wet op het primair onderwijs (Wpo), de Wet Medezeggenschap scholen (WMS), de Leerplichtwet en daarop gebaseerde regelgeving (artikel 6 lid 1c en 1e AVG);
f. het verstrekken of ter beschikking stellen van leermiddelen (artikel 6 lid 1c AVG);
g. het geven van onderwijs met behulp van digitale leermiddelen en diensten van de informatiemaatschappij (artikel 6 lid 1a AVG);
h. het verstrekken van inloggegevens voor het schoolnetwerk en digitale leermiddelen en – diensten (artikel 6 lid 1b AVG);
i. het berekenen en vaststellen van ouderbijdragen (artikel 6 lid 1b AVG);
j. het behandelen van geschillen aanhangig gemaakt bij klachten- en geschillencommissies (artikel 6 lid 1c AVG);
k. het laten uitoefenen van accountantscontrole (artikel 6 lid 1c AVG);
l. het medewerking verlenen aan een aanvraag van ouders, respectievelijk leerlingen, van leerlingenvervoer (artikel 6 lid 1c AVG);
m. het bekend maken van informatie over de organisatie, de activiteiten van de school in de schoolgids, op de website en sociale media (artikel 6 lid 1a AVG);
n. het opstellen en vormgeven van een (digitaal) smoelenboek met de foto's van leerlingen (artikel 6 lid 1a AVG);
o. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van de Stichting (artikel 6 lid 1f AVG);
p. het uitvoering geven aan de wettelijke verplichting gegevens te verstrekken aan het Ministerie van Onderwijs en Wetenschappen, de onderwijsinspectie, en overige instanties, voor zover de verplichting daartoe voortvloeit uit de wetgeving, inclusief de op de onderwijswetgeving gebaseerde bekostigingsvoorwaarden (artikel 6 lid 1c AVG);
q. het voldoen aan een verzoek van een bestuursorgaan dat is belast met de uitvoering van een publiekrechtelijke taak (artikel 6 lid 1e AVG);
r. het aanbieden van diensten door de schoolfotograaf (artikel 6 lid 1a AVG).

5.1.2. Geen andere persoonsgegevens worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens zoals het e-mailadres, alsmede het bankrekeningnummer van de betrokkene;
b. het BSN-nummer;
c. nationaliteit en geboorteplaats;
d. persoonsgebonden leerlingnummer;
e. gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling;
f. gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor het onderwijs;
g. gegevens over de leerresultaten, waaronder maar niet uitsluitend gerekend worden test- en toetsgegevens, gegevens betreffende de aard en het verloop van het onderwijs, zaken die volgens de basisschool van invloed kunnen zijn op de prestaties in het voortgezet onderwijs, verzuim en afwezigheid van de leerling, de diagnostische eindtoets, het werk van het centraal examen en de rekentoets;
h. gegevens met het oog op de organisatie van het onderwijs en het verstrekken of ter beschikking stellen van (digitale) leermiddelen;
i. gegevens met het oog op het berekenen, vastleggen en innen van inschrijvingsgelden, ouderbijdragen, vergoedingen voor leermiddelen en buitenschoolse activiteiten;
j. foto's en videobeelden met of zonder geluid van (les)activiteiten van de school;
k. (digitale) pasfoto’s;
l. inloggegevens voor het schoolnetwerk, de door de school gebruikte digitale leermiddelen, sociale media en software applicaties voor onderwijsdoeleinden alsmede inlogcodes voor de bestelling van reguliere leermiddelen bij de leverancier;
m. gegevens als bedoeld onder a. en c., van de ouders, voogden of verzorgers van leerlingen en of sprake is van gezamenlijk ouderlijk gezag en gegevens over lidmaatschap van de ouderraad of de oudergeleding van de medezeggenschapsraad en beroep of hoogst genoten opleidingsniveau;
n. camerabeelden van het schoolterrein en de algemeen toegankelijke ruimten van de school;
o. de gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camera-opnamen zijn gemaakt;
p. andere dan de onder a. tot en met o. bedoelde gegevens waarvan de verwerking wordt vereist of noodzakelijk is met het oog op de toepassing van een wettelijke regeling.

5.2. Personeel

5.2.1. De verwerking van gegevens van personeel heeft ten doel:

a. het aangaan van de arbeidsovereenkomst (artikel 6 lid 1b AVG);
b. het vaststellen van het salaris en overige arbeidsvoorwaarden (artikel 6 lid 1b AVG);
c. het (laten) uitbetalen van salaris, de afdracht van belastingen en premies (artikelen 6 lid 1b en 6 lid 1c AVG);

d. de uitvoering van een voor de betrokkene geldende arbeidsvoorwaarde (artikel 6 lid 1b AVG);
e. het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen (artikel 6 lid 1b AVG);
f. het verlenen van ontslag (artikel 6 lid 1b AVG);
g. de overgang van de betrokkene naar diens (tijdelijke) tewerkstelling bij een ander onderdeel van de groep, bedoeld in artikel 2:24b van het Burgerlijk Wetboek waaraan de verwerkingsverantwoordelijke is verbonden (artikel 6 lid 1b AVG);
h. het geven van leiding en het begeleiden van betrokkene (artikel 6 lid 1b AVG);
i. het verstrekken van de bedrijfsmedische zorg voor betrokkene en het kunnen nakomen van re-integratieverplichtingen bij verzuim (artikel 6 lid 1c AVG);
j. het toegang verlenen tot het schoolnetwerk (artikel 6 lid 1b AVG);
k. het regelen van en de controle van aanspraken op uitkeringen in verband met de beëindiging van een dienstverband (artikel 6 lid 1b AVG);
l. de verkiezing van de leden van een bij wet geregeld medezeggenschapsorgaan (artikel 6 lid 1c AVG);
m. het behandelen van geschillen (artikel 6 lid 1b AVG);
n. de behandeling van personeelszaken, anders dan genoemd onder a. t/m m. (artikel 6 lid 1b AVG);
o. de organisatie of het geven van het onderwijs (artikel 6 lid 1b AVG);
p. het laten uitoefenen van accountantscontrole en het laten vaststellen van aanspraken op bekostiging (artikel 6 lid 1c AVG);
q. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van de Stichting (artikel 6 lid 1f AVG);

5.2.2. Geen andere persoonsgegevens worden verwerkt dan:
a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede bank- en giroreke-ningnummer van de betrokkene;
b. BSN-nummer;
c. kopie ID-bewijs/paspoort en Verklaring Omtrent Gedrag (VOG);
d. een personeelsnummer dat geen andere informatie bevat dan bedoeld onder a;
e. nationaliteit, geboorteplaats;
f. gegevens betreffende de godsdienst of levensovertuiging, voor zover die noodzakelijk zijn voor een goede functie-uitoefening conform de benoemingsvoorwaarden;
g. gegevens betreffende gevolgde en te volgen opleidingen, cursussen en stages en assessments;
h. gegevens betreffende de arbeidsvoorwaarden;
i. gegevens betreffende het berekenen, vastleggen en betalen van salarissen, vergoedingen en andere geldsommen en beloningen in natura;
j. gegevens betreffende het berekenen, vastleggen en betalen van belasting en premies;

k. gegevens betreffende de functie of de voormalige functie(s), alsmede betreffende de aard, de inhoud en de beëindiging van voorgaande dienstverbanden;
l. gegevens met het oog op de administratie van de aanwezigheid van de betrokkenen op de plaats waar de arbeid wordt verricht en hun afwezigheid in verband met verlof, arbeidsduurverkorting, bevalling of ziekte, met uitzondering van gegevens over de aard van de ziekte;
m. gegevens die in het belang van de betrokkenen worden opgenomen met het oog op hun arbeidsomstandigheden en veiligheid;
n. gegevens, waaronder begrepen gegevens betreffende gezinsleden en voormalige gezinsleden van de betrokkenen, die noodzakelijk zijn met het oog op een overeengekomen arbeidsvoorwaarden;
o. gegevens met betrekking tot de functie-uitoefening, de personeelsbeoordeling en de loopbaanbegeleiding, voor zover die gegevens bij de betrokkenen bekend zijn;
p. gegevens van docenten, onderwijsondersteunend personeel en begeleiders, voor zover deze gegevens van belang zijn voor de organisatie van de school of de instelling en het geven van onderwijs, opleidingen en trainingen;
q. inloggegevens van het schoolnetwerk en digitale leermiddelen;
r. foto's en videobeelden met of zonder geluid van activiteiten van de school en van lessen van onderwijzend personeel;
s. camerabeelden van het schoolterrein en de algemeen toegankelijke ruimten van de school;
t. de gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camera-opnamen zijn gemaakt;
u. andere dan de onder a. tot en met t. bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere niet nader genoemde wet.

5.3. Sollicitanten

5.3.1. De Stichting hanteert de sollicitatiecode zoals opgenomen in bijlage XII van de cao Primair Onderwijs, waarin de procedures van de organisatie inzake werving en selectie zijn opgenomen als ook de wijze van omgang met persoonsgegevens.

5.3.2. De verwerking van gegevens van sollicitanten heeft ten doel:
a. de beoordeling van de geschiktheid van betrokkene voor een functie die vacant is (artikelen 6 lid 1a en 6 lid 1b AVG);
b. de beoordeling van de geschiktheid van betrokkene voor een functie die in de nabije toekomst vacant kan komen (artikelen 6 lid 1a en 6 lid 1b AVG);
c. de afhandeling van de door de sollicitant gemaakte onkosten (artikel 6 lid 1a AVG);
d. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van de Stichting (artikel 6 lid 1f AVG);
e. de uitvoering of toepassing van wetgeving (artikel 6 lid 1c AVG).

5.3.3. Geen andere gegevens worden verwerkt dan:
a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie

benodigde gegevens, zoals het e-mailadres alsmede bank- en girorekeningnummer van de betrokkene;
b. nationaliteit en geboorteplaats;
c. gegevens betreffende de godsdienst of levensovertuiging, voor zover die noodzakelijk zijn voor de beoordeling of de sollicitant voldoet aan de benoemingsvoorwaarden;
d. gegevens betreffende gevolgde en te volgen opleidingen, cursussen en stages;
e. gegevens betreffende de functie waarnaar gesolliciteerd is;
f. gegevens betreffende de aard en inhoud van de huidige dienstbetrekking, alsmede betreffende de beëindiging ervan;
g. gegevens betreffende de aard en inhoud van de vorige dienstbetrekkingen, alsmede betreffende de beëindiging ervan;
h. andere gegevens met het oog op het vervullen van de functie (bijvoorbeeld gegevens in het kader van een te voeren voorkeursbeleid voor minderheden of re-integratiebeleid);
i. foto's en videobeelden met of zonder geluid;
j. camerabeelden van het schoolterrein en de algemeen toegankelijke ruimten van de school;
k. de gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camera-opnamen zijn gemaakt;
l. andere gegevens met het oog op het vervullen van de functie, die door of na toestemming van de betrokkene zijn verstrekt (assessments, psychologisch onderzoek);
m. andere dan de onder a. tot en met j. bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet;
n. gegevens verkregen uit internetsearch.

5.4. <u>Oud-medewerkers</u>

5.4.1. De verwerking van gegevens van oud-medewerkers heeft ten doel:
a. het onderhouden van contacten met oud-medewerkers (artikel 6 lid 1a AVG);
b. het verzenden van informatie aan oud-medewerkers (artikel 6 lid 1a AVG);
c. het verwerken van de aanmeldingen van oud-medewerkers voor mede voor hen georganiseerde activiteiten en bijeenkomsten (artikel 6 lid 1a AVG);
d. het berekenen, vastleggen en innen van bijdragen en giften, waaronder begrepen het in handen van derden stellen van vorderingen, alsmede andere activiteiten van intern beheer (artikel 6 lid 1a AVG);
e. het doen uitoefenen van accountantscontrole (artikel 6 lid 1c AVG).

5.4.2. Geen andere persoonsgegevens worden verwerkt dan:
a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede bank- en girorekeningnummer van de betrokkene;

b. gegevens betreffende de functie waarin en de periode gedurende welke de oud-medewerker voor de verwerkingsverantwoordelijke werkzaam is geweest;
c. gegevens met het oog op het berekenen, vastleggen en innen van bijdragen en giften;
d. een administratiecode dat geen andere informatie bevat dan bedoeld onder a. tot en met c.;
e. gegevens met betrekking tot aanmelding activiteiten/bijeenkomsten.

5.5. Oud-leerlingen

5.5.1. De verwerking van gegevens van oud-leerlingen heeft ten doel:
a. het onderhouden van contacten met de oud-leerlingen (artikel 6 lid 1a AVG);
b. het verzenden van informatie aan de oud-leerlingen (artikel 6 lid 1a AVG);
c. het verwerken van de aanmeldingen van oud-leerlingen voor mede voor hen georganiseerde activiteiten en bijeenkomsten (artikel 6 lid 1a AVG);
d. het berekenen, vastleggen en innen van bijdragen en giften, waaronder begrepen het in handen van derden stellen van vorderingen, alsmede andere activiteiten van intern beheer (artikel 6 lid 1a AVG);
e. het doen uitoefenen van accountantscontrole (artikel 6 lid 1c AVG);
f. het archiefbeheer, het behandelen van geschillen, het verrichten van wetenschappelijk, statistisch of historisch onderzoek (artikel 6 lid 1a en artikel 6 lid 1f AVG).

5.5.2. Geen andere persoonsgegevens worden verwerkt dan:
a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens, zoals het e-mailadres alsmede bankrekeningnummer van de betrokkene;
b. gegevens betreffende de aard van de (vervolg) studie respectievelijk toekomstige werkkring en de periode gedurende welke de oud-leerling, de opleiding heeft gevolgd;
c. gegevens met het oog op het berekenen, vastleggen en innen van bijdragen en giften;
d. een administratiecode dat geen andere informatie bevat dan bedoeld onder a. tot en met c.;
e. gegevens met betrekking tot aanmelding activiteiten/bijeenkomsten.

5.6. Leden de Raad van Toezicht (RvT)

5.6.1. De verwerking van gegevens van de (kandidaat-)leden van RvT heeft ten doel:
a. het vastleggen van de benoeming, de functie binnen de RvT en de benoemingstermijn (artikel 6 lid 1b AVG);
b. het vastleggen en (laten) uitbetalen van de – door de RvT - vastgestelde beloning alsmede overige activiteiten van intern beheer (artikel 6 lid 1b AVG);
c. de aanmelding voor de aansprakelijkheidsverzekering voor RvT-leden (artikel 6 lid 1b AVG);

d. het uitvoering geven aan het recht van de medezeggenschapsraad om op grond van de WMS een bindende voordracht te doen voor een RvT-lid (artikel 6 lid 1c AVG);
e. de organisatie van de school waaronder het informeren van personeel en leerlingen over de samenstelling en bereikbaarheid van de RvT (artikel 6 lid 1b AVG);
f. het onderhouden van contacten tussen de Stichting en de medezeggenschapsraad met de RvT (artikel 6 lid 1b AVG);
g. het verzenden van (management)informatie aan de RvT (artikel 6 lid 1 b AVG);
h. het laten uitoefenen van accountantscontrole (artikel 6 lid 1c AVG);
i. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van de Stichting (artikel 6 lid 1f AVG).

5.6.2. Geen andere persoonsgegevens worden verwerkt dan:
a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede bank- en giroreke-ningnummer van de betrokkene;
b. BSN-nummer;
c. kopie ID-bewijs/paspoort;
d. nationaliteit en geboorteplaats;
e. gegevens betreffende de godsdienst of levensovertuiging, voor zover die noodzakelijk zijn voor een goede functie-uitoefening conform de benoemingsvoorwaarden;
f. gegevens betreffende het berekenen, vastleggen en betalen van salarissen, vergoedingen en andere geldsommen en beloningen in natura;
g. gegevens betreffende gevolgde en te volgen opleidingen;
h. gegevens betreffende de functie binnen het toezichthoudend orgaan, alsmede betreffende de aard, de inhoud van de overige werkzaamheden en expertise;
i. camerabeelden van het schoolterrein en de algemeen toegankelijke ruimten van de school;
j. de gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camera-opnamen zijn gemaakt;
k. andere dan de onder a. tot en met i. bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere niet nader genoemde wet.

5.7. <u>Bezoekers</u>

5.7.1. De verwerking van gegevens van bezoekers van een van de schoolgebouwen van de Stichting heeft ten doel:
a. het interne beheer (artikel 6 lid 1f AVG);
b. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van de Stichting (artikel 6 lid 1f AVG).

5.7.2. Geen andere persoonsgegevens worden verwerkt dan:
a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie

benodigde gegevens, zoals het e-mailadres alsmede de organisatie waartoe de bezoeker behoort;
b. een administratienummer dat geen andere informatie bevat dan onder a.;
c. gegevens betreffende de persoon en afdeling die de betrokkene wenst te bezoeken;
d. gegevens betreffende de reden van het bezoek;
e. gegevens betreffende de datum en het tijdstip van de aankomst en het vertrek van de bezoeker;
f. gegevens inzake het identiteitsbewijs van de bezoeker;
g. camerabeelden van het schoolterrein en de algemeen toegankelijke ruimten van de school;
h. gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camerabeelden zijn gemaakt.

5.7.3. Website
De Stichting informeert bezoekers van de website van de Stichting (www.stichting-invitare.nl) bij een bezoek aan de website over de doeleinden en gegevens die worden verwerkt bij een bezoek aan de website door middel van een privacy statement dat op de website is geplaatst.

5.8. Leveranciers/dienstverleners

5.8.1. De verwerking van gegevens van leveranciers van de Stichting heeft ten doel:
a. het doen van bestellingen of de opdrachtverlening aan dienstverleners (artikel 6 lid 1b AVG);
b. het berekenen en vastleggen van inkomsten en uitgaven en het doen van betalingen (artikel 6 lid 1b AVG);
c. het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen alsmede andere activiteiten van intern beheer (artikel 6 lid 1b AVG);
d. het onderhouden van contacten door de verwerkingsverantwoordelijke met de leveranciers (artikel 6 lid 1b AVG);
e. het behandelen van geschillen en het doen uitoefenen van accountantscontrole (artikel 6 lid 1c AVG);
f. de uitvoering of de toepassing van een andere wet (artikel 6 lid 1c AVG);
g. beveiliging van en toezicht op personen, zaken en gebouwen die zijn toevertrouwd aan de zorg van de Stichting (artikel 6 lid 1f AVG).

5.8.2. Geen andere persoonsgegevens worden verwerkt dan:
a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede de organisatie waartoe de betrokkene behoort;
b. een administratienummer dat geen andere informatie bevat dan onder a.;
c. gegevens met het oog op het doen van bestellingen of het opdracht verlenen aan dienstverleners;
d. camerabeelden van het schoolterrein en de algemeen toegankelijke ruimten van de scholen;

e. andere dan de onder a. tot en met d. bedoelde gegevens waarvan de verwerking is vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet;
f. gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camerabeelden zijn gemaakt.

5.9. Huurders

5.9.1. De verwerking van gegevens van huurders van de Stichting heeft ten doel:
a. de uitvoering van de overeenkomst (artikel 6 lid 1 b AVG);
b. het berekenen en vastleggen van inkomsten en uitgaven en het doen van betalingen (artikel 6 lid 1b AVG);
c. het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen (artikel 6 lid 1b AVG);
d. het behandelen van geschillen en het doen uitoefenen van accountantscontrole (artikel 6 lid 1c AVG);
e. activiteiten van intern beheer, beveiliging van en toezicht op personen, zaken en goederen die zijn toevertrouwd aan de zorg van de Stichting (artikel 6 lid 1f AVG);
f. de uitvoering of toepassing van wet- en regelgeving (artikel 6 lid 1c AVG).

5.9.2. Geen andere persoonsgegevens worden verwerkt dan:
a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens, zoals het e-mailadres alsmede de organisatie waartoe de betrokkene behoort;
b. een administratienummer dat geen andere informatie bevat dan onder a.;
c. gegevens die noodzakelijk zijn voor de uitvoering van de huurovereenkomst;
d. gegevens met het oog op het berekenen en vastleggen van inkomsten en uitgaven, het doen van betalingen en het innen van vorderingen;
e. gegevens betreffende de datum en het tijdstip van de aankomst en het vertrek van de betrokkene;
f. gegevens inzake het identiteitsbewijs van de betrokkene;
g. camerabeelden van het schoolterrein en de algemeen toegankelijke ruimten van de scholen;
h. gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de camerabeelden zijn gemaakt.

Artikel 6. Rechten betrokkenen

6.1. Privacyverklaring

6.1.1. De Stichting beschikt over een privacyverklaring, waarin betrokkenen in duidelijke, begrijpelijke en gemakkelijk toegankelijke vorm, in het bijzonder wanneer de informatie specifiek voor de leerling is, worden geïnformeerd over de gegevens die van hem worden verwerkt, de wijze waarop, en de redenen waarom dit gebeurt.

6.2. Recht op informatie

6.2.1. Betrokkenen van wie persoonsgegevens worden verwerkt, dan wel - indien zij de leeftijd van zestien jaar nog niet bereikt hebben - hun wettelijke vertegenwoordigers, hebben het recht van inzage in, en recht op een kopie van de over hen, respectievelijk hun pupil, opgenomen gegevens en van de volgende informatie over:

a. de verwerkingsdoeleinden en de rechtsgrond voor de verwerking;
b. de betrokken categorieën van persoonsgegevens;
c. de ontvangers en/of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
d. de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen of indien dat niet mogelijk is de criteria om die termijn te bepalen;
e. de herkomst van de verwerkte gegevens indien deze niet van betrokkene afkomstig zijn;
f. het bestaan van geautomatiseerde besluitvorming, alsmede het belang en de verwachte gevolgen van die verwerking voor betrokkene.

6.3. Recht op rectificatie en wissing

6.3.1. Betrokkenen hebben het recht op rectificatie van onjuiste persoonsgegevens.

6.3.2. Betrokkenen hebben recht op wissing van gegevens ('recht op vergetelheid') in de volgende situaties:

a. de persoonsgegevens zijn niet langer nodig;
b. de betrokkene trekt de toestemming waarop de verwerking overeenkomstig artikel 5 lid 2.a. berust in en er is geen andere rechtsgrond voor die verwerking;
c. de betrokkene maakt bezwaar tegen de verwerking en er zijn geen prevalerende dwingende vormen voor verwerking;
d. de gegevens zijn onrechtmatig verwerkt;
e. er is een wettelijke verplichting om de persoonsgegevens te wissen;
f. de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij.

6.3.3. In het geval de te wissen gegevens openbaar zijn gemaakt en de Stichting besluit de gegevens te wissen, neemt de Stichting rekening houdend met de beschikbare technologie en uitvoeringskosten redelijke maatregelen waaronder technische maatregelen, om andere verwerkingsverantwoordelijken ervan op de hoogte te stellen dat de betrokkene heeft verzocht om iedere koppeling naar of kopie of reproductie van die gegevens te wissen.

6.3.4. Artikel 6.3.1 en 6.3.2 zijn niet van toepassing als verwerking nodig is voor het uitoefenen van het recht op vrijheid van meningsuiting of voor het nakomen van een wettelijke verwerkingsverplichting, of voor het vervullen van een taak van algemeen belang, om redenen van algemeen belang op het gebied van volksgezondheid, d. met het oog op archivering in het algemeen belang wetenschappelijk of historisch onderzoek, voor zover het in 6.3.1 en 6.3.2. bedoelde recht de

verwezenlijking van de deze doeleinden onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen.

6.4. Recht op beperking van verwerking van gegevens

6.4.1. Betrokkene heeft op grond van de verordening in nader bepaalde situaties een recht op beperking van de verwerking van zijn gegevens. Dit houdt in dat de Stichting de persoonsgegevens, met uitzondering van de opslag, slechts verwerkt met toestemming van betrokkene of voor de instelling, uitoefening of onderbouwing van een rechtsvordering of ter bescherming van de rechten van een ander natuurlijk persoon of rechtspersoon of om gewichtige redenen van algemeen belang.

6.5. Recht op overdraagbaarheid van gegevens

6.5.1. Betrokkene heeft recht de hem betreffende persoonsgegevens die hij zelf aan de Stichting heeft verstrekt in een gestructureerde, gangbare en machine leesbare vorm te verkrijgen en hij heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen in de gevallen dat persoonsgegevens door hem op basis van verleende toestemming (artikel 6 lid 1a AVG) zijn verstrekt of op basis van een overeenkomst (artikel 6 lid 1b AVG) en de verwerking via geautomatiseerde procedés wordt verricht.

6.5.2. Bij de uitoefening van zijn recht op gegevensoverdraagbaarheid uit hoofde van het vorige lid heeft de betrokkene het recht dat gegevens indien dit technisch mogelijk is rechtstreeks van de ene naar de andere verwerkingsverantwoordelijke worden doorgezonden.

6.5.3. Het recht geldt niet voor verwerkingen die noodzakelijk zijn voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend.

6.6. Indiening van een verzoek

6.6.1. Een verzoek als bedoeld in dit artikel wordt gericht aan de Stichting ter attentie van het college van bestuur. Betrokkene kan zijn verzoek richten aan info@stichting-invitare.nl.

6.6.2. Aan een verzoek zijn geen kosten verbonden. Wanneer verzoeken van een betrokkene kennelijk ongegrond, of buitensporig zijn, met name vanwege hun repetitieve karakter kan de Stichting echter:
- een redelijke vergoeding aanrekenen in het licht van de administratieve kosten waarmee het verzoek gepaard gaat; ofwel
- weigeren gevolg geven aan het verzoek.

6.6.3. De Stichting verstrekt de betrokkene binnen een maand na ontvangst van het verzoek informatie over het gevolg dat aan het verzoek is gegeven.

6.6.4. Indien de betrokkene een verzoek doet omdat bepaalde opgenomen gegevens onjuist c.q. onvolledig zouden zijn, hij een belang heeft bij beëindiging van de verwerking dat zwaarder weegt dan dat van de organisatie, dan wel de verwerking gezien de doelstelling van het reglement niet (langer) noodzakelijk is, dan wel strijdig zijn met dit reglement, neemt de Functionaris Gegevensbescherming namens de verwerkingsverantwoordelijke binnen een maand nadat betrokkene dit verzoek heeft ingediend, hierover een schriftelijke beslissing.

6.6.5. Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken kan die termijn indien nodig met nog eens twee maanden worden verlengd. De Stichting stelt de betrokkene binnen een maand in kennis van een dergelijke verlenging. Wanneer betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt.

6.6.6. Indien de Stichting twijfelt aan de identiteit van de verzoeker, vraagt hij zo spoedig mogelijk aan de verzoeker schriftelijk nadere gegevens inzake zijn identiteit te verstrekken of een geldig identiteitsbewijs te overleggen. Door dit verzoek wordt de termijn opgeschort tot het tijdstip dat het gevraagde bewijs is geleverd.

6.6.7. Indien de Stichting geen gevolg wenst te geven aan een verzoek als bedoeld in dit artikel doet hij hiervan – gemotiveerd - schriftelijk mededeling aan de betrokkene, binnen een maand na ontvangst van het verzoek.

6.7. <u>Beperkingen</u>

6.7.1. De reikwijdte van verplichtingen van de Stichting enerzijds en de rechten van betrokkene anderzijds kunnen zijn beperkt op grond van wet- en regelgeving die

op de Stichting en/of zijn verwerkers van toepassing zijn.

6.8. <u>Recht op het indienen van een klacht</u>

6.8.1. De betrokkene die zich niet kan verenigen met de afwijzing van zijn verzoek als bedoeld in dit artikel kan zich wenden tot de externe klachtencommissie zoals bedoeld in de klachtenregeling van de Stichting of de Autoriteit Persoonsgegevens benaderen met een verzoek tot bemiddeling.

Artikel 7. Beveiliging

7.1. De Stichting hanteert het voor de onderwijssector vastgestelde normenkader bij het vaststellen van passende technische en organisatorische maatregelen waartoe de Verordening verplicht.

7.2. De Stichting treft maatregelen die een effectief beschermingsniveau bieden, afhankelijk van de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. Daarbij rekening houdend met de stand van de techniek en de uitvoeringskosten. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

Artikel 8. De verwerker

8.1. De verwerkers zijn degenen die op basis van een overeenkomst voor of namens de Stichting gegevens verwerken.

8.2. De verwerker verwerkt de gegevens op de wijze zoals overeengekomen in een verwerkersovereenkomst tenzij de verwerker die gegevens verwerkt bij het gebruik van leermiddelen, toetsen, school- en leerlinginformatiemiddelen (zoals gedefinieerd in de Model Verwerkersovereenkomst behorend bij het Convenant Digitale Onderwijsmiddelen). In dat geval verwerkt de verwerker de gegevens zoals voorgeschreven in de Model Verwerkersovereenkomst eventueel met inachtneming van de aanvullingen en wijzigingen zoals opgenomen in bijlage 3 behorend bij de model verwerkersovereenkomst.

8.3. De verwerker is verantwoordelijk voor het juiste gebruik van de nodige voorzieningen om de bescherming van de persoonlijke levenssfeer van de personen van wie gegevens in de persoonsregistratie zijn opgenomen, in voldoende mate te waarborgen, zoals aangegeven en beschreven in de verwerkersovereenkomst.

8.4. De Functionaris Gegevensbescherming ziet erop toe dat de in het vorige lid bedoelde voorzieningen worden getroffen en in acht worden genomen.

Artikel 9. Inbreuk op de beveiliging

9.1. Indien zich binnen de organisatie van de Stichting of bij een door de Stichting ingeschakelde verwerker een inbreuk op de beveiliging voordoet, waarbij een aanzienlijke kans bestaat op verlies of onrechtmatige verwerking van persoonsgegevens die door de Stichting worden verwerkt, dan wel dit verlies of onrechtmatige verwerking zich daadwerkelijk voordoet, zal de Stichting daarvan melding doen bij de Autoriteit Persoonsgegevens, tenzij kan worden aangetoond dat het onwaarschijnlijk is dat deze inbreuk risico's voor de rechten en vrijheden van natuurlijke personen met zich brengt.

9.2. De Stichting zal iedere inbreuk op de beveiliging als bedoeld in artikel 9.1. documenteren, ongeacht of deze wordt gemeld bij de AP.

9.3. Indien de inbreuk een hoog risico voor de rechten en vrijheden van betrokkene inhoudt, stelt de Stichting ook de betrokkene onverwijld in kennis van inbreuk. Deze mededeling kan achterwege blijven indien:
- de persoonsgegevens versleuteld zijn en niet toegankelijk voor derden;
- er inmiddels maatregelen getroffen zijn die het hoge risico hebben weggenomen;
- de mededeling een onevenredige inspanning vergt. Een openbare mededeling kan dan volstaan.

9.4. Bij het vaststellen of sprake is van een inbreuk op de beveiliging en of melding daarvan moet worden gedaan bij de Autoriteit Persoonsgegevens hanteert de

Stichting de procedures die zijn opgenomen in het handboek en protocol Datalekken.

Artikel 10. Klachten

10.1. Indien de betrokkene van mening is dat de bepalingen van de Verordening en overige wet- en regelgeving en (onderwijs)gedragscodes zoals uitgewerkt in dit reglement niet door de instelling worden nageleefd dient hij/zij zich te wenden tot de FG.

10.2. Indien de ingediende klacht voor de betrokkene niet leidt tot een voor hem/haar acceptabel resultaat, kan hij zich wenden tot de Autoriteit Persoonsgegevens dan wel tot de rechter.

10.3. (Ouders/verzorgers van) leerlingen en medewerkers kunnen zich tevens wenden tot de externe klachtencommissie waarbij de Stichting is aangesloten (zoals vermeld in de Klachtenregeling van de Stichting.

Artikel 11. Inwerkingtreding, wijziging en citeertitel

11.1. Dit reglement kan aangehaald worden als '*Privacyreglement'* en treedt in werking op vaststellingsdatum van het Privacybeleid van Stichting Invitare Openbaar Onderwijs.

11.2. Het reglement is vastgesteld door de Stichting met instemming van de gemeenschappelijke medezeggenschapsraad en vervangt eventuele vorige versies.

11.3. Het reglement zal periodiek worden geëvalueerd met beide geledingen van de gemeenschappelijke medezeggenschapsraad en kan indien dit wordt gewenst of nodig is om de AVG correct na te leven, worden gewijzigd, nadat instemming van de medezeggenschapsraad is verkregen.

<u>Artikelsgewijze toelichting ten behoeve van implementatie van het reglement</u>

Artikel 1. Begripsbepalingen
De meeste begripsbepalingen vloeien direct voort uit de AVG, de Wet op het Primair onderwijs en de Wet op de expertisecentra.

Autoriteit Persoonsgegevens (AP)
De Autoriteit Persoonsgegevens ziet, op grond van de AVG, als onafhankelijke instantie erop toe, dat persoonsgegevens zorgvuldig worden gebruikt en beveiligd en dat de privacy van burgers gewaarborgd blijft. Wanneer een organisatie zich niet houdt aan de wet, kan de autoriteit maatregelen nemen. De AP kan ook boetes opleggen.

Betrokkene
De persoon wiens gegevens worden verwerkt, wordt in de AVG 'de betrokkene' genoemd. Indien de school ook gegevens van andere betrokkenen (bijvoorbeeld: donateurs etc.) verwerkt, dient het modelreglement daarop te worden aangepast.

Dienst van de informatiemaatschappij
Kortgezegd iedere internetdienst (bijvoorbeeld: digitale leermiddelen, spellingapps, etc.). Een dienst is een dienst van de informatiemaatschappij als de dienst elektronisch wordt geleverd zonder dat de aanbiedende partij en ontvangende partij gelijktijdig aanwezig zijn en de dienst enkel wordt geleverd omdat de afnemer (school/docent/leerling) daarom vraagt.

Leerling- of personeelsnummer
Niet zijnde het Burgerservicenummer. Een nummer dat binnen de administratie verwijst naar de gegevens van één persoon en dat wordt gebruikt om die gegevens op effectieve en efficiënte wijze te kunnen raadplegen en verwerken. Hiermee kunnen de persoonsgegevens die worden verwerkt van een persoon worden geminimaliseerd. Het leerling- en personeelsnummer kan dan dienen als koppelinstrument tussen de verschillende bestanden/verwerkingen zonder dat steeds de naam, etc. van de betrokkenen hoeft te worden verwerkt.

In dit model wordt als mogelijkheid genoemd gegevens te verwerken op basis van een personeels- en leerlingnummer. Het gebruik van een persoonsgebonden nummer kan ertoe bijdragen dat minder gegevens van betrokkenen hoeven te worden verwerkt en dat de toegang tot vertrouwelijke gegevens binnen en buiten de organisatie eveneens tot een minimum kan worden beperkt.

Deze gedachte ligt ook ten grondslag aan het wetsvoorstel '*Pseudonimisering leerlinggegevens'*. Met dit wetsvoorstel wordt het voor onderwijsinstellingen in alle sectoren mogelijk om het persoonsgebonden nummer van een onderwijsdeelnemer te gebruiken ten behoeve van het genereren van een pseudoniem voor deze onderwijsdeelnemer in het kader van de toegang tot en het gebruik van digitale leermiddelen alsmede het digitaal afnemen van toetsen. Daarnaast voorziet het wetsvoorstel in een grondslag om voor andere doeleinden andere pseudoniemen te genereren.

Personeel
Personen in dienst van of werkzaam (geweest) voor de Stichting: zij die ten behoeve van de Stichting werkzaamheden verrichten of hebben verricht. Hieronder vallen niet alleen de personen die een akte van benoeming/aanstelling hebben, maar ook uitzendkrachten, stagiaires, vrijwilligers, personen die bij de Stichting zijn gedetacheerd, ouders, oud-medewerkers, etc.

Dienstverleners daarentegen zijn veelal verwerker (bijvoorbeeld het administratiekantoor) of medeverwerkingsverantwoordelijke (zoals de accountant). De arbodienst kan zowel worden aangemerkt als verwerker én verwerkingsverantwoordelijke.

Persoonsgegevens
Alle gegevens die informatie kunnen verschaffen over een identificeerbare natuurlijke persoon zijn persoonsgegevens in de zin van de AVG. Om te bepalen of een persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren.

De aard van sommige persoonsgegevens brengt met zich mee dat de verwerking ervan een grote inbreuk kan vormen op de persoonlijke levenssfeer van de betrokkene, omdat

die gegevens gevoelige informatie over iemand verschaffen. De AVG noemt deze gegevens bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn alle persoonsgegevens die informatie verschaffen over iemands:

- godsdienst of levensovertuiging;
- ras (etniciteit of afkomst);
- genetische kenmerken;
- biometrische kenmerken;
- gezondheid;
- seksuele leven; en
- lidmaatschap van een vakvereniging.

Verder zijn bijzondere persoonsgegevens:

- strafrechtelijke persoonsgegevens; en
- persoonsgegevens over onrechtmatig of hinderlijk handelen waarvoor een verbod is opgelegd (bijvoorbeeld een straatverbod).

Hoofdregel is dat bijzondere persoonsgegevens niet mogen worden verwerkt. De AVG kent een aantal algemene en een aantal specifieke uitzonderingen op dit verbod. Voor het onderwijs is de belangrijkste dat verwerking van bijzondere persoonsgegevens op grond van de AVG is toegestaan indien de verwerking noodzakelijk is met het oog op het verstrekken van zorg, behandeling of het beheren van diensten dan wel op een andere wettelijke grondslag (uitvoeringswet AVG).

De verwerkingsverantwoordelijke dient aan te geven om welke gegevens het gaat. De AVG verplicht verwerkingsverantwoordelijken daarnaast om de gegevens te classificeren als openbaar, vertrouwelijk of gevoelig.

Stichting/bevoegd gezag
In dit reglement komt de term bevoegd gezag niet meer terug. Hoofdregel in de Wpo is dat de rechtspersoon die de school in stand houdt het bevoegd gezag is tenzij de gemeente (of de gemeenschappelijke) regeling de school in eigen beheer in stand houdt (artikel 1 Wpo).

Verwerker
Onderscheid wordt gemaakt tussen in- en externe verwerkers (in het register van verwerkingsactiviteiten aangeduid als 'Ontvangers'). Interne verwerkers zijn het personeel van de Stichting. Externe verwerkers zijn bijvoorbeeld het administratiekantoor. Soms zijn externe verwerkers ook zelf verwerkingsverantwoordelijke met betrekking tot de persoonsgegevens, zoals de Arbodienst. Naast de taken die zij in opdracht en namens de verwerkingsverantwoordelijke uitvoeren op basis van de afgesloten overeenkomst, verwerken zij medische gegevens op basis van artikel 7:464 Burgerlijk Wetboek (BW), die de Wet Geneeskundige Behandelovereenkomst (WGBO) naar analogie van toepassing verklaart. Ratio van deze bepaling is dat de rechten van de patiënt niet alleen in zuiver contractuele behandelingssituaties, maar ook in andersoortige situaties waarin een patiënt wordt onderworpen aan een geneeskundige handeling bescherming behoeven.

Als besloten wordt om feitelijke handelingen met betrekking tot gegevensverwerking door een verwerker te laten verrichten, zal met die verwerker een relatie worden aangegaan. De AVG stelt eisen aan de keuze van een verwerker en aan de manier waarop de

relatie met die verwerker vastligt. De AVG eist in artikel 32 dat de onderdelen die betrekking hebben op de bescherming van persoonsgegevens en op de beveiligingsmaatregelen, schriftelijk worden vastgelegd.

Verwerking van persoonsgegevens
Het gaat erom of iemand enige feitelijke macht of invloed, al dan niet via een computersysteem, over de gegevens kan uitoefenen. Iemand moet een handeling met de gegevens kunnen verrichten. Als iemand geen macht of invloed kan uitoefenen op de persoonsgegevens, valt deze verwerking niet onder de AVG.

Verwerkingsverantwoordelijke
De verwerkingsverantwoordelijke is de Stichting dat wordt vertegenwoordigd door het (college van) bestuur van de Stichting.

Artikel 2. Verantwoordelijkheden
De AVG richt zich tot de verwerkingsverantwoordelijke, in casu het schoolbestuur dat verantwoordelijk is voor een gegevensbeschermingsbeleid conform de in dit artikel genoemde uitgangspunten. In het beleidskader wordt verwezen naar de beleidsdocumenten die daarbij ondersteunend kunnen zijn. In het beleidskader en in beleidsdocumenten zelf wordt ook verwezen naar producten en beleidsdocumenten ontwikkeld door Kennisnet met bronvermelding en de hyperlink waarmee de documenten op de website van Kennisnet zijn terug te vinden.

Artikel 3. Functionaris Gegevensbescherming (FG)
De verplichting tot het aanstellen van een FG geldt voor overheidsinstanties en publieke organisaties, ongeacht het type persoonsgegevens dat ze verwerken. Het kan dan bijvoorbeeld gaan om de Rijksoverheid, gemeenten of provincies maar ook om zorg- en onderwijsinstellingen. In de AVG wordt geen definitie gegeven van "overheidsinstantie of –orgaan". De Artikel 29-werkgroep (de gezamenlijke Europese toezichthouders) heeft een richtlijn gepubliceerd over het aanstellen van een FG. In deze richtlijn wordt voor het begrip "overheidsinstantie of –orgaan" verwezen naar de definitie van "publiekrechtelijke instelling". Een publiekrechtelijke instelling is een aanbestedende dienst in de zin van de Aanbestedingsrichtlijn. Op grond van die definitie en bijlage uit deze richtlijn, kan ook een bijzondere onderwijsinstelling worden gekwalificeerd als een aanbestedende dienst als de financiering van een school voor meer dan de helft van de begroting afkomstig is van de overheid.

Een organisatie is overigens ook verplicht een FG aan te stellen als zij regelmatig en stelselmatig betrokkenen observeren. Scholen voldoen snel aan deze eis, aangezien zij vaak leerlingvolgsystemen gebruiken. Daarnaast heeft het verwerken van bijzondere en strafrechtelijke gegevens op 'grote schaal' ook tot gevolg dat een organisatie een FG moet aanstellen. Bijzondere persoonsgegevens zijn gegevens die iets zeggen over iemands ras, godsdienst, seksuele leven, politieke opvatting, gezondheid, maar ook genetische gegevens (zoals DNA) en biometrische gegevens (bijvoorbeeld vingerafdrukken). Elke onderwijsinstelling verwerkt in ieder geval enkele bijzondere persoonsgegevens van leerlingen in een onderwijskundig rapport. Bijvoorbeeld of een leerling ADHD heeft, dyslectisch of depressief is. Onderwijsinstellingen voldoen (in bijna alle gevallen) aan de drie verschillende vereisten om een FG aan te moeten stellen. Let op: het voldoen aan één van de drie vereisten is al genoeg om verplicht een FG aan te moeten stellen.

Artikel 4. Informatie en toegang
De Verordening verplicht de verwerkingsverantwoordelijke om de informatie over de gegevensverwerking eenvoudig toegankelijk en begrijpelijk te maken.

Artikel 5. Categorieën van betrokkenen, doeleinden en persoonsgegevens
Om de Verordening na te leven en te voldoen aan de in de Verordening opgenomen verplichtingen is het van belang om in kaart te brengen welke gegevens van welke personen, met welk doel worden verwerkt en op welke grondslag. Het gaat in dit verband nadrukkelijk om gegevens die onderdeel uitmaken van een bestand als gedefinieerd in dit reglement.

Grondslagen voor het verwerken
Een gegevensverwerking dient in overeenstemming met de wet, behoorlijk en zorgvuldig te geschieden. De persoonsgegevens moeten verzameld zijn voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De verwerking moet een rechtmatige grondslag hebben en mag niet onverenigbaar zijn met het doel waarvoor de werkgever de gegevens heeft verzameld. Artikel 6 lid 1 AVG bevat een opsomming van de enige gronden voor een toelaatbare gegevensverwerking. Met verwerken wordt bedoeld alle handelingen met persoonsgegevens vanaf het verzamelen tot aan het vernietigen. Verstrekken is een vorm van verwerken. De wet kent een limitatief aantal grondslagen op grond waarvan persoonsgegevens mogen worden verwerkt. Deze zijn in de volgorde van artikel 6 lid 1 van de AVG:

Toestemming (artikel 6 lid 1a AVG)
Toestemming is de eerste grondslag op basis waarvan persoonsgegevens mogen worden verwerkt en/of verstrekt aan derden. Deze toestemming kan echter op elk moment worden ingetrokken. Daarmee vervalt de grondslag van de verstrekking en is verwerking van de persoonsgegevens daarna onrechtmatig. Instemming van de (Gemeenschappelijke) Medezeggenschapsraad voor een bepaalde verstrekking vervangt de individuele toestemming niet.

Het spreekt voor zich dat toestemming vrijwillig moet worden gegeven. Binnen een arbeidsrelatie mag een werkgever echter er niet te snel vanuit gaan dat de werknemer deze toestemming daadwerkelijk vrijwillig heeft gegeven. Geadviseerd wordt om deze grondslag slechts bij uitzondering te gebruiken – wanneer één van de andere grondslagen geen uitkomst kan bieden - en/of in het geval dat uitsluitend de werknemer belang heeft bij verwerking van de gegevens. Denk bijvoorbeeld aan een kortingsactie voor personeel bij de plaatselijke sportschool. Als de verwerkingsverantwoordelijke toestemming vraagt, moet deze duidelijk uitleggen waarvoor de toestemming nodig is en wat de gevolgen zijn van het geven van toestemming.

Voor toestemming gelden drie voorwaarden. De toestemming moet 'vrij' en niet onder druk zijn gegeven. Toestemming moet ondubbelzinnig zijn. Dat betekent dat een school niet uit mag gaan van het principe 'wie zwijgt, stemt toe'. Bij ondubbelzinnige toestemming moet elke twijfel zijn uitgesloten. Het moet dus volstrekt duidelijk zijn óf de betrokkene toestemming heeft gegeven. En de toestemming moet specifiek zijn, voor een specifieke verwerking en voor een specifiek doel. Leerlingen of ouders/voogd moeten hun toestemming ook altijd weer kunnen intrekken.

Verwerkingen waarvoor in ieder geval voorafgaande toestemming is vereist:

1. Foto's en beeldmateriaal van leerlingen

De Autoriteit Persoonsgegevens heeft de onderwijssector op 30 augustus 2017 een brief gestuurd met daarin aanwijzingen met betrekking tot het gebruik van foto's en video's van leerlingen. De AP geeft aan dat zij van mening is dat dit gebruik uitsluitend is toegestaan indien scholen daarvoor toestemming nodig hebben van elke leerling dan wel zijn ouders als de leerling jonger is dan 16 jaar.

2. Diensten van de informatiemaatschappij die rechtstreeks aan de leerling worden aangeboden

De AVG verplicht dienstverleners van de informatiemaatschappij om voor deze verwerkingen voorafgaande toestemming te vragen. Voor dit type verwerkingen bepaalt de AVG dat leerlingen die 16 jaar zijn zelf toestemming moet worden gevraagd. Voor leerlingen die jonger zijn dan 16 moet de ouder om toestemming worden gevraagd. Dat laatste geldt ook voor andere verwerkingen echter alleen voor zover die op basis van de toestemmingsgrondslag plaats vinden. Dit volgt niet uit de AVG zelf maar uit de (concept)uitvoeringswet AVG.

Delen van informatie met ouders

Ouders hebben een informatierecht dat is vastgelegd in het BW en in de onderwijswetten. Informatie die met ouders wordt gedeeld betreft:

a. administratieve gegevens;
b. gegevens over onderwijshistorie, leerresultaten en stage- en werkervaring;
c. gegevens over de sociaal-emotionele ontwikkeling en het gedrag;
d. gegevens met betrekking tot de gegeven of geïndiceerde begeleiding;
e. gegevens omtrent de verzuimhistorie.

Dit informatierecht geldt ten aanzien van minderjarige kinderen, die nog niet de leeftijd van 18 jaar hebben bereikt. Omdat de school met het verstrekken van deze informatie uitvoering geeft aan een wettelijke verplichting, is voorafgaande toestemming van de leerling niet nodig, ook niet als deze de leeftijd van 16 jaar nog niet heeft bereikt.

Uitvoeren van een overeenkomst (artikel 6 lid 1b AVG)

Gegevens kunnen worden verstrekt aan derden indien dit noodzakelijk is voor het aangaan van en het uitvoeren van een (arbeids)overeenkomst. Er wordt vanuit gegaan dat ouders, leerlingen en medewerkers bij het sluiten van de overeenkomst zich ervan bewust zijn dat bepaalde gegevens moeten worden verstrekt.

Hoewel de rechtspraak en rechtsliteratuur daarover niet eensluidend zijn, is inmiddels de overheersende opvatting dat het onderwijs tussen leerling/ouders en de school op bijzondere grondslag eveneens op basis van een overeenkomst wordt verstrekt. Over het openbaar onderwijs is de literatuur niet eenduidig.

Omdat voor de meeste gegevensverwerkingen geldt dat deze zijn ingekaderd in wet- en regelgeving en noodzakelijk zijn met het oog op de nakoming van wettelijke verplichtingen dan wel vanwege de uitvoering van een publieke taak, is ervoor gekozen zoveel mogelijk de gegevensverwerkingen te baseren op de op de onderwijsinstelling rustende wettelijke verplichting/publieke taak en – met uitzondering van de inschrijving van de leerling, niet te baseren op de (onderwijs)overeenkomst.

Wettelijke verplichting (artikel 6 lid 1c AVG)
De onderwijsinstelling kan verplicht zijn om bepaalde persoonsgegevens te verstrekken die noodzakelijk zijn voor de uitvoering van een wettelijke plicht. Ten aanzien van leerlingen zijn deze wettelijke verplichtingen neergelegd in de sectorwetten en de daarop gebaseerde uitvoeringsregelgeving. De onderwijsinstelling is onder andere op grond van artikel 47 van de Algemene wet inzake rijksbelastingen verplicht om de fiscus te voorzien van alle gegevens die van belang kunnen zijn voor de belastingheffing. Ook moet deze op grond van een bevel van de rechter-commissaris in strafzaken verplicht bepaalde persoonsgegevens van een verdacht personeelslid te verstrekken. Ook intern kan de verplichting tot het verwerken van gegevens bestaan, zoals aan de medezeggenschapsraad met het oog op te organiseren verkiezingen of met het oog op het verzorgen van onderwijs, dat eveneens plaats vindt op grond van wettelijke verplichtingen, neergelegd in de Wet op het primair onderwijs en daarop gebaseerde regelgeving.

Vitaal belang (artikel 6 lid 1d AVG)
Deze grond komt niet terug in het reglement, maar kan wel worden gebruikt om gegevens te verstrekken als daarmee een vitaal belang van een leerling of personeelslid is gediend. Gedacht moet worden aan situaties waarin met spoed gehandeld moet worden in het (gezondheids)belang van de betrokkene.

Publiekrechtelijke taak (artikel 6 lid 1e AVG)
Artikel 6, onder lid 1e, maakt gegevensverwerking mogelijk voor zover deze noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door de school dan wel het bestuursorgaan aan wie de gegevens worden verstrekt.

Gerechtvaardigd belang (artikel 6 lid 1f AVG)
Deze grondslag betreft een restbepaling. In sommige gevallen bestaat de noodzaak voor het behartigen van een gerechtvaardigd belang van de verwerkingsverantwoordelijke en/of derde om gegevens te verwerken. Het belang op privacy van personeel of leerlingen dient daarvoor dan te wijken. Er dient dan ook steeds een belangenafweging te worden gemaakt waarbij onder meer van belang is wat de aard van de verwerking is, wat voor gegevens er worden verwerkt en hoe deze worden beveiligd. Voor publiekrechtelijke instanties, waartoe in de regel ook het onderwijs wordt gerekend, geldt dat het gerechtvaardigd belang geen grondslag kan vormen voor de kerntaken, omdat daarvoor zou moeten zijn voorzien in een wettelijke grondslag.

Artikel 6. Rechten van betrokkenen
De informatie met betrekking tot dit reglement en de uitvoering ervan die voor de betrokkenen is bestemd moet eenvoudig toegankelijk en begrijpelijk te zijn. De onderwijsinstelling dient op eigen initiatief aan de betrokkenen kenbaar te maken welke verwerkingen van persoonsgegevens hij heeft en waarom. Dit is een belangrijk instrument in de AVG om het gegevensverkeer transparant te maken. Betrokkenen hoeven niet geïnformeerd te worden als hun gegevens worden vastgelegd of verstrekt op grond van een wettelijke plicht. De betrokkene moet op een gemakkelijke wijze zijn rechten op basis van de Verordening en het reglement kunnen uitoefenen. Verzoeken dienen in beginsel kosteloos in behandeling te worden genomen. Betrokkenen dienen middelen te krijgen waarmee verzoeken elektronisch kunnen worden ingediend.

Artikel 7. Beveiliging

De AVG verplicht de verwerkingsverantwoordelijke zorg te dragen voor '*een passend beveiligingsniveau'* tegen verlies of tegen enige vorm van onrechtmatige verwerking van persoonsgegevens. De term '*een passend beveiligingsniveau'* geeft in dit verband aan, dat een afweging wordt gemaakt tussen de te leveren beveiligingsinspanning (waaronder ook de kosten!) en de gevoeligheid van de persoonsgegevens. Ook als de verwerkingsverantwoordelijke een verwerker inschakelt voor de verwerking van persoonsgegevens moet hij zorgdragen voor, en toezien op, een afdoende beveiliging van de persoonsgegevens door de verwerker. Dat betreft dan zowel de beveiliging van de apparatuur en programmatuur van de verwerker als de bescherming van de gegevens die door de verschillende communicatienetwerken reizen. Over de beveiliging van persoonsgegevens is meer informatie te vinden op de website van de autoriteit persoonsgegevens.

Stichting Kennisnet ontwikkelt voor de sector PO/VO een normenkader op basis van de ISO-normen, waarin per privacy-norm (afkomstig uit de AVG) of uit de ISO 27001/27002 is beschreven wat scholen ten minste moeten regelen voor een passend beveiligingsniveau. Tot het moment dat dit gereed is, is het advies om gebruik te maken van het normenkader dat is ontwikkeld voor het MBO door saMBO-ICT (bijlage VIII).

Artikel 32 AVG eist dat de onderdelen die betrekking hebben op de bescherming van persoonsgegevens en op de beveiligingsmaatregelen, schriftelijk worden vastgelegd (bijlage VIII).

Artikel 9. Inbreuken op de beveiliging

Voor een uitgebreide toelichting op de wijze van het vaststellen of sprake is van een datalek en/of deze gemeld moet worden wordt verwezen naar de voorschriften en werkwijzen die zijn opgenomen in het handboek en protocol Datalekken (bijlage XIII).

Artikel 10. Klachten

Door betrokkenen met een klacht te wijzen op de mogelijkheid tot klachtafwikkeling door de klachtencommissie waarbij de school is aangesloten, kunnen klachten bij de AP voorkomen worden.

Bijlage 2: Overzicht in- en externe communicatie

Onderstaand een aantal tabellen waarmee helder gemaakt wordt wie betrokken is bij de in- en externe communicatie betreffende leerlingen en wat het doel hiervan is.

Tabel 1: Overzicht van persoonsgegevens leerlingen

Categorie Persoonsgegevens	Doel van registratie
Naam, voornamen, voorletters, geslacht, geboortedatum, adres, postcode, woonplaats van leerling	Onderwijs geven en organiseren; leermiddelen verstrekken, uitvoering wet;
Telefoonnummer en soortgelijke gegevens van de leerling die bedoeld zijn voor de communicatie	Informatie geven
Burgerservicenummer	Uitvoering wet
Nationaliteit	Uitvoering wet
Naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens van de ouders of een andere wettelijk vertegenwoordiger of verzorger van de leerling	Informatie geven
Opleidingsniveau van de ouders van de leerling	Uitvoering wet
Gegevens over de gezondheid of het welzijn van de leerling, voor zover die noodzakelijk zijn voor de ondersteuning	Leerlingen begeleiden
Gegevens over de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor de school, het onderwijs of de te geven ondersteuning	Leerlingen begeleiden
Gegevens over de aard en het verloop van het onderwijs en ondersteuning en de behaalde leerresultaten	Leerlingen begeleiden
Schoolgegevens waaronder naam school, naam leerkracht, naam intern begeleider, groep, tijdstip van inschrijving bij deze school, naam van de indiener van de aanmelding bij het samenwerkingsverband als dat het geval is, schoolloopbaan, en rapportage vanuit primair onderwijs	Onderwijs geven en organiseren; Leerlingen begeleiden
Aanleiding voor de aanmelding bij het samenwerkingsverband als dat het geval is, relevantie screenings- en onderzoeksgegevens en omschrijving van de problematiek die aan de orde is;	Leerlingen begeleiden
Activiteiten die door de school zijn ondernomen rond de betreffende leerling en de resultaten hiervan	Leerlingen begeleiden
Bestaand of relevantie afgesloten hulpverleningscontacten en namen van contactpersoon	Leerlingen begeleiden

Relevante persoonsgegeven die door externe partijen worden verstrekt over de aangemelde problematiek van de leerling	Leerlingen begeleiden
Relevante financiële gegevens over bijvoorbeeld schoolgeld	Berekenen, vastleggen en innen van schoolgelden.

Tabel 2: Overzicht vertrouwelijke communicatie over leerlingen ten behoeve van het realiseren van onderwijs en ondersteuning door directie, IB-er en leerkracht (soms in het kader van het leerproces van de leerkracht, stagiair of student). Met * aangegeven voor een beperkt aantal leerlingen van toepassing met ** aangegeven dat er sprake is van toestemming van ouders

	Verbaal	*Schriftelijk*	*Elektronisch*
INTERN			
Personeel (directie, IB-er, leerkracht en collega leerkrachten en het bevoegd gezag)	X	X	X
Andere leerlingen (individueel en als groep)	X		
Andere ouders / verzorgers (individueel en als groep)	X		
Hulpouders en vrijwilligers	X		
Studenten en stagiairs	X	X	X
Ouderraad	X	X	X
Mosagroep		x	x
Vertrouwenspersoon / contactpersoon i.k.v klachtenregeling	x		
EXTERN			
Cfi (ministerie OC&W)			X
Arbeidsinspectie (m.b.t. ongevallen)		X	
Gemeente (i.k.v. financiering)		X	
Inspectie van Onderwijs	X	X	X
Leerplichtambtenaar*	X	X	X
Voor-/naschoolse opvang*	X	X	X
Medisch kinderdagverblijf*/**	X	X	X
Peuterspeelzaal/kinderopvang*/**	X	X	X
Voortgezet onderwijs	X	X	X
Andere scholen (bij verandering van school)*/**	X	X	X
Logopedie*/**	X	X	X
Fysiotherapie */**	X	X	X
Schoolarts / Jeugdgezondheidszorg (GGD)	X	X	X
Begeleiders i.k.v. arrangementen*/**	X	X	X
OSL Noord Limburg / Stromenland LVC	X	X	X
Externe deskundigen*/**	X	X	x
Trainingsinstellingen t.b.v. medewerkers / studenten / stagiairs	X	X	X
Jeugdzorg*	X	X	
Curium (academisch centrum voor kinder- en jeugdpsychiatrie)*	X	X	
Vertrouwensarts*	X	X	
Veilig Thuis	x	X	

Tabel 3: Overzicht registratiemethodes ten behoeve van de voortgang van het onderwijs.

	verbaal	*schriftelijk*	*elektronisch*
Leerlingenadministratie:			
Met de administratie van de leerlingengegevens voldoen de scholen aan de verplichtingen vanuit het bekostigingsbesluit van de Wet Primair Onderwijs. Deze administratie bevat de persoonsgegevens en de gegevens rond de inschrijving, uitschrijving en het verzuim.		X	X
Leerlingvolgsysteem:			
Dit betreft voornamelijk de toetsresultaten plus de registratie van de eventuele acties die hierop zijn genomen. Het leerlingvolgsysteem heeft een duidelijke relatie met de leerlingendossiers.		X	X
Leerlingendossiers:			
Deze dossiers bevatten rapporten, uitslagen van toetsresultaten, gegevens uit het leerlingvolgsysteem, verslagen van gesprekken met ouders en afspraken die er over de leerling zijn gemaakt zoals bijvoorbeeld handelingsplannen.		X	X
Werkdossier t.b.v. de leerkracht / IB-er:			
In deze dossiers zitten voor betreffende (groeps)leerkrachten en IB-er relevante stukken voor betreffend schooljaar		X	X
Methode gebonden software			
De leermethodes bieden de mogelijkheid om lesstof te oefenen en om te toetsen in welke mate de leerlingen de lesstof beheersen.		x	x

Tabel 4: Overzicht openbare communicatieve uitingen over algemene schoolaangelegenheden waarbij beeldmateriaal, verhaaltjes e.d. van leerlingen kunnen worden gebruikt.

	Verbaal	*Schriftelijk*	*Elektronisch beeld /geluidsregistratie*
Website		X	X
Schoolkrant		X	X
Schoolmededelingen		X	X
Schoolgids/schoolkalender		X	X
Lokale krant			X
Lokale tv	X		X
Lokale radio	X		X
Ouderportal			x

Tabel 5: Overzicht van toegangsrechten interne verwerkers

Overzicht van diegenen die toegang hebben tot de persoonsregistratie zoals bedoeld in artikel 4 van het Privacyreglement:

Functie	Toegang tot welke persoonsgegevens
Het bestuur	Alle gegevens van het personeel, sollicitanten, leerlingen en hun ouder(s)/verzorger(s), leden van het toezichthoudend orgaan en overig betrokkenen.
Directeur	Alle gegevens van personeel werkzaam op de betreffende vestiging, sollicitanten voor op de vestiging vacante posities, alle gegevens van leerlingen en hun ouder(s)/verzorger(s) van de betreffende vestiging.
Functionaris Gegevensbescherming	Alle gegevens van het personeel, sollicitanten, leerlingen en hun ouder(s)/verzorger(s), leden van het toezichthoudend orgaan en overige betrokkenen.
Stafmedewerker Personeel en PSA-medewerkers (van de Mosagroep)	Alle gegevens van het personeel en sollicitanten.
Stafmedewerker Financiën en FZ-medewerkers (van de Mosagroep)	Alle gegevens van het personeel die noodzakelijk zijn voor de uitvoering van de salarisadministratie, of voor de uitbetaling van gemaakte reiskosten van sollicitanten, NAW-gegevens van leerlingen en hun ouder(s)/verzorger(s).
Preventiemedewerker	Gegevens nodig voor het uitvoeren van de wet Poortwachter, NAW-gegevens van het personeel.
Bestuurssecretariaat	NAW-gegevens van personeel, leerlingen en hun ouder(s)/verzorger(s).
ICT-coach en ICT-er van @Land van Cuijk	Alle gegevens van het personeel, leerlingen en hun ouder(s)/verzorger(s) van de betreffende vestiging, LVS / LAS voor zover noodzakelijk voor de uitvoering van de functie.
Administratief medewerker	Alle NAW-gegevens van het personeel, leerling en hun ouders/verzorgers, leerresultaten, aanwezigheidsregistratie, LVS
Leraren (en langtijdelijke invallers), leraarondersteuners en onderwijsassistenten	Alle gegevens van de leerlingen van de betreffende vestiging en de ouder(s)/verzorger(s) van de leerlingen aan wie zij lesgeven, cijfers, aanwezigheidsregistratie, LVS / LAS.
Intern begeleider (Ib'er)	Alle gegevens van de leerlingen aan wie leraren lesgeven en daarin door de intern begeleider worden ondersteund, cijfers, LVS.
Leerlingen	Voortgang in de onderwijssoftware en toegang de eigen online-cloud
Ouders	De NAW-gegevens, leerling dossier, behaalde leerresultaten en aanwezigheidsregistratie van de eigen kinderen, de eigen persoonsgegevens.
Zorgverleners	Gegevens van de leerlingen die zij begeleiden: de NAW-gegevens van de ouder(s)/verzorger(s) en de leerresultaten, aanwezigheidsregistratie en LVS.
Conciërges	De NAW-gegevens van personeel
Leden Raad van Toezicht (met name de voorzitter)	Alle gegevens van de bestuursleden
Stagiairs en korttijdelijke invalkrachten	Toegang tot onderwijssoftware

Bijlage 3: Bewaartermijnen

Deze bijlage bevat een overzicht van de van de door ons gehanteerde bewaartermijnen ten aanzien van de brondocumenten en brongegevens.

Tabel a: Categorie: leerlingen/oud-leerlingen (onderwijskundig)

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Het onderwijskundig rapport	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving
Gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving
Gegevens over leerprestaties van de leerling	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving
Verslagen van gesprekken met de ouders	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving
Psychologisch rapport	maximaal 2 jaar Wanneer het rapport wordt opgevraagd bij een school voor po in het kader van toelating tot een school voor vo minimaal 3 en maximaal 5 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving
Adresgegevens	maximaal 2 jaar (art. 19 lid 7 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk	maximaal 6 maanden (art. 32 lid 6 en art. 34 lid 5 Vrijstellingsbesluit Wbp *oud*)	moment van opname

De gehanteerde bewaartermijn voor alle hierboven genoemde stukken is 2 jaar.

Tabel b: Categorie: leerlingen/oud-leerlingen (administratief)

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Gegevens die nodig zijn om te berekenen hoeveel bekostiging de school ontvangt	minimaal 7 jaar (art. 172 lid 3 Wpo) Let op: verplichte wettelijke termijn!	na afloop van het schooljaar waarop de bekostiging betrekking heeft
Gegevens over in– en uitschrijving	minimaal 5 jaar (art. 9 Bekostigingsbesluit Wpo) Let op: verplichte wettelijke termijn!	datum van uitschrijving
Gegevens over verzuim en afwezigheid	minimaal 5 jaar (art. 9 Bekostigingsbesluit Wpo) Let op: verplichte wettelijke termijn!	datum van uitschrijving
Gegevens met betrekking tot de vergoeding van de kosten verbonden aan leerlingvervoer	maximaal 2 jaar (art. 21 lid 5 Vrijstellingsbesluit Wbp *oud*)	na afloop van het schooljaar waarop de verstrekking van de vergoeding betrekking heeft
Communicatiegegevens oud-leerlingen	Verwijderen op verzoek van de leerling of bij diens overlijden (art. 41 lid 5 Vrijstellingsbesluit Wbp *oud*)	datum van uitschrijving

Gehanteerde termijn voor alle hierboven genoemde stukken is 7 jaar

Tabel c: Categorie: personeel/oud-medewerkers/leden toezichthoudend orgaan

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Akte van aanstelling/ arbeidsovereenkomst	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband
Wijzigingen arbeidsovereenkomst	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband
Correspondentie inzake benoemingen, promotie, demotie	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband
Aanspraken in verband met de beëindiging van het dienstverband	maximaal 2 jaar (art. 9 lid 5 Vrijstellingsbesluit Wbp *oud*)	datum waarop aanspraken zijn geëindigd
Afspraken inzake werk MR	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde lidmaatschap
Burgerlijke staat werknemer	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband
Kopie getuigschrift	maximaal 2 jaar (art. 9 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband
Afspraken inzake opleidingen	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband
Aanvraag opleiding door werknemer	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband
Afspraken omtrent loopbaan	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband
Verslagen functionerings- en beoordelingsgesprekken	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband
Correspondentie UWV en bedrijfsarts	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband
Verslaglegging inzake Wet Verbetering Poortwachter	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband
Verzuimregistratie als werkgever eigenrisicodrager Ziektewet is	minimaal 5 jaar De bedrijfsarts moet de gegevens minimaal 10 jaar bewaren. In verband met eigen risicodragerschap WGA mogen de gegevens voor de duur van het WGA-traject bewaard blijven (10 jaar). (art. 3 lid 2 Regeling werkzaamheden, administratieve voorschriften en kosten eigen risicodragen ZW) Let op: verplichte wettelijke termijn!	einde dienstverband
Verslaglegging van correspondentie met betrekking tot problematische (financiële) privé-situatie	maximaal 2 jaar (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband
Loonbeslagen	tot opheffing (art. 9 lid 5 Vrijstellingsbesluit Wbp *oud*)	-
Correspondentie met betrekking tot jubilea	tot einde dienstverband (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	-
Correspondentie directie/PZ/direct leidinggevende	afhankelijk van ontslagsituatie bij einde dienstverband of tot maximaal 2 jaar daarna (art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	-
Identiteitspapieren van derden ingeleende vreemdelingen waarvoor een tewerkstellingsvergunning is verleend	minimaal 5 jaar (art. 15 lid 4 Wet arbeid vreemdelingen) Let op: verplichte wettelijke termijn!	einde dienstverband
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk	maximaal twee jaar (art. 32 lid 6 en art. 34 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband
Loonadministratie	minimaal 7 jaar (art. 52 lid 4 Algemene wet inzake rijksbelastingen) Let op: verplichte wettelijke termijn!	na afloop boekjaar
Loonbelastingverklaringen en kopie identiteitsbewijs uit loonadministratie	minimaal 5 jaar (art. 7.5. lid 4 en art. 7.9. lid 2 Uitvoeringsregeling loonbelasting) Let op: verplichte wettelijke termijn!	na einde kalenderjaar waarin dienstverband is geëindigd

Brondocument/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Communicatiegegevens oud-personeelsleden	Verwijderen op verzoek van het oud-personeelslid of bij diens overlijden (art. 41 lid 5 Vrijstellingsbesluit Wbp *oud*)	einde dienstverband

Gehanteerde bewaartermijn is gelijk aan de richtlijn

Tabel d: Categorie: sollicitanten

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Sollicitatiebrief, -formulier, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek	maximaal 4 weken zonder toestemming, maximaal 1 jaar met toestemming van de sollicitant (art. 5 lid 6 en art. 7 lid 5 Vrijstellingsbesluit Wbp *oud*)	na beëindiging sollicitatieprocedure of einde dienstverband/benoemingstermijn

Gehanteerde bewaartermijn is gelijk aan de richtlijn

Tabel e: Categorie: leveranciers

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Persoonsgegevens van (vertegenwoordigers van) leveranciers	maximaal 2 jaar (art. 13 lid 5 Vrijstellingsbesluit Wbp *oud*)	nadat de desbetreffende transactie is afgewikkeld

Gehanteerde bewaartermijn is gelijk aan de richtlijn

Tabel f: Categorie: huurders

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Persoonsgegevens van huurders	maximaal 2 jaar (art. 14 lid 5 Vrijstellingsbesluit Wbp *oud*)	maximaal 2 jaar nadat de huur is beëindigd

Gehanteerde bewaartermijn is gelijk aan de richtlijn

Tabel g: Categorie: alle bovengenoemde categorieën en bezoekers

Brondocumenten/brongegevens	Richtlijn bewaartermijn	Ingangsdatum bewaartermijn
Camera en videobeelden	maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten (art. 38 lid 6 Vrijstellingsbesluit Wbp *oud*)	moment van opname
Gegevens met betrekking tot het tijdstip, de datum en de plaats waarop de video-opnamen zijn gemaakt.	maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten (art. 38 lid 6 Vrijstellingsbesluit Wbp *oud*)	moment van opname
Registratielijsten bezoekers	niet langer dan nodig (art. 5 lid 1e AVG)	moment van registratie

ehanteerde bewaartermijn is gelijk aan de richtlijn

Bijlage 4: Overzicht verwerkingsovereenkomsten

Voor het personeel is de geactualiseerde lijst beschikbaar op Sharepoint. Ouders / verzorgers kunnen desgewenst een overzicht opvragen door een mail te sturen aan info@stichting-invitare.nl. Dit is het overzicht per 25 september 2018.

	Data	Contract met	Betreft scholen	Verwerkings-overeenkomst	bewerkingsover-eenkomst	door beide par-tijen ondertekend ondertekend
1	14-2-2017	Raet B.V.	Algemeen	x		ja
2	22-2-2017	CED groep	Algemeen		x	ja
3	14-7-2017	Gynzy	Elckerlyc, Startblok, Klimop		x	ja
4	31-8-2017	OSO	Algemeen		x	nee
5	8-11-2017	Bloon	Startblok		x	ja
6	1-2-2018	Avision	Hartenaas		x	ja
7	6-3-2018	VABO	Vervangingen (CPV)		x	ja
8	19-3-2018	G Suite		standaard con-tractvoorwaarden		nee
9	11-4-2018	Ricoh	De Wingerd	x		ja
10	30-4-2018	ParnasSys	Algemeen	x		ja
11	7-5-2018	Cito	Algemeen	x		ja
12	8-5-2018	Human Capital Alert	Algemeen	x		ja
13	8-5-2018	Human Capital Scan	Algemeen	x		ja
14	15-5-2018	Noordhoff Uigevers B.V.		x		ja
15	16-5-2018	Prowise	Algemeen	x		ja
16	22-5-2018	Momento, Heutink	Algemeen	x		ja
17	22-5-2018	Blink			x	ja
18	22-5-2018	ThiemeMeulenhoff B.V.	alle scholen		x	ja
19	22-5-2018	Uitgeverij Zwijsen B.V.	alle scholen behalve de Nienekes	x		ja
20	23-5-2018	Basis Poort		x		ja
21	12-6-2018	Spring, kinderopvang	Alle scholen behalve Hartenaas	x		ja
22	18-6-2018	Isy School BV	Klimop	x		ja
23	18-6-2018	Oefenweb		x		ja

24	18-6-2018	Jeelo B.V.		x		ja
25	20-6-2018	Malmberg B.V.	Algemeen	x		ja
26	20-6-2018	St. Bazalt		x		ja
27	25-6-2018	Bureau ICE B.V.	Algemeen en bestuur	x		ja
28	27-6-2018	Schoolwise, St. Biblio-theek Biblioplus			x	Nog niet
29	4-7-2018	ZuluDesk B.V.	Hartenaas en de Nienekes	x		ja
30	21-8-2018	678 Onderwijs Advise-ring B.V.		x		ja

Bijlage 5: Protocol datalekken

1. Inleiding

Om persoonsgegevens te mogen verwerken kent de AVG een aantal uitgangspunten. Deze uitgangspunten gelden voor elke school. Zonder al te eenvoudig over privacy te willen spreken, zijn de uitgangspunten samengevat tot vijf praktische vuistregels:

Doelbepaling en doelbinding: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen. In een bijlage van de eerdere Wbp is opgenomen wat enkele belangrijke doelen zijn voor het onderwijs, namelijk:

- de organisatie van het onderwijs en het begeleiden van het kind;
- het verstrekken of ter beschikking stellen van leermiddelen aan het kind;
- het bekend maken van informatie over de hierboven genoemde organisatie en leermiddelen;
- het bekend maken van de activiteiten van de instelling of het instituut op de eigen website;
- het berekenen, vastleggen en innen van gelden, zoals de vrijwillige ouderbijdrage;
- het behandelen van geschillen, of het doen uitoefenen van accountantscontrole;
- de uitvoering/toepassing van een wet, zoals de Wet op het Primair Onderwijs/Wet Kinderopvang.

Grondslag: verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.

Dataminimalisatie: bij de verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (dit noemen we proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (dit noemen we subsidiair). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk: aan ieder persoonsgegeven zit een houdbaarheid vast, die we bewaartermijn noemen.

Transparantie: het schoolbestuur legt aan betrokkenen (kinderen, hun ouders/verzorgers en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens. Deze informatievoorziening vindt ongevraagd plaats bijvoorbeeld bij inschrijving of bij in dienst treding. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens, en betrokkenen kunnen zich verzetten tegen het gebruik van hun gegevens. De AVG geeft ook het recht 'om te worden vergeten' en het recht om je data mee te nemen (dataportabiliteit). Uitvoering van de laatste 2 rechten is (nog) niet altijd goed mogelijk.

Data-integriteit: er zijn organisatorische en technische maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn. Dat betekent ook dat persoonsgegevens adequaat moeten worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

2. Protocol Datalekken

2.1 Wat is een Datalek?

Bij een datalek is sprake van een inbreuk op de beveiliging van persoonsgegevens waarbij deze zijn blootgesteld aan verlies of onrechtmatige verwerking ervan. Denk hierbij aan een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop, een inbraak in een databestand door een hacker of het ten onrechte verstrekken van persoonsgegevens aan derden. Nadere uitleg volgt hieronder.

2.2 De vijf rollen

Invitare onderscheidt vijf rollen om een beveiligingsincident/datalek af te handelen:

Rol een:

Ontdekker: degene (medewerker, kind, ouder/verzorger, of externe) die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
Afspraak: Deze persoon meldt zo snel mogelijk bij de leidinggevende en de Functionaris Gegevensbescherming.

Rol twee:

Lokaal verantwoordelijke: de leidinggevende van de melder.
Afspraak: Deze persoon wordt door de Ontdekker altijd direct op de hoogte gesteld in het kader van verantwoordelijkheid voor de veiligheid van de eigen locatie een blijft verantwoordelijk voor de lokale afhandeling en schakelt daarvoor altijd met de FG en evt. het Bevoegd gezag.

Rol drie:

Melder: degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens (AP).
Afspraak: Dat is altijd de FG. De FG brengt eerst een advies uit aan het Bevoegd gezag over het wel of niet melden bij de AP, en de inhoud van de melding en evt. maatregelen. De FG adviseert ook of de betrokkene(n) wel of niet ingelicht dienen te worden.

Rol vier:

Technicus: degene die de oorzaak van het datalek kan onderzoeken en kan (laten) repareren.
*Afspraak***:** Deze verantwoordelijkheid wordt afhankelijk van de locatie van het datalek door de FG belegd op het niveau van de lokale of de centrale ICT-coördinator en zal in de praktijk vaak in afstemming gaan met de technicus van een leverancier. De FG is altijd betrokken.

Rol vijf:

Bevoegd gezag: het bestuur van de stichting is eindverantwoordelijk voor de goede afhandeling van een beveiligingsincident/datalek en wordt daarin met advies bijgestaan door de FG.

3. Meldplicht: zeven vragen

Mocht er een datalek geconstateerd worden of er een vermoeden zijn dat hiervan sprake is, dan helpen de volgende zeven vragen om te bepalen of dit gemeld moet worden bij de AP en betrokkene(n).

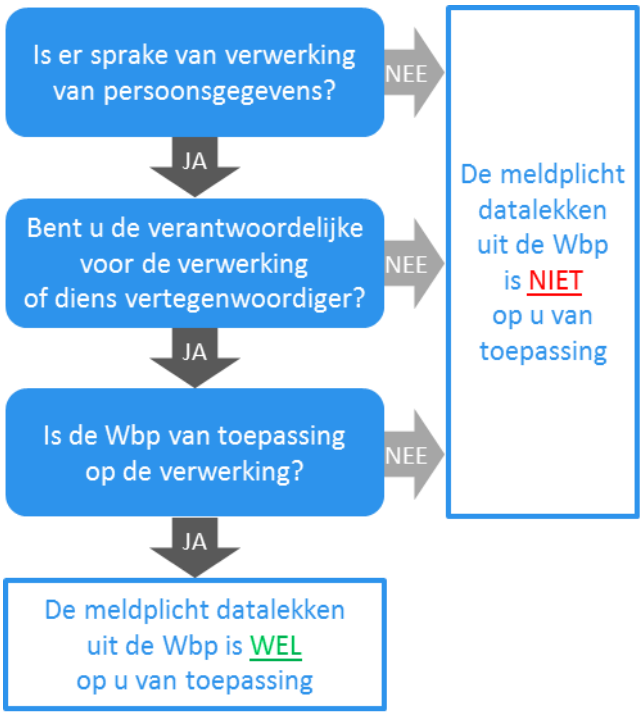
1. Is de meldplicht datalekken uit de AVG van toepassing?
2. Is een gebeurtenis te beschouwen als een datalek?

3. Moet het datalek worden gemeld aan de Autoriteit Persoonsgegevens?
4. Hoe en wanneer moet het datalek worden gemeld aan de Autoriteit Persoonsgegevens?
5. Moet het datalek ook worden gemeld aan de betrokkene(n)?
6. Hoe en wanneer moet het datalek worden gemeld aan de betrokkene(n)?
7. Welke gegevens moeten worden vastgelegd?
8. Deze vragen worden in onderstaand verder toegelicht.

Vraag 1: Is de meldplicht datalekken uit de AVG van toepassing?

Dat is het geval indien:

a) er sprake is van verwerking van persoonsgegevens (elk gegeven betreffende een geïdentificeerde of identificeerbare persoon, zoals NAW-gegevens, IP-adressen en foto's). Verwerking van persoonsgegevens betreft elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, zoals het verzamelen, vastleggen, ordenen, raadplegen en verspreiden.



b) het bevoegd gezag van Invitare de verantwoordelijke is - degene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking vaststelt - of diens vertegenwoordiger is. Als je bij de verwerking derden inschakelt, blijf je ter zake de meldplicht de eindverantwoordelijke.

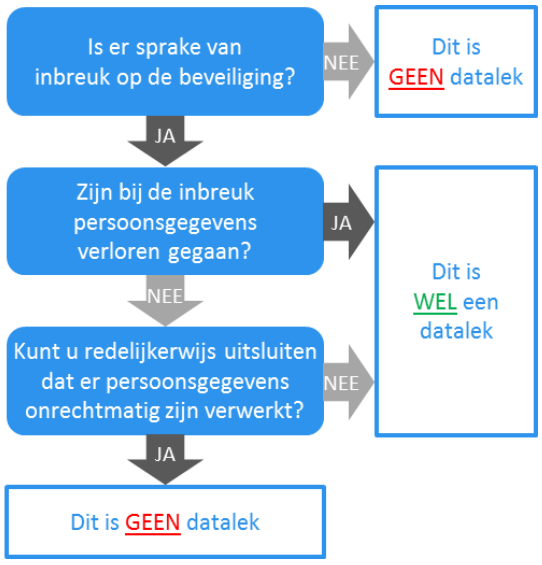
c) de AVG op de verwerking van toepassing is. Bepaalde verwerkingen vallen door hun aard of hun doelstelling buiten de reikwijdte van de AVG, bijvoorbeeld verwerkingen ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden. Op de verwerking van persoonsgegevens voor uitsluitend journalistieke, artistieke of

literaire doeleinden is de AVG gedeeltelijk van toepassing maar de meldplicht datalekken niet. Daarnaast is van belang waar de activiteiten plaatsvinden waarvoor de persoonsgegevens worden verwerkt en waar de al dan niet geautomatiseerde middelen zich bevinden die bij de verwerking worden gebruikt (in een ander land). In beginsel is op de verwerking van persoonsgegevens binnen Invitare altijd de AVG van toepassing, dus ook de meldplicht is van toepassing!

Vraag 2: Is een gebeurtenis te beschouwen als een datalek?

Dat is het geval indien:

a) er sprake is van een inbreuk op de beveiliging, dat wil zeggen dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan, en



b) bij de inbreuk persoonsgegevens verloren zijn gegaan of redelijkerwijs niet kan worden uitgesloten dat er persoonsgegevens onrechtmatig zijn verwerkt, waaronder moet worden begrepen de aantasting van de persoonsgegevens, onbevoegde kennisneming, wijziging of verstrekking daarvan.

c) Wie onderzoekt of er sprake is van een datalek en zo ja, wat de aard en de ernst daarvan is, dient onderzocht te worden. De FG is de aangewezen persoon om dit onderzoek te starten. De FG zal bepalen of een technisch onderzoek intern of extern (of beiden) belegd dient te worden. Dit laatste is al snel aan de orde aangezien het technisch beheer van applicaties zoveel mogelijk is uitbesteed. De FG zorgt aan de hand van het onderzoek ook voor de registratie van het incident, bijv. in een incidentregister.

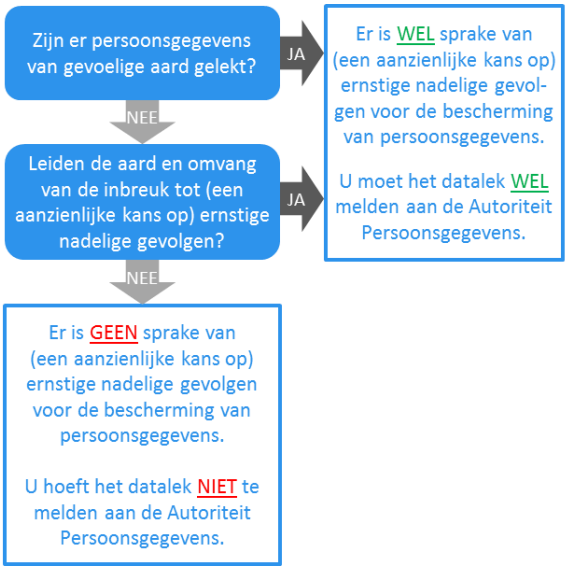
Vraag 3. Moet een melding gedaan worden naar de Autoriteit

Persoonsgegevens?

Een datalek moet worden gemeld aan de Autoriteit Persoonsgegevens indien sprake is van (een aanzienlijke kans op) (ernstige) nadelige gevolgen voor de bescherming van persoonsgegevens.

a) Dat is het geval indien één van de volgende situaties aan de orde is: Persoonsgegevens van gevoelige aard zijn gelekt, namelijk:
   - bijzondere persoonsgegevens zoals bedoeld in artikel 9 AVG:
     - betreffende iemands levensovertuiging of godsdienst, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging
     - strafrechtelijke persoonsgegevens en
   - persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag, of persoonsgegevens die anderszins van gevoelige aard zijn, waaronder:
     - gegevens over de financiële of economische situatie van de betrokkene;
     - gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene;
     - gebruikersnamen, wachtwoorden en andere inloggegevens;
     - gegevens die kunnen worden misbruikt voor (identiteits-)fraude;
     - gegevens uit DNA-databanken, gegevens waar een bijzondere, wettelijk bepaalde geheimhoudingsplicht op rust en gegevens die onder een beroepsgeheim vallen.

b) De aard en omvang van de inbreuk leiden tot (een aanzienlijke kans op) ernstige nadelige gevolgen. Hierbij is van belang:
   - gaat het om veel persoonsgegevens per persoon of om gegevens van grote groepen?
   - zijn de beslissingen die op basis van de verwerkte persoonsgegevens worden genomen ingrijpend?
   - worden de persoonsgegevens binnen ketens (zoals binnen de overheid) gedeeld?
     - gaat het om persoonsgegevens van kwetsbare groepen (van toepassing bij kinderen)?



Vraag 4: Hoe en wanneer moet het datalek worden gemeld aan de Autoriteit Persoonsgegevens?
De Autoriteit Persoonsgegevens stelt voor de melding een webformulier beschikbaar. Het datalek moet onverwijld worden gemeld. Dit houdt in dat de verantwoordelijke, na het

ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek teneinde een onnodige melding te voorkomen. De termijn voor het melden begint te lopen op het moment dat de verantwoordelijke of een verwerker op de hoogte raakt van een incident dat mogelijk onder de meldplicht datalekken valt.

Zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, moet een melding worden gedaan bij de Autoriteit Persoonsgegevens, tenzij op dat moment inmiddels uit onderzoek is gebleken dat het incident niet onder de meldplicht datalekken valt.

Bij Invitare dient de Functionaris Gegevensbescherming direct en minimaal binnen 12 uur ingelicht te worden. Op deze manier kan worden gevraagd om advies en om de melding en eventuele opvolging – in de vorm van maatregelen en communicatie betrokkene(n) – te verzorgen.

Er kan een vermoeden zijn van strafbaar handelen. Zo is bijvoorbeeld hacken strafbaar gesteld. Wanneer dat vermoeden er is, dan is er alle aanleiding om daarvan aangifte te doen bij de politie. Dit dient beoordeeld te worden door de Functionaris Gegevensbescherming. Verder handelen gaat altijd in afstemming met het bevoegd gezag, de locatieleider en eventueel met een communicatieadviseur. Het kan ook zijn dat een voorval de pers bereikt of het wordt verspreid via sociale media.

Vraag 5: Moet het datalek ook worden gemeld aan de betrokkene(n)?
Uitgangspunt is dat indien er persoonsgegevens zijn gelekt, dit wordt gemeld aan degene wiens persoonsgegevens het betreft, de betrokkene. Het datalek hoeft niet te worden gemeld aan de betrokkene(n) indien één van de volgende situaties zich voordoet:

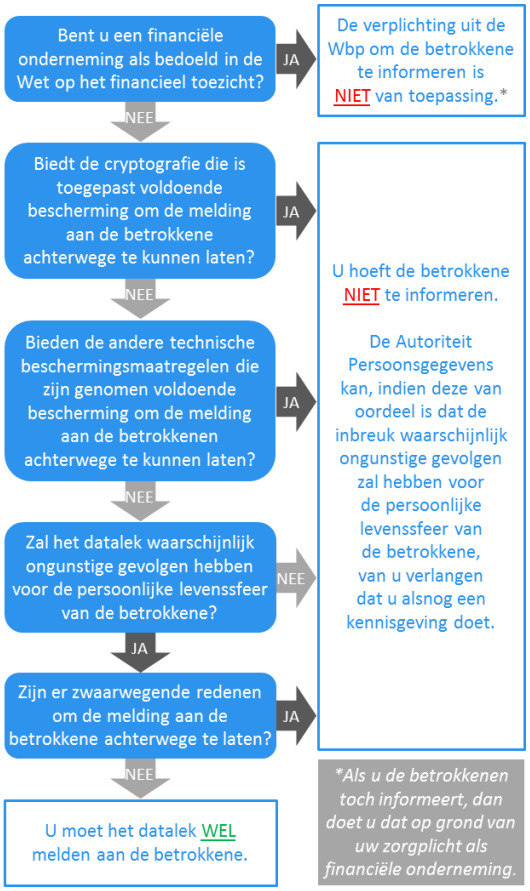
a) u bent een financiële onderneming zoals bedoeld in de Wet op het financieel toezicht;

b) er zijn passende technische beschermingsmaatregelen genomen waardoor de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor eenieder die geen recht heeft op kennisname van de gegevens, bijvoorbeeld door adequate encryptie (versleuteling) en hashing (het omzetten van gegevens in een unieke code);

c) andere technische beschermingsmaatregelen bieden voldoende bescherming om de melding aan de betrokkene achterwege te kunnen laten, bijvoorbeeld door een tijdige en adequate remote wiping (het op afstand wissen van de gegevens die op een apparaat staan) en pseudonimisering (technische maatregelen om te voorkomen dat de persoonsgegevens worden gekoppeld aan de oorspronkelijke identiteit van de betrokkene);

d) het is onwaarschijnlijk dat het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkene: als persoonsgegevens van gevoelige aard zijn gelekt, moet sowieso worden gemeld;

e) er zijn andere zwaarwegende redenen om de melding aan de betrokkene achterwege te laten.



Vraag 6: Hoe en wanneer moet het datalek worden gemeld aan de betrokkene(n)?

In de kennisgeving aan de betrokkene moet in ieder geval worden vermeld:

- de aard van de inbreuk;
- de instanties waar de betrokkene meer informatie over de inbreuk kan krijgen (contactgegevens, waaronder die van de Functionaris Gegevensbescherming);
- de maatregelen die zijn aanbevolen om de negatieve gevolgen van de inbreuk te beperken.

Het datalek moet onverwijld worden gemeld. Dit houdt in dat de verantwoordelijke, na het ontdekken van een mogelijk datalek, enige tijd mag nemen voor nader onderzoek zodat betrokkene op een behoorlijke en zorgvuldige manier kan worden geïnformeerd.

De manier waarop de betrokkene wordt geïnformeerd wordt altijd eerst afgestemd met het bevoegd gezag, de locatieleider en eventueel een communicatieadviseur. Het kan namelijk ook zijn dat een voorval de pers bereikt of dat het wordt verspreid via sociale media.

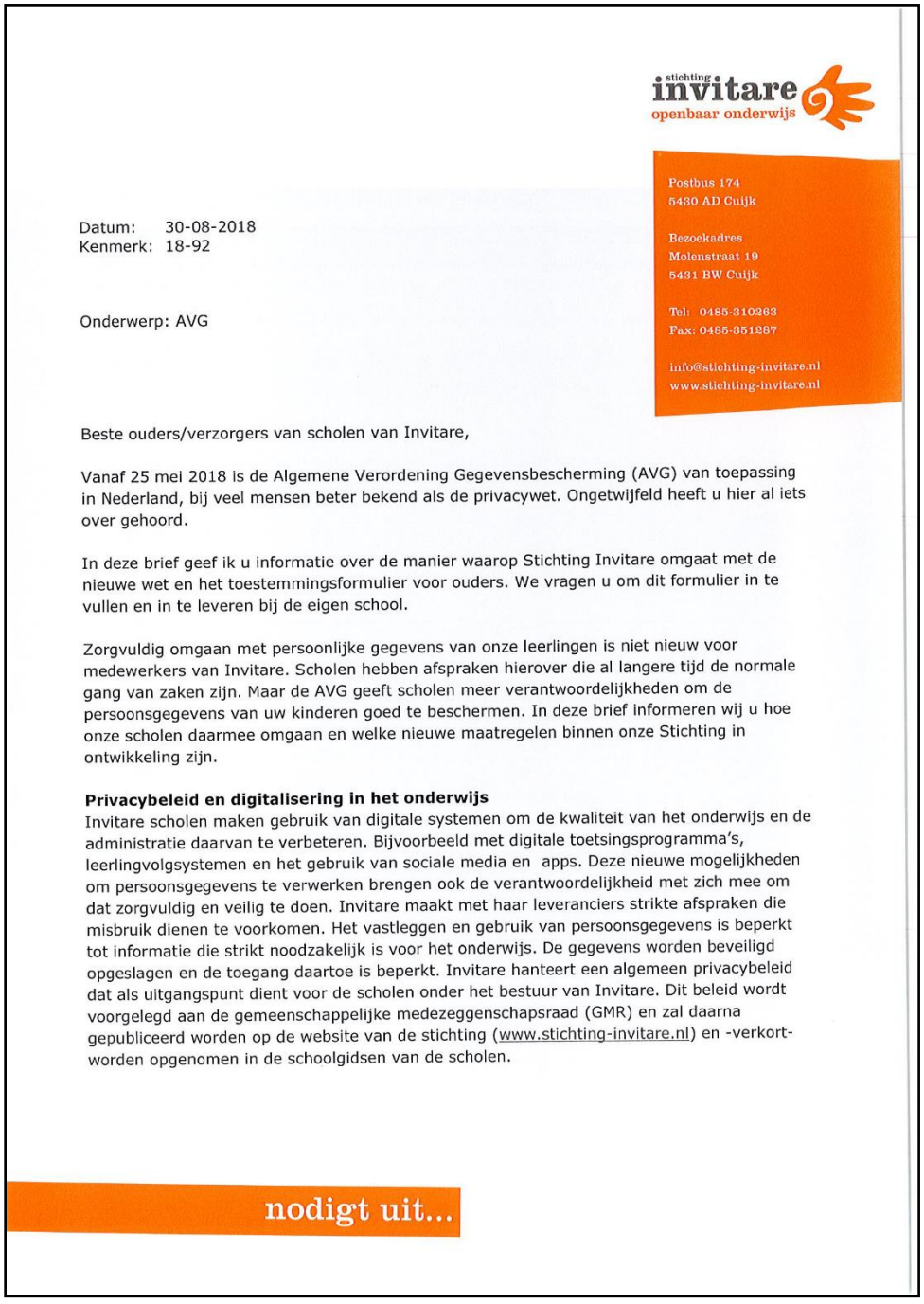
Vraag 7: Welke gegevens moeten worden vastgelegd?
Er moet intern een overzicht worden bijgehouden van alle beveiligingsincidenten en datalekken, dus ook van datalekken die aan de AP moeten worden gemeld. Per incident bevat het overzicht in ieder geval de gegevens omtrent de aard van de inbreuk en, indien aan de betrokkene is gemeld, de tekst van de kennisgeving. De wet schrijft niet voor hoe lang het overzicht moet worden bewaard. We gaan uit van een bewaartermijn van minimaal twee jaar. In bepaalde gevallen kan het nodig zijn een langere bewaartermijn te hanteren. De Functionaris Gegevensbescherming houdt dit overzicht bij, zo mogelijk in een (integraal) systeem voor de registratie van veiligheidsincidenten.

Bijlage 6: Toestemmingsbrief ouders / verzorgers

Toegevoegd zijn:

- Een brief van het bestuur met betrekking tot de AVG (deze wordt jaarlijs verzonden met de volgende twee bijlagen);
- Een voorbeeldbrief voor de school (deze moet per school aangepast worden);
- Een voorbeeld toestemmingsformulier (ook deze moet per school worden aangepast aan de eigen situatie).

N.B. De scholen kunnen ouders ook vragen om zelf via Parro de wijzigingen in hun toestemming bij te houden.



stichting invitare
openbaar onderwijs

Postbus 174
5430 AD Cuijk

Bezoekadres
Molenstraat 19
5431 BW Cuijk

Tel: 0485-310263
Fax: 0485-351287

info@stichting-invitare.nl
www.stichting-invitare.nl

Datum: 30-08-2018
Kenmerk: 18-92

Onderwerp: AVG

Beste ouders/verzorgers van scholen van Invitare,

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing in Nederland, bij veel mensen beter bekend als de privacywet. Ongetwijfeld heeft u hier al iets over gehoord.

In deze brief geef ik u informatie over de manier waarop Stichting Invitare omgaat met de nieuwe wet en het toestemmingsformulier voor ouders. We vragen u om dit formulier in te vullen en in te leveren bij de eigen school.

Zorgvuldig omgaan met persoonlijke gegevens van onze leerlingen is niet nieuw voor medewerkers van Invitare. Scholen hebben afspraken hierover die al langere tijd de normale gang van zaken zijn. Maar de AVG geeft scholen meer verantwoordelijkheden om de persoonsgegevens van uw kinderen goed te beschermen. In deze brief informeren wij u hoe onze scholen daarmee omgaan en welke nieuwe maatregelen binnen onze Stichting in ontwikkeling zijn.

Privacybeleid en digitalisering in het onderwijs
Invitare scholen maken gebruik van digitale systemen om de kwaliteit van het onderwijs en de administratie daarvan te verbeteren. Bijvoorbeeld met digitale toetsingsprogramma's, leerlingvolgsystemen en het gebruik van sociale media en apps. Deze nieuwe mogelijkheden om persoonsgegevens te verwerken brengen ook de verantwoordelijkheid met zich mee om dat zorgvuldig en veilig te doen. Invitare maakt met haar leveranciers strikte afspraken die misbruik dienen te voorkomen. Het vastleggen en gebruik van persoonsgegevens is beperkt tot informatie die strikt noodzakelijk is voor het onderwijs. De gegevens worden beveiligd opgeslagen en de toegang daartoe is beperkt. Invitare hanteert een algemeen privacybeleid dat als uitgangspunt dient voor de scholen onder het bestuur van Invitare. Dit beleid wordt voorgelegd aan de gemeenschappelijke medezeggenschapsraad (GMR) en zal daarna gepubliceerd worden op de website van de stichting (www.stichting-invitare.nl) en -verkort- worden opgenomen in de schoolgidsen van de scholen.

nodigt uit...

Verantwoordingsplicht
Onder de AVG hebben scholen een verantwoordingsplicht. De verantwoordingsplicht houdt onder meer in dat scholen moet kunnen aantonen welke technische en organisatorische maatregelen zijn genomen om de persoonsgegevens van de leerlingen te beschermen. En of de regels die de AVG voorschrijft worden nageleefd bijvoorbeeld met betrekking tot de leerlingendossiers. Invitare zal dit onder andere doen door het opstellen van een register van verwerkingsgegevens.

Wat gaat u als ouder merken?
Jaarlijks vraagt de school u om toestemming te geven voor het gebruik van beeldmateriaal en voor het gebruik van de persoonsgegevens (NAW-gegevens) via een toestemmingsformulier. Verder zal de school bewust omgaan met het delen van bijvoorbeeld klassenlijsten en terughoudend zijn in het mailen van privacygevoelige gegevens. We rekenen op uw begrip daarvoor.

Zoals gezegd is het zorgvuldig omgaan met persoonsgegevens niet nieuw binnen Invitare. We vinden privacy belangrijk en zullen bewustwording rondom dit onderwerp bij onze medewerkers actief stimuleren. Mocht u vragen hebben over de AVG dan kunt u in eerste instantie terecht bij de directie van uw school.

Met vriendelijke groeten,

Mw. drs. F.M. van Veen
Voorzitter College van Bestuur

Bijlage: brief van uw school en het toestemmingsformulier

Voorbeeldbrief voor de scholen

Toestemming gebruik beeldmateriaal (foto's en film),
gebruik mailadressen op school en vermelding
gegevens op groepslijsten.

……., ….. 20xx

Beste ouder(s)/verzorger(s),

Zoals u weet is vanaf 25 mei 2018 de Algemene Verordening ingegaan. Vanzelfsprekend heeft onze Stichting Invitare maatregelen genomen en is het Privacybeleid aangepast aan de huidige AVG (Algemene Verordening Gegevensbescherming).

Eén van de maatregelen is het vragen van toestemming aan ouders voor het gebruik van beeldmateriaal (foto's en filmopnames) en het gebruik van persoonsgegevens (NAW-gegevens) op de groepslijst van uw kind. We zijn vanuit de wetgeving verplicht om jaarlijks uw toestemming te vragen.

Toestemming
Wij gaan zorgvuldig om met de foto's en opnames die we maken. Wij plaatsen geen beeldmateriaal waardoor leerlingen schade kunnen ondervinden. We plaatsen bij foto's en video's geen namen van leerlingen. Het is goed om het geven van toestemming samen met uw zoon/dochter te bespreken. Als u uw keuze thuis bespreekt, dan weten ze zelf waarom het gebruik van foto's en video's wel of niet mag.

Er is geen toestemming van ouders nodig voor het gebruik van beeldmateriaal in de groep en les voor onderwijskundige doeleinden. Ook is er geen toestemming nodig voor het plaatsen van een foto op een schoolpas of voor gebruik van een foto in het administratiesysteem. Wel gelden voor het gebruik van dat beeldmateriaal de gewone privacyregels (zoals dataminimalisatie: terughoudend omgaan met beeldmateriaal van leerlingen).

In het toestemmingsformulier is aparte toestemming opgenomen voor verschillende categorieën. De wetgever eist dat een ouder een goed geïnformeerde beslissing kan nemen, die ook **specifiek** is. Wanneer wij bijvoorbeeld beeldmateriaal voor een ander doel wil gebruiken, dan op het antwoordformulier vermeld staat, nemen we contact met u op.

Foto's maken op school bij verschillende activiteiten en deze foto's op een beveiligd deel van de website plaatsen.
Als er beeldmateriaal op het beveiligde deel van de website door ouders gekopieerd wordt en vervolgens gedeeld via sociale media is dat niet meer de verantwoordelijkheid van de school. Het maken van foto's van andere kinderen tijdens verjaardagen in de groep, tijdens weeksluitingen of andere activiteiten die onder schooltijd plaatsvinden is niet toegestaan.

Leerling dossier
Ons leerling administratiesysteem Parnassys voldoet aan de wettelijk gestelde eisen in het kader van AVG. Bij overdracht van leerling dossiers naar andere basisscholen, scholen voor Voortgezet Onderwijs of andere instanties vragen wij altijd apart uw toestemming. Deze dossiers worden via beveiligde systemen overgedragen.

Toestemming geven door ouders
Wanneer beide ouders het wettelijk gezag hebben over hun kind(eren), moeten beide ouders het toestemmingsformulier ondertekenen.

Dank voor uw medewerking!

Voorbeeld voor de scholen

Toestemmingsformulier (mei 2018 tot en met 31 juli 2019) voor beeldmateriaal, gebruik mailadressen op school en vermelding gegevens op de groepslijsten

Hierbij verklaren ondergetekenden, ouder(s)/verzorger(s) van ……groep …….. het volgende. Graag aankruisen wat van toepassing is:

Beeldmateriaal mag door [OBS DEeKameleon) gebruikt worden:	Beeldmateriaal wordt gebruikt voor de volgende doelen
□ in de schoolgids en/of schoolbrochure	Informeren van (toekomstige) ouders en (toekomstige) leerlingen over de school en de onderwijs mogelijkheden.Hiernaast wordt het beeldmateriaal gebruikt voor PR-doeleinden van de school.
□ op de openbare website van de school	Informeren van (toekomstige) ouders en (toekomstige) leerlingen over de school, het gegeven en te volgen onderwijs en diverse onderwijsactiviteiten zoals schoolreisjes, schoolfeesten, etc.
□ op het besloten deel van de website van de school	Informeren van ouders en leerlingen over de onderwijsactiviteiten zoals schoolreisjes, excursies, schoolfeesten, etc.
□ oudercommunicatie Apps (zoals Parro)	Informeren van ouders en leerlingen over de onderwijsactiviteiten binnen de eigen leergroep. Parro is een beveiligde omgeving en gekoppeld aan Parnassys.
□ in besloten onderwijssystemen zoals Google Suite (Classroom)	Voor het maken en presenteren van onderwijsopdrachten door leerlingen.
□ groepsfoto	schoolfotograaf
Overige categorieën	
□ gebruik van mailadressen	Uw kind maakt gebruik van een chromebook als leer- en verwerkingsmateriaal. Om hierin te kunnen werken, heeft uw kind een mailadres. Emailadressen worden beheerd door de school en de mailomgeving voldoet aan de gestelde veiligheidseisen.
□ NAW gegevens op groepslijsten	Iedere leerling krijgt aan het begin van het schooljaar van zijn/haar groep een groepslijst mee naar huis, met naam, adresgegevens en telefoonnummer.
□ NAW gegevens uitwisselen aan Oudervereniging	Voor het informeren van ouders over de jaarlijkse ouderbijdrage aan de ouders, heeft de Oudervereniging naam en adresgegevens van de leerlingen nodig.

Datum: ..... Datum: .....

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

Handtekening ..... Handtekening .....

Bijlage 7: Protocol voor het gebruik van e-mail, ICT en sociale media

Onderwijskundig uitgangspunt
Internet is een informatiemedium en leerlingen moeten daar mee leren omgaan. De strategie is begeleidend confronteren. Internet is een afspiegeling van de maatschappij. Kinderen moeten leren wat goed is en wat niet kan. Begeleidend confronteren is leren omgaan met Internet zoals het zich dagelijks aan ons voordoet. Begeleiden doen we stapje voor stapje en we bespreken de ins en outs ervan. We benaderen Internet zoals we ook kinderen leren omgaan met verkeer of de televisie.

Internet op school
De kinderen van onze school kunnen gebruik maken van Internet. Deze internetverbinding wordt 24/7 gemonitord door de Firewall die ingesteld en beheerd wordt door ICT -partner DWE.
De leerlingen werken op Chromebooks. Deze worden beheerd door Bovenschoolse ICT-er en IPOS. Zij beheren ook de Gsuite workspace omgeving en alle instellingen die daarbij horen.

Artikel 1 Werkingssfeer van deze regeling, begrippen

1.1 Deze regeling geeft de wijze aan waarop binnen Stichting Invitare Openbaar Onderwijs wordt omgegaan met informatie- en communicatietechnologie (hierna: ICT). Deze regeling omvat (gedrags)regels ten aanzien het gebruik van de ICT en geeft regels voor welke doeleinden en op welke wijze controle plaats vindt op dit gebruik.

1.2 Deze regeling geldt voor eenieder die ten behoeve van de school werkzaamheden verricht (personeelsleden, maar bijvoorbeeld ook: stagiaires en vrijwilligers) of onderwijs volgt (leerlingen). Gezamenlijk worden zij in dit reglement ook aangeduid als 'gebruiker(s)'.

1.3 Elke nieuwe gebruiker wordt gewezen op de toepasselijkheid van deze regeling. Daarbij wordt aangegeven waar de volledige tekst van deze regeling geraadpleegd/ingezien kan worden. Alle personeelsleden en leerlingen ontvangen eens per jaar een herinnering aan de geldende regels.

1.4 Voor zover de gebruikers thuis of elders gebruik maken van de ICT (bijvoorbeeld het e-mailadres van de school of de schoolwebsite) zijn de bepalingen van deze regeling eveneens van toepassing.

Artikel 2 Toegang tot en gebruik van de ICT

2.1 Stichting Invitare geeft de gebruiker het recht op toegang tot de ICT (en de daarmee verbonden systemen en faciliteiten), maar behoudt zich het recht voor de toegang weer in te trekken.

2.2 Gebruikersidentificatie (gebruikersnaam) en authenticatie (wachtwoord) worden door de directeur dan wel ICT-er verstrekt en zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven.

2.3 Het is gebruiker niet toegestaan om persoonsgegevens die gebruiker ter beschikking staan voor de uitoefening van zijn functie lokaal op te slaan (dus niet op het computernetwerk) noch op privé-apparatuur, noch op de cloud van eigen providers tenzij daarvoor voorafgaande toestemming is verleend door diens leidinggevende en adequate waarborgen zijn getroffen voor de beveiliging van de persoonsgegevens.

Artikel 3 Gebruik van de ICT-apparatuur

3.1 De gebruiker dient zorgvuldig om te gaan met de ICT-apparatuur, zodat deze niet beschadigd raakt. De apparatuur dient in goede orde te worden achtergelaten. Eventuele schade of ontbreken van onderdelen dient direct gemeld te worden aan de ICT-er.

3.2 Tijdens het gebruik van de ICT-apparatuur is het niet toegestaan etens- en drinkwaren te nuttigen.

3.3 Alleen de ICT-er (of een medewerker die door de ICT-er is geïnstrueerd) is bevoegd om apparatuur te ontkoppelen, verplaatsen of aan te sluiten aan het schoolnetwerk of aan apparatuur die aan het schoolnetwerk verbonden is.

3.4 De ICT-er verleent alleen ondersteuning op apparatuur die door de ICT-er is aangesloten en geïnstalleerd.

3.5 Het gebruik van eigen opslagmedia (bijvoorbeeld: een USB-stick) van de gebruikers is toegestaan, mits onder de volgende voorwaarden:

a) voor het correct laten functioneren van het opslagmedium kan geen beroep worden gedaan op de ICT-er;
b) de bestanden en programmatuur die op het opslagmedium staan moeten voldoen aan de voorwaarden zoals vastgelegd in dit reglement.

3.6 Het gebruik van eigen computerapparatuur (bijvoorbeeld laptops of tablets) is toegestaan onder de volgende voorwaarden:

a) Voorafgaand aan het gebruik is toestemming verleend door de leidinggevende en is contact opgenomen met de ICT-er. Deze is bevoegd om, met opgaaf van redenen, de apparatuur niet toe te staan;
b) de gebruiker geeft de ICT-er de gelegenheid om voorafgaand aan het gebruik maatregelen te treffen om de beheersbaarheid en de veiligheid te waarborgen;
c) het gebruik van de betreffende apparatuur moet voldoen aan de voorwaarden zoals vastgelegd in dit reglement.

Artikel 4 Toegang tot en gebruik van internet en e-mail

4.1 Stichting Invitare behoudt zich het recht voor om de toegang tot bepaalde sites door middel van een filtersysteem te beperken.

4.2 Het versturen van e-mailberichten moet voldoen aan de volgende algemene voorwaarden:

a) de afzender wordt correct weergegeven;
b) duidelijke onderwerp aanduiding;
c) terughoudend omgaan met vertrouwelijke gegevens en gevoelige informatie.

4.3 Voor het verzenden en ontvangen van e-mail binnen de school wordt alleen gebruik gemaakt van de e-mailprogrammatuur die de school hiervoor beschikbaar stelt. Het gebruik van andere mailprogrammatuur is niet toegestaan. Het is tevens niet toegestaan om de privé mailboxen te koppelen aan de zakelijke mailbox en v.v.

4.4 Omdat het verzenden van gegevens met gebruikmaking van Gmail, Hotmail, Dropbox, Whatsapp en WeTransfer leidt, dan wel kan leiden, tot doorgifte van Persoonsgegevens buiten de EER, hetgeen slechts is toegestaan onder voorwaarden, kan Stichting Invitare – indien door haar niet langer aan deze voorwaarden kan worden voldaan - besluiten het gebruik van deze software door medewerkers te verbieden.

Artikel 5 (On)verantwoord gebruik van de ICT

Verantwoord gebruik

5.1 Het gebruik van de ICT is primair verbonden met taken en bezigheden die voortvloeien uit het verstrekken of ontvangen van onderwijs en begeleiding. Als uitgangspunt geldt dat het gebruik van de ICT van de school ten dienste moet staan aan de werkzaamheden van het personeelslid of de opleiding van de leerling. Indien en voor zover sprake is van het verwerken van persoonsgegevens gebeurt dit met inachtneming van het Privacyreglement.

5.2 Personeelsleden mogen de ICT beperkt, incidenteel en kortstondig gebruiken voor persoonlijke doeleinden, mits dit niet storend is voor de dagelijkse werkzaamheden of het systeem en mits hierbij wordt voldaan aan de verdere regels van deze regeling. Leerlingen mogen de ICT onder schooltijd in principe niet voor persoonlijke doeleinden gebruiken, tenzij zij daarvoor toestemming hebben gekregen.

5.3 Gebruikers van de ICT-systemen melden gesignaleerde zwakke plekken in de systemen, zodat zo snel mogelijk maatregelen kunnen worden getroffen. Melding kan worden gedaan bij de Functionaris Gegevensbescherming.

Onverantwoord gebruik

5.4 Het is niet toegestaan om de ICT zodanig te gebruiken dat het systeem- en/of de beveiliging opzettelijk worden aangetast.

5.5 Het is niet toegestaan zich toegang te verschaffen tot gegevens van andere gebruikers, tenzij met uitdrukkelijke toestemming van de betreffende gebruiker.

5.6 Het is niet toegestaan pogingen te ondernemen om het filtersysteem te omzeilen.

5.7 Het is in het bijzonder niet toegestaan om:

a) sites te bezoeken die pornografisch, racistisch, discriminerend, (seksueel) intimiderend, beledigend of aanstootgevend materiaal bevatten;
b) pornografisch, racistisch, discriminerend, (seksueel intimiderend, beledigend of aanstootgevend materiaal te bekijken of te downloaden of te verspreiden;
c) zich tot niet-openbare bronnen op het netwerk, internet of andere computernetwerken toegang te verschaffen en het bewust informatie waartoe men via de ICT oneigenlijk toegang heeft verkregen zonder toestemming te veranderen of te vernietigen;
d) bestanden te downloaden en/of op het computernetwerk of lokaal op een PC van de school te plaatsen die geen verband houden met studie en/of werk;
e) software en applicaties te downloaden en/of te installeren zonder voorafgaande toestemming van de ICT-er;
f) niet-educatieve spelletjes te spelen;
g) anoniem of onder een fictieve naam via de ICT te communiceren;
h) op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende manier via de ICT te communiceren;
i) inkomende privé-berichten te genereren door het deelnemen aan niet-zakelijke nieuwsgroepen, abonnementen op e-zines, elektronisch winkelen, down- en uploaden van bestanden, nieuwsbrieven en dergelijke;
j) kettingmailberichten en andere berichten die verstopping veroorzaken of het werk van anderen verstoren te verzenden of door te sturen;
k) iemand lastig te vallen via de ICT;
l) het introduceren en verspreiden van computervirussen en andere software die de integriteit van de gegevens of de computerbeveiliging van de ICT kunnen beschadigen;

m) gebruik te maken van MSN Messenger en andere chatvoorzieningen.

5.8 Het is niet toegestaan om foto's, video's of ander materiaal van op school werkzame personen of leerlingen of andere bij de school betrokkenen via de ICT (daaronder ook begrepen: social media) te publiceren, tenzij dit gericht is op een aan het onderwijs gerelateerde doelstelling en de afgebeelde personen hebben aangegeven in te stemmen met dergelijke publicaties.

5.9 Het is ook anderszins niet toegestaan om door middel van de ICT in strijd met de wet of onethisch te handelen.

5.10 De schoolleiding kan de ICT-er opdracht geven geconstateerde ongeoorloofde data van het computernetwerk te verwijderen.

5.11 Voor personeelsleden is het voor testdoeleinden toegestaan software lokaal te installeren die nodig is voor de werkzaamheden ten behoeve van school.

5.12 Een vermoeden van misbruik van ICT en inbreuken op de beveiliging, van binnenuit of van buiten de school dienen onmiddellijk aan de ICT-er gemeld te worden, hieronder vallen tevens inbreuken op de beveiliging die bij toeval worden ontdekt.

5.13 Als de gebruiker eraan twijfelt of een bepaald gebruik van ICT wel verantwoord is, dan overlegt hij daarover met de ICT-er.

Artikel 6 Algemene uitgangspunten van controle op gebruik

6.1 De schoolleiding heeft er recht op en belang bij dat zij het gebruik van de ICT door personeelsleden en leerlingen kan controleren. De controle op gebruik van de ICT zal overeenkomstig deze regeling uitgevoerd worden. Als zich situaties voordoen waarin deze regeling niet voorziet, dan zal conform de Algemene Verordening Gegevensbescherming (AVG) gehandeld worden.

6.2 Als een directielid merkt of erop geattendeerd wordt dat het ICT-gedrag van een personeelslid niet binnen de kaders van dit reglement verloopt, wordt het personeelslid hierop door het directielid gewezen en wordt een controle van zijn ICT-gebruik door bevoegde personen van de ICT-er als mogelijkheid genoemd. Het directielid meldt dit aan de locatiedirecteur of de centrale directie.

6.3 Als een personeelslid merkt dat het ICT-gedrag van een leerling niet binnen de kaders van dit reglement verloopt, dan spreekt het personeelslid deze leerling hierop aan en meldt dit aan het locatiedirectielid waaronder deze leerling resorteert.

6.4 Gestreefd wordt naar een goede balans tussen enerzijds controle op het gebruik van de ICT en anderzijds de bescherming van de privacy van personeelsleden en leerlingen.

6.5 Controle op het gebruik van de ICT zal waar mogelijk zoveel mogelijk geautomatiseerd plaatsvinden, waarbij in geval van verdachte berichten, het bericht geautomatiseerd wordt teruggezonden aan de verzender. Voor zover geautomatiseerde controle niet mogelijk, dan wel ontoereikend is, zal de controle op het gebruik van de ICT in beginsel steekproefsgewijs plaatsvinden.

6.6 In geval dat ten aanzien van een gebruiker, vanwege een concreet vermoeden van oneigenlijk gebruik, een gerichte controle is uitgevoerd, stelt de schoolleiding deze gebruiker daarvan zo spoedig mogelijk nadat de controle heeft plaatsgevonden van op de hoogte.

6.7 Persoonsgegevens met betrekking tot het gebruik van ICT worden niet langer bewaard dan noodzakelijk, met een bewaartermijn van [maximaal 6 maanden]. Onder omstandigheden kan een langere bewaartermijn gerechtvaardigd zijn. In dat geval zal de verwerking worden gemeld bij de Autoriteit Persoonsgegevens.

6.8 Privémail/-gebruik (voorzien van het label ‘persoonlijk’) wordt zoveel mogelijk ontzien van controle.

6.9 Elektronische informatie- en communicatieberichten van vertrouwenspersonen en andere personeelsleden met een vertrouwensfunctie, gecommuniceerd in het kader van hun functie, zijn uitgesloten van inhoudelijke controle.

6.10 De schoolleiding treft voorzieningen voor de positie en de integriteit van de ICT-er. De medewerkers van de ICT-er hebben een geheimhoudingsplicht die inhoudt dat ten aanzien van de verzamelde en voor hen inzichtelijke informatie strikte geheimhouding betracht dient te worden.

Artikel 7 Doeleinden van controle

7.1 De controle op persoonsgegevens bij gebruik van de ICT vindt slechts plaats met als doel:
   a) het tegengaan van onverantwoord en ontoelaatbaar gebruik;
   b) de naleving van het Privacyreglement;
   c) het bewaken van de voortgang van werkzaamheden;
   d) het vastleggen van bewijs en/of archief;
   e) de systeem- en netwerkbeveiliging;
   f) de kosten- en capaciteitsbeheersing.

7.2 Onder 'onverantwoord en ontoelaatbaar gebruik' als bedoeld in artikel 7.1 wordt begrepen: het onverantwoord gebruik als opgenomen in artikel 5.4 tot en met 5.13.

7.3 Onder 'bewaking van de voortgang van de werkzaamheden' als bedoeld in artikel 7.1 wordt begrepen: controle op de inhoud van zakelijke e-mails van personeelsleden voor wie het communiceren per e-mail rechtstreeks met de te verrichten taken verband houdt. Middels deze controle kan de voortgang van de werkzaamheden worden gegarandeerd bij ziekte of afwezigheid van de medewerker.

7.4 Onder 'vastleggen van bewijs en/of archief' als bedoeld in artikel 7.1 wordt begrepen: het maken van kopieën van e-mails vanuit de behoefte aan bewijs voor zakelijke transacties en dossiervorming (al dan niet met het oog op het voeren van juridische procedures).

7.5 Onder 'systeem- en netwerkbeveiliging' als bedoeld in artikel 7.1 wordt begrepen: controle op het e-mail- en internetgebruik ter voorkoming van systeemaanvallen door onder andere virussen, trojans of andere schadelijke programma's.

7.6 Onder 'kosten- en capaciteitsbeheersing' als bedoeld in artikel 7.1 wordt begrepen: controle op het e-mail- en internetgebruik ter inventarisering en/of beheersing van de kosten die gemoeid zijn met het gebruik van de ICT.

Artikel 8 Specifieke uitgangspunten van controle op gebruik

8.1 In het kader van de controle op de gebruikers voor het doel als bedoeld in artikel 7.1a geldt dat:
   a) controle op de naleving van de regels vindt in beginsel geautomatiseerd en steekproefsgewijs plaats;
   b) indien er een concreet vermoeden is dat een gebruiker de regels, waarvan de naleving wordt gecontroleerd, overtreedt, vindt zo nodig een in tijd en omvang zo beperkt mogelijke gerichte controle op persoonsniveau plaats;
   c) daarbij worden in eerste instantie de berichten en/of het surfgedrag gescreend op (onder andere) verdachte afzender(s), bestemming, website, verdacht onderwerp, verdachte zoekopdracht, verboden woord in de inhoud of verboden extensies van de bijlage(n);
   d) Vervolgens worden de berichten, waarvan aannemelijk is dat het regulier verkeer betreft of waartegen ook overigens geen bedenkingen bestaan, ongeopend doorgezonden (bij originelen) of vernietigd (kopieën);
   e) de overgebleven berichten kunnen worden geopend voor nader inhoudelijk onderzoek.

8.2 In het kader van de controle voor het doel als bedoeld in artikel 7.1 b geldt dat slechts berichten worden verwerkt die rechtstreeks verband houden met uitvoering van de te verrichten taken door het personeelslid.

8.3 In het kader van de controle voor het doel als bedoeld in artikel 7.1 c geldt dat slechts de e-mailverkeersgegevens en inhoud van de berichten wordt verwerkt.
8.4 In het kader van de controle voor het doel als bedoeld in artikel 7.1 d geldt dat slechts zakelijke berichten worden verwerkt voor zover deze kunnen dienen als bewijs van zakelijke transacties en dossiervorming.
8.5 In het kader van de controle voor het doel als bedoeld in artikel 7.1 e geldt dat:
a) de controle geheel geautomatiseerd plaatsvindt;
b) een gevonden besmet bericht/bestand op een aparte locatie bewaard wordt voor nader onderzoek en eventuele herstelwerkzaamheden.
8.6 In het kader van de controle voor het doel als bedoeld in artikel 7.1 e geldt dat slechts de
a) e-mailverkeersgegevens en inhoud (en bijlagen) van berichten met een verdachte inhoud worden gecontroleerd;
b) internetverkeersgegevens en inhoud van berichten met een verdachte inhoud worden gecontroleerd.
8.7 In het kader van de controle voor het doel als bedoeld in artikel 7.1 f geldt dat de controle van het e-mail- en internetverkeer beperkt blijft tot de verkeersgegevens.
8.8 In het kader van de controle voor het doel als bedoeld in artikel 7.1 f geldt dat slechts de
a) e-mailverkeersgegevens over tijd, hoeveelheid, omvang en dergelijke worden verwerkt;
b) internetverkeersgegevens over tijd en dergelijke worden verwerkt.

Artikel 9 Gebruik van social media

9.1 Onder social media wordt verstaan alle huidige en toekomstige online platformen waarbij de gebruikers de inhoud verzorgen.
9.2 Indien social media voor onderwijsdoeleinden worden gebruikt dient dit – met het oog op de bescherming van leerlinggegevens - plaats te vinden conform het Privacyreglement.
9.3 Voor het overig gebruik geldt dat dit in eigen tijd dient plaats te vinden. Dat geldt ook voor het gebruik van social media door middel van smartphones of tablets.
9.4 Voor zover de gebruikers (leerlingen, personeelsleden of derden) aan de school verbonden zijn, geldt in algemene zin dat zich niet op social media zullen uitlaten op een wijze die schadelijk kan zijn voor de school dan wel stichting

Artikel 10 Richtlijnen voor het gebruik van social media

10.1 Voor zover de gebruiker op social media-uitingen doet die in relatie staan tot Stichting Invitare geeft hij steeds duidelijk aan in welke relatie (bijvoorbeeld: personeelslid of leerling) hij staat tot de school.
10.2 De gebruiker plaatst op social media geen content met een onverantwoorde inhoud.
10.3 De gebruiker deelt op social media geen interne- of bedrijfsvertrouwelijke informatie over de school.
10.4 De gebruiker deelt geen persoonsgegevens van personeel of leerlingen waartoe hij uit hoofde van zijn functie toegang heeft.
10.5 De gebruiker laat zich op social media niet negatief of anderszins ongepast uit over de school, over collega's, over personeelsleden en/of over (mede-)leerlingen.

10.6 De gebruiker plaatst op social media niet zonder toestemming foto's of andere afbeeldingen van de school en/of aan de school verbonden personen.
10.7 De gebruiker plaatst op social media geen content namens de Stichting Invitare, tenzij hij daarvoor toestemming heeft gekregen.
10.8 In zijn algemeenheid geldt dat de gebruiker op social media geen content zal plaatsen of zich anderszins zal gedragen op een wijze die de school schade kan toebrengen.

Artikel 11 Richtlijnen voor contact middels ICT

11.1 Onderling privé-contact tussen personeelsleden en leerlingen, binnen dan wel buiten schooltijd, door middel van e-mail en smartphones (bijvoorbeeld via Whatsapp) is in beginsel verboden.
11.2 Een uitzondering kan aan de orde zijn ten aanzien van leerlingen die speciale begeleiding op afstand nodig hebben, bijvoorbeeld in geval van ziekte. Een dergelijk contact mag alleen betrekking hebben op onderwijsgerelateerde zaken (bijvoorbeeld kennisoverdracht, afstemming huiswerk, ondersteuning) en dient vooraf gemeld te zijn bij de schooldirectie. Het personeelslid mag het contact met de leerling uitsluitend onderhouden via het e-mailadres van de school.
11.3 Onderling contact tussen personeelsleden over een leerling is uitsluitend toegestaan in verband met onderwijsgerelateerde zaken en mag uitsluitend verlopen via het e-mailadres van de school.
11.4 Het is personeelsleden niet toegestaan persoonsgegevens van leerlingen op te slaan op servers die niet worden gebruikt of beheerd door de school of lokaal op de eigen PC respectievelijk tablet of smartphone.
11.5 Gewisselde (e-mail)correspondentie wordt maandelijks door de betrokken docenten vernietigd dan wel – indien de informatie relevant is voor de begeleiding van de leerling - verplaatst en opgeslagen in het leerlingvolgsysteem van de Stichting.

Artikel 12 Disciplinaire maatregelen bij leerlingen

12.1 Indien door de schoolleiding wordt vastgesteld dat een leerling onverantwoord gebruik heeft gemaakt van de ICT, kan de schoolleiding – afhankelijk van de aard en de ernst van het onverantwoorde gebruik – overgaan tot:
a) het tijdelijk uitsluiten van inlogmogelijkheden voor de betrokken leerling;
b) het melden van dit gedrag en de consequenties aan de ouder(s)/verzorger(s); en/of
c) het opleggen van een straf/maatregel.

Artikel 13 Disciplinaire maatregelen bij personeelsleden

Indien door de schoolleiding wordt vastgesteld dat een personeelslid onverantwoord gebruik heeft gemaakt van de ICT, kan het schoolbestuur - afhankelijk van de aard en de ernst van het onverantwoorde gebruik – maatregelen treffen, zoals een berisping, schorsing of ontslag.

Bijlage 8: Overzicht websites Stichting Invitare

Website /portal	Beheerder	Cookies
www.stichting-invitare.nl	FIZZ	Alleen functionele cookies
www.hartenaas.nl	Cybox Internet en communicatie	Alleen functionele cookies
www.obsharlekijn.nl	Assuport BV	Alleen functionele cookies
www.ojbs-elkerlyc.nl	FIZZ	Alleen functionele cookies
www.nienekes.nl	Mijn domein	Alleen functionele cookies
www.daltonschooldeklimop.nl	FIZZ	Alleen functionele cookies
www.kameleonmill.nl	FIZZ	Alleen functionele cookies
www.debonckert.nl	FIZZ	Alleen functionele cookies
www.startblokcuijk.nl	FIZZ	Alleen functionele cookies
www.sbodewingerd.nl	FIZZ	Alleen functionele cookies

De facebookpagina's van de scholen zijn bedrijfspagina en als zodanig beveiligd.

Bijlage 9: protocol gebruik van camera- en videobeelden

Artikel 1 Doel van camera- en video-opnames

Het maken van (digitale)opnames heeft ten doel:

- het zorgdragen voor beveiliging om ongewenst gedrag (waaronder, maar niet uitsluitend: diefstal, vandalisme en pestgedrag) te voorkomen en in voorkomende gevallen te kunnen signaleren en vastleggen.
- het begeleiden en coachen van medewerkers, in het bijzonder maar niet uitsluitend onderwijzend personeel in lessituaties.

Artikel 2 Begripsbepaling

2.1 camera's: het betreft camera's die bedoeld zijn voor algemeen toezicht;
2.2 camerasysteem: het geheel van camera's, monitoren, opnameapparatuur, verbindingskasten, glasvezelverbindingen en bevestigingen;
2.3 video-opnames: camera-opnames met als doel begeleiding en coaching van personeel;
2.4 beheer: zorg voor de continuïteit van het cameratoezicht;
2.5 Functionaris Gegevensbescherming: degene die is belast met het beheer van het camerasysteem;
2.6 beeldinformatie: de door het camerasysteem verkregen en geregistreerde filmbeelden.

Artikel 3 Plaats- en tijdbepaling cameratoezicht en video-opnames

3.1 Cameratoezicht vindt plaats op het schoolterrein van de scholen van Stichting Invitare. Binnen de scholen vindt cameratoezicht plaats op de plaatsen en de tijdvakken als omschreven in bijlage 1 bij dit protocol.
3.2 Video-opnames worden gemaakt in lessituaties, op incidentele basis. Over het moment waarop de opnames worden gemaakt worden de betrokken leerlingen en hun ouders/verzorgers vooraf geïnformeerd.
3.3 Indien een leerling en/of zijn ouders bezwaar hebben tegen de opnames die met het oog op begeleiding en coaching van personeel worden gemaakt, dan zal de school ervoor zorgen dat de leerling tijdens de opnames een dusdanige plek krijgt in de klas dat deze niet in beeld komt.

Artikel 4 Taken, verantwoordelijkheden en beveiliging

4.1 Het cameratoezicht en het maken van video-opnames geschiedt onder verantwoordelijkheid van het College van Bestuur.
4.2 Afhankelijk van de school en het doel worden specifieke medewerkers belast met het beheer van het camerasysteem. De namen zijn op school bekend.
4.3 Afhankelijk van de school en het doel worden specifieke medewerkers bevoegd tot het bedienen van het camerasysteem en het bekijken van de beelden zijn. De namen zijn op school bekend.
4.4 Degenen die toegang hebben tot de camera en videobeelden zullen daarmee strikt vertrouwelijk omgaan. Zij zullen geheimhouding betrachten (zie artikel 4.b. van het Privacyreglement).
4.5 Er zijn passende technische en organisatorische maatregelen getroffen ter beveiliging van de camerabeelden en het camerasysteem.

Artikel 5 Kenbaarheid

5.1 Het cameratoezicht wordt kenbaar gemaakt door middel van stickers op de plaatsen waar cameratoezicht plaatsvindt en bij de ingang van het terrein.
5.2 Video-opnames met als doel begeleiding en coaching worden uitsluitend gemaakt nadat daarvoor uitdrukkelijke toestemming van de betrokken personeelsleden is verkregen en de betrokken leerlingen vooraf zijn geïnformeerd.
5.3 Alle personeelsleden en ouders/verzorgers worden geïnformeerd over dit protocol.
5.4 Voor betrokkenen (niet zijnde personeelsleden of leerlingen) is het protocol beschikbaar via de site van Stichting Invitare.

Artikel 6 Doelbinding, zorgvuldigheid, bewaartermijnen en rechten van betrokkenen

6.1 De geregistreerde camera- en videobeelden worden uitsluitend gebruikt voor de doelstellingen zoals in dit protocol zijn verwoord.
6.2 Het gebruik van de camera- en videobeelden zal niet verder gaan dan strikt noodzakelijk is voor het doel waarvoor het toezicht is ingesteld.
6.3 De camerabeelden die gemaakt zijn met het oog op de veiligheid van de school worden na [4 weken] nadat deze zijn gemaakt, verwijderd. De camerabeelden mogen langer bewaard worden in het kader van een wettelijke bewaarplicht of als dat noodzakelijk is voor de afhandeling van geconstateerde incidenten. Zodra het incident is afgehandeld, worden de beelden vernietigd.
6.4 Videobeelden die zijn gemaakt met het oog op begeleiding en coaching van personeel, worden bewaard gedurende het begeleidingstraject. Na afronding van het begeleidingstraject of zoveel eerder als daarom door de medewerker wordt verzocht, worden de beelden vernietigd.
6.5 De betrokkene van wie beelden zijn vastgelegd heeft recht van inzage, recht op rectificatie, recht op wissing en recht op beperking van verwerking van gegevens conform artikel 6 van het Privacyreglement.

Artikel 7 Heimelijk cameratoezicht

7.1 Heimelijk cameratoezicht kan worden ingezet indien er sprake is van een serieus en concreet vermoeden van diefstal, c.q. andere onrechtmatigheden en Stichting Invitare er niet in is geslaagd om met behulp van minder vergaande middelen – waaronder het reguliere cameratoezicht – tot uitkomsten te komen.
7.2 Het heimelijk cameratoezicht wordt in duur en omvang zo beperkt mogelijk gehouden.
7.3 Het heimelijk cameratoezicht zal zich niet uitstrekken tot plaatsen waar de privacy van de betrokkenen onder alle omstandigheden gewaarborgd dient te zijn, waaronder in ieder geval doch niet uitsluitend, de was-en toiletruimten, de kamers van de schoolleiding, de vertrouwenspersoon e.d.

Bijlage 10: geheimhoudingsverklaring

De heer/mevrouw ……., hierna 'medewerker',

- werkzaam op basis van een aanstelling of
- werkzaam op basis van een uitzendovereenkomst of
- werkzaam als vrijwilliger of
- werkzaam als stagiair.

voor stichting Invitare Openbaar Onderwijs

verklaart zich akkoord met het volgende:

1. Medewerker heeft uit hoofde van zijn functie toegang tot persoonsgegevens van leerlingen en/of personeel. Medewerker heeft kennisgenomen van het Privacyreglement van de Stichting en de daarin opgenomen voorschriften die gelden bij het verwerken van persoonsgegevens waartoe hij toegang heeft.

2. Het is de medewerker zowel gedurende als na afloop van zijn arbeidsovereenkomst met de Stichting /zijn werkzaamheden voor de Stichting verboden om - ongeacht de wijze waarop en de redenen waarom de arbeidsovereenkomst/de werkzaamheden tot een einde is/zijn gekomen - op enigerlei wijze aan derden, direct of indirect, in welke vorm en op welke wijze dan ook enige mededeling te doen van of aangaande gegevens betreffende de leerlingen en personeel, waarvan de medewerker in het kader van de uitoefening van zijn werkzaamheden voor de Stichting kennis heeft genomen.

3. Deze persoonsgegevens zijn privacygevoelig en mogen uitsluitend worden verwerkt voor het doel waarvoor ze zijn verkregen. De medewerker zal zich bij zijn werkzaamheden ervan vergewissen dat gegevens van leerlingen en personeel uitsluitend worden gedeeld conform het in het Privacyreglement bepaalde.

4. De geheimhoudingsplicht mag worden doorbroken indien het verstrekken van de informatie aan derden logischerwijs noodzakelijk is gezien de aard van de opdracht en de uitvoering van de functie van medewerker of indien er een wettelijke verplichting bestaat om de informatie aan een derde te verstrekken.

5. Indien medewerker een (mogelijke) inbreuk op de beveiliging signaleert waarbij (mogelijk) persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking, meldt de medewerker dit per omgaande aan de Functionaris Gegevensbescherming (FG) ongeacht het tijdstip van de dag. De medewerker is te allen tijde bevoegd zelfstandig een melding te doen bij de voorzitter van het bestuur (info@stichting-invitare.nl / 0485- 351287) dus ook bij het ontbreken van een voorafgaande melding aan de FG.

Plaats : ……. Datum: ……..

Naam : ……. Handtekening: …….

Bijlage 11: Regeling taken en verantwoordelijkheden Functionaris Gegevensbescherming

Bron: Handreiking Functionaris Gegevensbescherming po/vo versie 1.0 (24 januari 2018) door PO-Raad, VO-raad en Kennisnet.

Artikel 1: definities

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

Artikel 2: 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 Invitare;
    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 met alle verwerkingen persoonsgegevens binnen Stichting Invitare;
    f. Het (laten) afhandelen van klachten inzake privacy;
    g. Overige door het bestuur of directie van Stichting Invitare 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 3: 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 Invitare in gebruik zijn en waar persoonsgegevens worden verwerkt, te betreden.
2. De FG is bevoegd inlichtingen te vorderen van eenieder die onder gezag of in opdracht van Stichting Invitare werkzaam is of overeenkomstig voor of namens de stichting 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 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 4: Weigering

1. Eenieder, die werkzaam is bij en/of in opdracht werkt van de verantwoordelijke, is verplicht aan de FG medewerking te verlenen, die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden.
2. Indien de medewerking aan de uitoefening van de bevoegdheden van de FG zoals bedoeld in artikel 3, wordt geweigerd, kan het schoolbestuur, 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 schoolbestuur wordt zo spoedig mogelijk in kennis gesteld over de uitvoering van het bepaalde in dit artikel.

Artikel 5: Geheimhouding

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

Artikel 6: Regeling

1. Deze regeling wordt vastgesteld en gewijzigd bij besluit van de Verwerkingsverantwoordelijke.

Bijlage 12: Privacy statement voor op de websites

Stichting Invitare Openbaar Onderwijs neemt privacy serieus. Indien u wilt weten welke persoonsgegevens wij over u en/of uw kind hebben vastgelegd, dan kunt u altijd contact opnemen met de school.

In dit privacy statement wordt in het kort beschreven hoe wij met persoonsgegevens van bezoekers van deze website omgaan en deze beveiligen.

Doeleinden van de gegevensverwerking van bezoekers van de website
Als u een contact- of aanmeldformulier op de website invult, of ons een e-mail stuurt, dan worden de gegevens die u ons toestuurt bewaard zolang als naar de aard van het formulier of de inhoud van uw e-mail nodig is voor de volledige beantwoording en afhandeling daarvan.

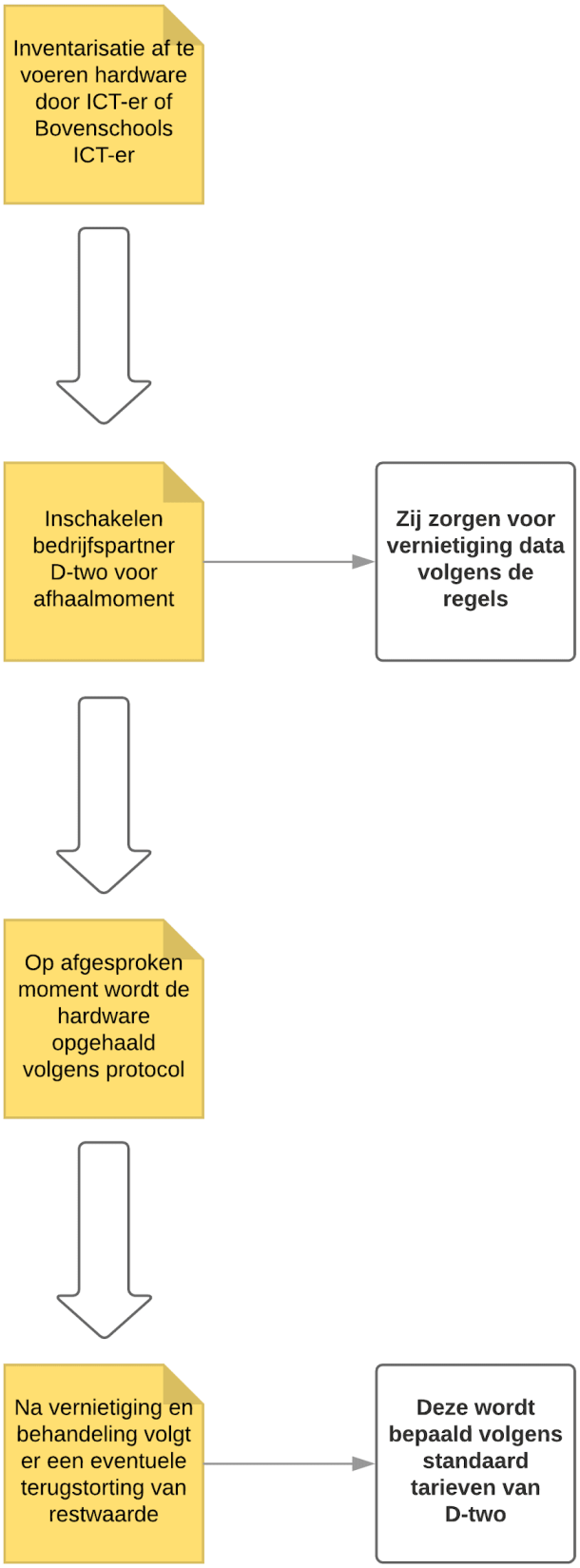
Klikgedrag en bezoekgegevens
Op de website worden algemene bezoekgegevens bijgehouden. In dit kader kan met name het IP-adres van uw computer, de eventuele gebruikersnaam, het tijdstip van opvraging en gegevens die de browser van een bezoeker meestuurt, worden geregistreerd en worden gebruikt voor statistische analyses van bezoek- en klikgedrag op de website. Tevens optimaliseren wij hiermee de werking van de website. Wij proberen deze gegevens zo veel mogelijk te anonimiseren. Deze gegevens worden niet aan derden verstrekt.

Sociale media
Op deze website kunnen knoppen opgenomen zijn om pagina's te delen op sociale netwerken (Sharepoint, Facebook en Twitter. Deze knoppen worden gerealiseerd door een code die wordt aangeleverd door Facebook en Twitter zelf. Deze code plaatst onder meer een cookie (zie boven).

Leest u de privacyverklaring van Facebook en van Twitter (welke regelmatig kunnen wijzigen) om te zien wat zij met uw persoonsgegevens doen die zij met deze code verwerken.

Gebruik van functionele cookies
Wij maken bij het aanbieden van elektronische diensten gebruik van functionele cookies. Een cookie is een eenvoudig klein bestandje dat met pagina's van deze website wordt meegestuurd en door uw browser op de harde schijf van uw computer wordt opgeslagen. Wij gebruiken cookies om uw instellingen en voorkeuren te onthouden. U kunt deze cookies uitzetten via uw browser, zie bijvoorbeeld deze toelichting door de Consumentenbond voor uitleg. Ons cookiegebruik is in overeenstemming met de daarvoor geldende regels uit onder meer de Telecommunicatiewet. Voor het gebruik van deze cookies hebben wij geen toestemming nodig.

Bijlage 13: Verwijderen hardware…



Bijlage 14: Uitdiensttreding; *Wat moet ik doorgeven?*

Het zal regelmatig voorkomen dat er personele wijzigingen zijn of iemand uit dienst gaat bij jullie om welke reden dan ook. Het is in deze tijd van AVG en Privacy extra belangrijk dat wij van ICT dit dan ook te weten komen zodat we zorg kunnen dragen voor het afsluiten van accounts en juiste verwerking van alle gegevens. Vandaar dus dit lijstje waarin jullie kunnen zien waar rekening mee te houden.

- Opzeggen of opschorten account O365;
- Opzeggen of opschorten account Google (@jeschoolnaam.nl);
- Opzeggen of opschorten account Cloudwise;
- Wisselingen in OR of (G)MR-samenstelling;
- Wisselingen in werklocatie (bijvoorbeeld bij mobiliteit);
- Inleveren van eventuele mobiele telefoons, laptops of andere devices.

Geef ons alstublieft zo spoedig mogelijk door:
- Om wie gaat het (volledige naam)?
- Op welke locatie is deze persoon werkzaam?
- Wat is zijn of haar functie en wat wordt die eventueel?
- Per wanneer gaat de wijziging in?

De school is zelf verantwoordelijk voor:
- Het opschonen en bijhouden van Parnassys;
- Educatieve software (als dat al niet via koppelingen van Parnassys gebeurt);
- Afmelden bij eventuele alarmdienst.

Alles wat er dus gemeld moet worden, mailen naar Marco van Oort: m.voort@stichting-invitare.nl

Bijlage 15: Mailen of delen?

N.B. de termen die in deze tekst gebruikt worden kunnen op jouw scherm soms anders zijn. Zo staat bij sommige in plaats van "versleutelen" het woord "beveiligen". Dat is niet erg, want de inhoud van die knopen is hetzelfde.

Wanneer je een document hebt dat je ook aan anderen wilt geven dan moet je mailen of delen. Dit kan zowel in Office 365 als in Google. Wanneer kies je nu voor delen en wanneer voor mailen? Delen doe je als je een document hebt waarin je bijvoorbeeld samen wilt werken. Mailen doe je als het niet nodig is om in een document samen te werken maar wanneer je iemand stukken wil doen toekomen of iemand wilt informeren of ergens over wilt bevragen.

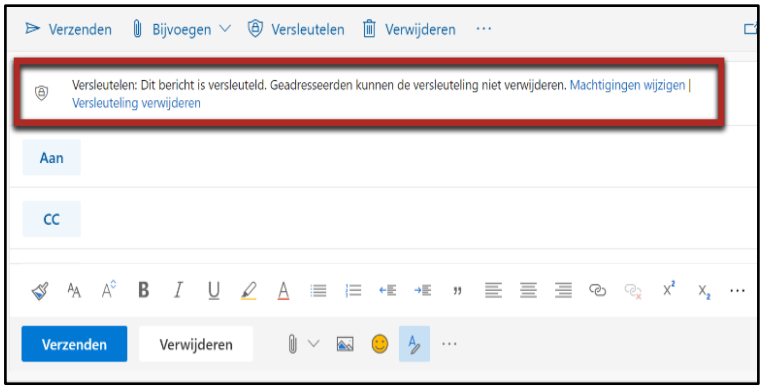
1. Mailen

- Versleuteld => dit doe je als je documenten wil versturen met daarin privacygevoelige informatie; denk aan handelingsplannen, medische gegevens, of rapporten en/of resultaten, maar ook adresgegevens. Met andere woorden gegevens gekoppeld aan of te herleiden naar een persoon;
- Niet versleuteld => in principe alle andere mails. Let wel!! jouw verzend-emailadres moet ingesteld zijn als @stichting-invitare.nl

1.1 Hoe versleutel je mail in Office365?

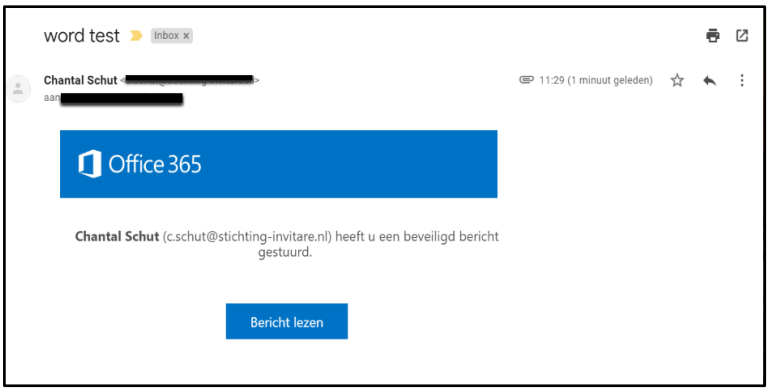
Als je een mail wil versturen met informatie die beveiligd moet worden (handelingsplannen, medische gegevens en/of andere persoonsgegevens van leerlingen of van personeel; met andere woorden gegevens gekoppeld aan of te herleiden naar een persoon), kan je dat doen met de knop versleutelen. Deze staat boven elke nieuwe mail
Deze knop zorgt ervoor dat een externe persoon de mail niet zomaar kan openen maar een code moet gaan ophalen.

Als je dat gedaan hebt krijg je onderstaande zin te zien. Zo weet je altijd dat een mail versleuteld is.



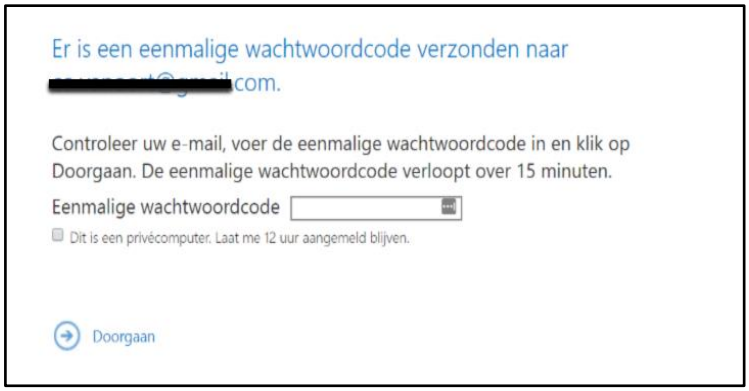
Je kunt de machtigingen van de versleuteling wijzigen door te klikken op “machtigingen wijzigen”. Je kan dan bijvoorbeeld kiezen voor de variant “niet doorsturen. Standaard is de instelling “versleutelen” het beste.

Voor de ontvanger ziet dit er als volgt uit wanneer hij deze mail opent



Klik dan op “bericht lezen”; dan verschijnt volgend scherm

Klik dan op “Meld u aan” met eenmalige code. Je ontvangt nu een nieuwe mail met een eenmalige code. Voer die in dit veld in.



Nu kan je de mail en de eventuele bijlagen openen en lezen.

1.2 Hoe versleutel je in Gmail (E-mailversleuteling tijdens de overdracht)?
S/MIME wordt gebruikt om geavanceerde versleuteling te ondersteunen tijdens de berichtoverdracht. Je uitgaande e-mails worden automatisch versleuteld als dat mogelijk is. Opmerking: Deze stappen werken alleen als je S/MIME hebt ingeschakeld voor je account.

Controleren of een bericht dat je wilt verzenden, is versleuteld:

1. Begin met het opstellen van een bericht;
2. Voeg ontvangers toe in het veld "Aan";
3. Rechts van je ontvangers wordt een hangslotpictogram weergegeven waarmee het versleutelingsniveau wordt aangegeven dat wordt ondersteund door de ontvangers van je bericht. Als er meerdere gebruikers met verschillende versleutelingsniveaus zijn, geeft het pictogram de laagste versleutelingsstatus weer;
4. Klik op het hangslot en "Details weergeven" om je S/MIME-instellingen te wijzigen of meer informatie over het versleutelingsniveau van je ontvanger te bekijken.

Controleren of een bericht dat je hebt ontvangen, is versleuteld:

1. Open een bericht;
2. Klik op de pijl-omlaag ▾ rechts van de mensen die de e-mail hebben ontvangen;
3. Er wordt een gekleurd hangslotpictogram weergegeven dat aangeeft welk versleutelingsniveau is gebruikt om het bericht te verzenden.

Betekenis van de versleutelingspictogrammen:
Wanneer je berichten verzendt of ontvangt, kunt je het versleutelingsniveau van een bericht bekijken. De kleur van het pictogram verandert op basis van het versleutelingsniveau.

Groen (uitgebreide versleuteling via S/MIME) 🔒. Geschikt voor de meest gevoelige informatie. S/MIME versleutelt alle uitgaande berichten als we beschikken over de openbare sleutel van de ontvanger. Alleen de ontvanger met de bijbehorende privésleutel kan dit bericht ontsleutelen.

Grijs (standaardversleuteling via TLS) 🔒. Geschikt voor de meeste berichten. TLS (Transport Layer Security) wordt gebruikt voor berichten die worden uitgewisseld met andere e-mailservices die geen ondersteuning bieden voor S/MIME.

Rood (geen versleuteling) 🔓. Niet-versleutelde e-mail die mogelijk niet veilig is. Eerdere berichten die zijn verzonden naar het domein van de ontvanger, worden

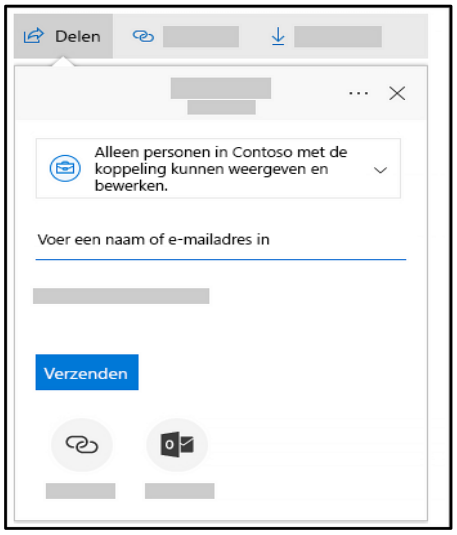
gebruikt om te voorspellen of het bericht dat je verzendt, niet op betrouwbare wijze wordt versleuteld.

Ik zie het rode hangslotpictogram:
Als je een bericht schrijft en het rode hangslotpictogram wordt weergegeven, kun je overwegen deze adressen te verwijderen of de vertrouwelijke informatie te wissen. Klik op "Details weergeven" om te bekijken welk adres niet is versleuteld. Als je een bericht met het rode hangslotpictogram hebt ontvangen en het bericht bijzonder gevoelige content bevat, stel je de afzender hiervan op de hoogte. Hij kan dan contact opnemen met zijn e-mailprovider.

2. Delen

2.1 Delen binnen Office 365

Selecteer het bestand (of de map) die je wilt delen en selecteer "Delen".



Voer de namen in van de personen of groepen waarmee je het bestand of de map wilt delen. Je hebt ook de mogelijkheid om een bericht toe te voegen. Optioneel: Klik op de vervolgkeuzelijst om het type koppeling te wijzigen. Het deelvenster "Details" wordt geopend. Hier kun je wijzigen wie de koppeling kan openen en of het gedeelde item kan worden bewerkt. Opties voor "Wie moet deze koppeling kunnen gebruiken?"

"Iedereen": hiermee krijgt iedereen toegang die deze koppeling ontvangt, rechtstreeks dan wel doorgestuurd door iemand anders. Dit kunnen personen van buiten jouw organisatie zijn.

- Personen in <uw organisatie>: hiermee kan iedereen in de organisatie de koppeling openen, of ze de koppeling rechtstreeks ontvangen of krijgen doorgestuurd.
- Personen die al toegang hebben: hiermee deel je het document of de map met personen die er reeds toegang tot hebben. Hierdoor worden de machtigingen voor het item

niet gewijzigd. Gebruik deze optie als je alleen een koppeling wilt verzenden naar iemand die al toegang heeft.

- Bepaalde personen: hiermee kunnen alleen de personen die je opgeeft de koppeling openen, hoewel andere personen deze mogelijkheid al kunnen hebben. Als de uitnodiging voor delen wordt doorgestuurd, dan kunnen alleen personen die al toegang tot het item hebben, de koppeling gebruiken.

De optie "Bewerken toestaan" is standaard ingeschakeld. Als je wilt dat anderen jouw bestanden alleen kunnen bekijken, schakel je het selectievakje uit. Klik op "Toepassen" wanneer je klaar bent. Klik op "Verzenden" als je de koppeling wilt verzenden.

2.2 Delen binnen Google

Stap 1: Zoek het bestand dat je wilt delen:
Eén bestand delen:

1. Ga op een computer naar Google Drive
2. Klik op het bestand dat je wilt delen.
3. Klik op Delen of op het deelpictogram .

Stap 2: Kies met wie je wilt delen en hoe anderen je bestand kunnen gebruiken:

Delen met bepaalde mensen

1. Geef bij Mensen het e-mailadres op waarmee je wilt delen. Opmerking: Als je deelt met een e-mailadres dat geen Google-account is, kan de ontvanger het bestand alleen weergeven.
2. Klik op de pijl-omlaag om te kiezen wat iemand met je bestand kan doen. Meer informatie over hoe anderen bestanden kunnen weergeven, bewerken of erop kunnen reageren.
3. Als je geen e-mail wilt verzenden naar mensen, klik je op "Geavanceerd" en verwijder je het vinkje uit het selectievakje "Meldingen verzenden". Als deze optie is ingeschakeld, wordt elk opgegeven e-mailadres opgenomen in de e-mail.
4. Klik op "Verzenden".

Bijlage 16: Wachtwoordenbeleid

We gaan ervan uit dat medewerkers zorgvuldig met hun wachtwoorden omgaan. Dat betekent onder andere dat wachtwoorden naar omgevingen waar zich privacygevoelige informatie bevindt nooit gedeeld worden met andere personen. Het zichtbaar ophangen van persoonlijke wachtwoorden is niet toegestaan.

In de systemen waar Stichting Invitare zelf het wachtwoordenbeleid kan bepalen en waar privacygevoelige data wordt opgeslagen (wordt periodieke maar minimaal eens per jaar) afgedwongen dat medewerkers een nieuw sterk wachtwoord kiezen. Ook worden accounts in die omgevingen automatisch uitgelogd als deze langere tijd ongebruikt ingelogd zijn op een apparaat. Ook in andere systemen raden we gebruikers aan regelmatig hun wachtwoord te vernieuwen.

We gaan met betrekking tot wachtwoordeneisen en -gebruik uit van drie basisregels:
- Je wachtwoord nooit delen, dat is iets van jou;
- Je wachtwoord mag niet gemakkelijk te raden zijn (bijvoorbeeld: Mijnkatisliefennietgroen!);
- Je wachtwoord niet hergebruiken.

Wij hebben voor Invitare de bruikbaarheid van een aantal wachtwoordenapps bekeken en vooralsnog besloten dat centrale aanschaf (waarbij het centrale beheer mogelijk is) te duur is.

Bijlage 17: Checklijstjes in het kader van de privacy van leerlingen en hun ouders/verzorgers

Onderstaande lijst dient als hulpmiddel voor een school om te verifiëren of er voldoende zorg is/wordt besteed aan de handhaving van het "Reglement verwerking leerlingengegevens Stichting Invitare Openbaar Onderwijs" en de overige afspraken in het "Privacybeleid van Stichting Invitare Openbaar Onderwijs.

- Zitten de leerlingendossiers en de werkdossiers achter slot?
- Zijn de digitale programma's (leerling-administratie en leerlingvolgsysteem) beveiligd en beperkt toegankelijk via wachtwoorden?
- Is het helder voor alle leerkrachten dat de leerlingendossiers te allen tijde op school aanwezig dienen te zijn?
- Is het helder voor alle leerkrachten welke functionaris bevoegd is tot het tekenen van welke uitgaande stukken?
- Zijn er heldere afspraken op schoolniveau over de inrichting van de leerlingendossiers en de werkdossiers (zie onderstaand hulplijstje)?
- Zijn stagiairs, studenten en hulpouders gewezen op de vertrouwelijke status van hetgeen zij horen en zien in de school, het liefst schriftelijk (zie voorbeeldbrief)?
- Zijn er overeenkomsten getekend met de vrijwilligers, waarin wordt gewezen op de vertrouwelijke status van hetgeen zij horen en zien in de school?
- Zijn allen die betrokken zijn bij de begeleiding van leerlingen zich ervan bewust dat er niet over leerlingen wordt gesproken in bijzijn van derden (dus bijvoorbeeld in de koffiekamer of de gangen, met name als er gasten zijn)?
- Is er bij inschrijving toestemming gevraagd aan ouders/verzorgers om bepaalde gegevens op te nemen in een klassenlijst ter verspreiding onder klasgenootjes? Wordt dit regelmatig actief geverifieerd?
- Zijn ouders/verzorgers erop gewezen dat er beeldmateriaal, teksten e.d. van hun kinderen incidenteel in communicatieve uitingen van de school worden opgenomen en dat de school dat alleen doet als de leerlingen hierdoor niet in verlegenheid worden gebracht?
- Is in de schoolgids en op de website van de school een tekst opgenomen waarin ouders erop gewezen worden dat ze tegen vermelden van de naam van hun kind en/of beeldmateriaal, teksten e.d. van hun kinderen bezwaar kunnen maken?
- Is de school zich ervan bewust dat bij vermelding van het schoolblad/nieuwsblad op de website de gegevens openbaar worden. Is de school voldoende kritisch op de inhoud?
- Realiseren wij ons dat op de website nooit namen gecombineerd met telefoonnummers en adressen vermeld mogen staan?
- Zijn de ouders in de MR en OR gewezen op de vertrouwelijke status van onderwerpen die herleidbaar zijn tot bepaalde ouders/verzorgers c.q. leerlingen dan wel medewerkers?
- Worden toehoorders bij de MR-vergaderingen verzocht om de vergadering te verlaten op het moment dat er onderwerpen worden besproken die herleidbaar zijn tot bepaalde ouders/verzorgers c.q. leerlingen dan wel medewerkers?
- Zijn de leerkrachten op de hoogte van de afspraak dat verzoeken om inzage van een dossier door de directie wordt afgehandeld?

Hulplijstje: wat moet in een dossier aanwezig zijn?

- Uitslagen van toetsresultaten;

- Gegevens uit het leerlingvolgsysteem;
- Handelingsplannen / dyslexiedossier;
- Verslagen van gesprekken met de ouders/verzorgers;
- Afspraken met ouders / verzorgers;
- Wanneer relevant het onderwijskundige rapport van de vorige school;
- Rapporten;
- Getekend inschrijfformulier;
- Wanneer relevant uitschrijfbewijs en een kopie van het onderwijskundige rapport dat aan een volgende school is toegestuurd.

Suggesties:
- Een algemeen opmerkingenblad waarop alle contacten worden genoteerd met betrekking tot de leerling;
- Werkaantekeningen van de leerkrachten horen thuis in het werkdossier van het lopende schooljaar. Wellicht zinvol om ze achter een tabblad "werkaantekeningen" op te bergen.
- Aan het einde van een schooljaar dienen de bovengenoemde stukken uit het werkdossier te worden overgeheveld in het leerlingendossier van betreffende leerlingen. De werkaantekeningen blijven echter in het werkdossier.