Handboek Informatiebeveiliging en privacy

Versie 1.0 , 13 juni 2018

Inhoudsopgave

Inleiding

Informatie en ict zijn noodzakelijk in de uitvoering van het onderwijs. Omdat we met persoonsgegevens van medewerkers, leerlingen en anderen werken, is privacywetgeving daarop van toepassing. Deze wetgeving bepaalt niet alleen onder welke voorwaarden persoonsgegevens gebruikt mogen worden, maar geeft ook aan dat er passende technische en organisatorische maatregelen op het gebied van informatiebeveiliging en privacy (afgekort: IBP) genomen moeten worden om persoonsgegevens te beschermen. Hiervoor is er binnen Het bestuur een IBP-beleidsplan opgesteld. Dit plan is op te vragen bij de beleidsmedewerker P&O.

Ons beleid is dat we op al onze scholen voldoen aan de privacywetgeving die wordt gesteld door de overheid. Dat betekent dat wij zorgvuldig omgaan met de gegevens van leerlingen, ouders, verzorgers en personeel. We zorgen ervoor dat onze digitale systemen voldoen aan de regels en dat alle teamleden goed weten hoe te handelen met privacygevoelige informatie. In het geval er toch iets misgaat melden wij dit – indien nodig – bij de Autoriteit Persoonsgegevens.

Dit handboek is bedoeld om uitvoering te geven aan het IBP-beleidsplan. In het handboek staan richtlijnen, procedures, afspraken en praktische handreikingen die nodig zijn om informatiebeveiliging en privacy goed te regelen. Deze maatregelen nemen we niet alleen omdat de wet dit voorschrijft, maar ook op basis van de normen en waarden die wij vanuit onze visie op onderwijs met elkaar delen en uitdragen: De Stichting 'Ieder kind telt' staat voor christelijk primair onderwijs in de gemeente Hellendoorn.

De missie van de Stichting ‘Ieder kind telt’ is het unieke van elk kind als schepsel van God te waarderen en te respecteren. Vanuit een christelijke inspiratiebron vorm en inhoud te willen geven aan opvoeding en onderwijs. Kennis en vaardigheden belangrijk te vinden, maar ook het omgaan met waarden en normen in het omgaan met elkaar.

Het handboek is onderverdeeld in twee delen voor afzonderlijke doelgroepen:

Deel A - Alle medewerkers
Dit deel bevat de algemene informatie die voor alle medewerkers binnen het bestuur van belang is. Van alle medewerkers wordt verwacht dat zij op de hoogte zijn van de afspraken die hierin vermeld staan en hier ook naar handelen.

Deel B – Schoolleiders en leidinggevenden
In dit deel is informatie terug te vinden die vooral van belang is voor de schoolleider: hoe zorg ik ervoor dat het IBP-beleid op mijn school goed geregeld is?

Elk deel begint met de meest gestelde vragen, waarop doorgeklikt kan worden om snel de antwoorden te kunnen vinden.

Deel A

Informatie voor alle medewerkers

Veelgestelde vragen

- Welke afspraken gelden er voor mij als het gaat om de verwerking van leerlinggegevens?
- Waar moet ik mij aan houden bij het gebruik van sociale media?
- Welke gegevens bewaart de school van mij en anderen en waarom?
- Waar moet ik op letten bij het gebruik van beeldmateriaal en online diensten?
- Als ik gegevens kwijt ben of ik heb een vermoeden van misbruik, bij wie moet ik dan zijn?
- Waar moet ik persoonsgegevens of persoonlijke informatie opslaan?
- Waar moet ik op letten bij het verzamelen of delen van gegevens?
- Waar moet ik op letten bij het uitwisselen van gegevens met externe partijen?

Vuistregels Privacy

Privacy is een lastig en vaag begrip. Privacy op school gaat over de bescherming van gegevens van leerlingen, hun ouders en medewerkers. Dit wordt geregeld in de Algemene Verordening Gegevensbescherming (voorheen de Wet Bescherming Persoonsgegevens).

In onderstaande vuistregels van Kennisnet worden de belangrijkste uitgangspunten voor het verantwoord omgaan met persoonsgegevens samengevat.

Wat zijn persoonsgegevens?
Dit zijn gegevens die direct over iemand gaan, ofwel naar deze persoon te herleiden zijn. Er zijn vele soorten persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats. Maar ook telefoonnummers en postcodes met huisnummers zijn persoonsgegevens. Gevoelige gegevens als iemands ras, godsdienst of gezondheid worden ook wel bijzondere persoonsgegevens genoemd.

Binnen ons bestuur worden gegevens van zowel leerlingen, ouders als medewerkers verwerkt. Welke gegevens dit zijn en voor welke doeleinden deze worden verwerkt staat omschreven in het privacyreglement.

Binnen ons bestuur spreken we met elkaar af dat we altijd nagaan of we aan deze vuistregels voldoen bij het verzamelen en verstrekken van persoonsgegevens aan de hand van de volgende vragen.

☐	**1. Doel en doelbinding** Heb ik vooraf een doel voor de verwerking van persoonsgegevens vastgesteld? Worden de persoonsgegevens alleen gebruikt voor dat doel dat ik vooraf heb vastgelegd?
☐	**2. Grondslag** Is er minimaal een wettelijke grondslag voor de verwerking? Er is een wettelijke grondslag als… • er een wettelijke plicht bestaat om deze gegevens te verstrekken. Bijv. voor bekostiging, inspectie, overdrachtsdossier, etc.; • er toestemming is verkregen van de ouders/verzorgers. Bijv. voor de begeleiding van een leerling door externe onderwijsspecialisten, foto's op website, etc.; • de partij een publiekrechtelijke taak heeft. Bijv. de uitwisseling van informatie met samenwerkingsverbanden; • dit nodig is voor het uitvoeren van een overeenkomst met de ouders/verzorgers. Bijv. voor de TSO van kinderen; • er sprake is van een gerechtvaardigd belang, zoals het goed laten werken van digitale leermiddelen. Bijv. voor Basispoort en educatieve uitgeverijen.
☐	**3. Dataminimalisatie** Gebruik ik alleen die gegevens die noodzakelijk zijn om het vastgestelde doel te verwezenlijken? Kan ik met minder of bijvoorbeeld anonieme gegevens werken? Bewaar ik de gegevens niet langer dan nodig?

☐	4. Transparantie Heb ik de leerling of zijn ouders vooraf helder geïnformeerd over het doel van de gegevensverwerking? Heb ik uitgelegd welke gegevens worden gebruikt en met wie deze worden gedeeld?
☐	5. Data-integriteit Kloppen de persoonsgegevens die ik gebruik nog steeds? Zijn de gegevens op het juiste moment, op de juiste plaats en voor de juiste mensen beschikbaar? Heb ik onjuiste gegevens gecorrigeerd of verwijderd?

Gedragscode

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

De afspraken zijn verdeeld in drie onderdelen:
A. Waar en hoe bewaar ik persoonsgegevens?
B. Hoe en wat communiceer ik online via e-mail en sociale media?
C. Hoe houd ik indringers op afstand?

Hieronder volgen per onderdeel de gedragsregels die voor iedereen gelden bij de verwerking van gegevens van zowel leerlingen, ouders als die van medewerkers.

A. Waar en hoe bewaar ik persoonsgegevens?

1. *Verwerk persoonsgegevens zoveel mogelijk digitaal in de daarvoor aangewezen bewaarplaatsen.*
   Leerlinggegevens worden zoveel mogelijk digitaal opgeslagen, geraadpleegd en bewerkt in een leerlingadministratie- of volgsysteem, zoals ParnasSys. Dit geldt ook voor gegevens die via ouders/verzorgers en/of externen worden ontvangen.
   Personeelsgegevens worden zoveel mogelijk digitaal opgeslagen in het financiële administratiesysteem en HR-systeem. Er worden geen persoonsgegevens op USB-sticks bewaard.
   Gegevens die op papier aangeleverd worden, worden gescand en aan bovengenoemde systemen toegevoegd. Vergeet niet om de scan van je eigen computer en uit je mail te verwijderen.

2. *Formuleer gegevens die je vastlegt over een persoon zorgvuldig en professioneel.*
   Ouders en medewerkers hebben het recht om hun dossier in te zien. Zorg ervoor dat de gegevens zodanig zijn geformuleerd dat dit kan. Het past ook bij je houding als professional.

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

4. *Ga na welke afspraken er binnen de school gemaakt zijn voordat je persoonsgegevens uitwisselt met derden.*
   Wanneer je gegevens uit wil wisselen met externen, zoals bijvoorbeeld de logopedist, een arbo- of schoolarts, jeugdzorg of een schoolbegeleidingsdienst dan is het nodig om toestemming te vragen van ouders. Zorg dat je de toestemming registreert en hou daarbij ook rekening met de verdeling van het ouderlijk gezag. Voor de uitwisseling

van gegevens met het samenwerkingsverband of een andere school gelden aparte afspraken. Vraag de IB-er voor meer informatie hierover.

Ook al vragen derden om de levering van persoonsgegevens, je bent niet altijd verplicht om ze te geven. Controleer bij het verzamelen of delen van persoonsgegevens of hiervoor een wettelijke grondslag bestaat aan de hand van de Vuistregels Privacy. Tip: Bekijk in het privacyreglement met welke partijen gegevens (mogen) worden uitgewisseld.

5. *Informeer derden (ouders, hupverleners etc.) wanneer je door hen aangeleverde informatie (zowel geschreven als mondeling) opslaat in het leerlingdossier.*
Wanneer je bijvoorbeeld telefonisch contact hebt over een leerling met een hulpverlener en je wilt die informatie opslaan in het leerlingdossier. Informeer dan zowel de hulpverlener als de ouders welke informatie je aan het dossier toevoegt.

B. Hoe en wat communiceer ik online?

1. *Maak gebruik van een link naar het digitaal administratiesysteem om persoonsgegevens uit te wisselen met collega's.*
Verstuur persoonsgegevens bij voorkeur niet per mail, maar verstuur een link met de online bewaarplaats van de benodigde gegevens.

2. *Vraag ouders om toestemming om een (privé)account aan te maken voor online diensten.*
Leerlingen (jonger dan 16 jaar) moeten toestemming hebben van hun ouders/verzorgers om een (privé)account aan te maken voor onlinediensten zoals, Google etc. Dit punt staat in het toestemmingsformulier.

3. *Deel over leerlingen, ouders of collega's nooit privacygevoelige informatie via social media.* Doe dit vooral in persoon of desnoods via de telefoon. Wat je communiceert via social media kan makkelijk anders worden geïnterpreteerd door de lezer als je hier niet alert op bent.

4. *Deel alleen kennis en informatie over de school als het geen vertrouwelijke of persoonlijke informatie betreft en andere betrokkenen en de naam van de school niet schaadt.*
Wees voorzichtig met het online uiten van standpunten. Privé-meningen van medewerkers kunnen eenvoudig verward worden met de officiële standpunten van de school en/of het bestuur. Je blijft altijd persoonlijk verantwoordelijk voor wat je deelt of publiceert. Wees je ervan bewust dat gepubliceerde uitlatingen voor onbepaalde tijd openbaar zullen zijn, ook na het verwijderen van het bericht.
Het is voor medewerkers van ons bestuur niet toegestaan standpunten en/of overtuigingen uit te dragen die in strijd zijn met de missie en visie van de stichting en de school.

5. *Ga voordat je foto's of video's publiceert waar leerlingen op te zien zijn na of ouders hiervoor toestemming hebben gegeven.* Dit punt staat in het toestemmingsformulier.

Meer informatie hierover is te vinden in het onderdeel Toestemming foto's, video's en online diensten.

6. *Gebruik de accounts die door de school worden beheerd als je met anderen wil communiceren via e-mail of social media.*
   Formuleer je boodschap ook hier professioneel en zorgvuldig.

7. *Zet e-mailadressen altijd in de BCC-regel als je naar (grote) groepen mensen een bericht verstuurt.*
   Zo blijven de e-mailadressen van de groepsleden afgeschermd.

8. *Wanneer je een bericht stuurt met belangrijke en/of gevoelige informatie naar (een groep) ouders/verzorgers laat dit dan nalezen door een collega.*
   Een foutje is snel gemaakt en bovendien kan een ander kan je boodschap anders interpreteren dan jij hem bedoeld hebt. Het is dan fijn als er iemand met je meeleest voordat je hem verstuurt.

9. *Stuur nooit een e-mailbericht door naar derden zonder de degene van wie je het bericht ontvangen hebt hierover te informeren.*

C. Hoe houd ik indringers op afstand?

1. *Zorg er bij vertrouwelijke (telefonische) gesprekken voor dat er niet kan worden meegeluisterd.*
   Trek je je even terug als een gesprek een vertrouwelijk karakter heeft of krijgt.

2. *Bewaar laptops of tablets altijd op een veilige plek, zeker tijdens vakantieperiodes.*
   Het is een open deur, maar toch gebeurt het heel erg makkelijk. Maak elkaar er dus op attent als je een laptop of tablet onbeheerd ziet liggen. Als je computer gestolen wordt, heeft dat gevolgen voor de school en de leerling.

3. *Klik alleen op linkjes en open alleen bijlagen in e-mails van betrouwbare afzenders en pas op met het downloaden van bestanden.*
   Virussen kunnen makkelijk worden binnengehaald via (phising)mails. In het criminele circuit is dit een veelgebruikte methode om aan jouw gegevens te komen. Ook kunnen de gegevens op je computer versleuteld worden (ransomware).

4. *Meld je altijd af als je de computer onbeheerd achterlaat. En zorg ervoor dat er op je werkplek geen gevoelige informatie zichtbaar of voor het grijpen ligt, ook bij de printer.*
   Met de combinatie van de Windows- en L-toets kun je je makkelijk afmelden. Maak er een gewoonte van om papieren op je bureau om te draaien. Zo voorkom je dat anderen informatie zien die niet voor hen is bedoeld.

5. *Zet je digibord op freeze als je wachtwoorden intoetst of persoonsgegevens in je scherm ziet staan. En zorg dat niemand meekijkt als jij je wachtwoord intoetst.*
   Voordat je het weet zien leerlingen gevoelige gegevens of kunnen ze aan de hand van

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

6. *Laat je wachtwoorden van digitale (administratie)systemen met persoonsgegevens niet onthouden door je internetbrowser. En schrijf je logingegevens nooit op.*
   Maak gebruik van wachtwoordkluisjes, zoals Last Pass of True Key of de Sleutelhanger van Apple. Zonder dat je er erg in hebt, klik je de optie 'wachtwoord onthouden' in je browser aan. Heel makkelijk als je vaak moet inloggen, maar iemand anders kan dan dus ook inloggen. Kijk hier voor een tip om een sterk wachtwoord te kiezen die je makkelijk kunt onthouden.

7. *Houd je logingegevens altijd voor jezelf, ook al vragen anderen aan je om ze te delen.*
   Je login is in feite een sleutel om toegang te krijgen tot de informatie die voor jou toegankelijk moet zijn. Daarnaast herkent het systeem jou door je login, zodat het kan bijhouden wie welke gegevens heeft toegevoegd of gewijzigd.

In het verlengde van bovenstaande is het ook van belang dat leerlingen zich bewust zijn van risico's en er goede afspraken met hen gemaakt worden in het kader van privacy. In bijlage H is een voorbeeld opgenomen van dergelijke afspraken. Van iedere school wordt verwacht dat ze een dergelijk protocol hebben en toepassen.

Privacyreglement

Het privacyreglement is een verantwoordingsdocument waarin nauwkeurig en op een begrijpelijke manier beschreven is welke persoonsgegevens binnen de schoolorganisatie worden verwerkt en voor welke doeleinden. Ook is hierin te lezen wie toegang heeft tot deze gegevens, hoe de gegevens zijn beveiligd en met wie ze uitgewisseld mogen worden.

Het reglement is in te zien via de website www.iederkindtelt.nl Het reglement is ook als bijlage A toegevoegd bij dit handboek.

Ouders worden via het inschrijfformulier en via de website van de scholen gewezen op het privacyreglement.

Toestemming

Beeldmateriaal

Ouders, maar ook medewerkers, moeten altijd toestemming geven voor het gebruik van hun beeldmateriaal of die van hun kinderen. Die toestemming moet specifiek zijn. Dat betekent dat het voor ouders en medewerkers duidelijk moet zijn voor welk gebruik van het beeldmateriaal ze toestemming geven. Bijvoorbeeld voor het gebruik op de website, in een nieuwsbrief of de schoolgids. Ouders en medewerkers moeten ook de mogelijkheid hebben deze toestemming weer in te trekken.

De school moet een veilige omgeving zijn voor alle kinderen (en hun ouders) en zij moeten niet het risico lopen ongewenst gefotografeerd te worden.
Daarom wordt, voorafgaand aan activiteiten, aan ouders gevraagd om terughoudend te zijn met het maken van foto's en video's en is het niet toegestaan om foto- of video-opnames die gemaakt zijn op school te delen via sociale media of te gebruiken voor commerciële doeleinden. Dit is kenbaar gemaakt door deze afspraak op te nemen in het toestemmingsformulier en in de schoolgids en op de website.

Wanneer er activiteiten georganiseerd worden, zijn er vaak ouders die foto's of video's maken bijvoorbeeld bij feestelijke gelegenheden. We maken hierbij onderscheid tussen twee situaties:

- Ouders in algemene zin op het terrein van Stichting 'Ieder kind telt' bijvoorbeeld op het schoolplein. Als je ouders hier foto's of video's ziet maken, spreek ze hier dan op aan en wijs ze op de privacy van (andere) leerlingen. Echter is dit niet helemaal tegen te gaan en is er een grote mate van eigen verantwoordelijkheid van de ouders.
- Ouders die meegaan op schoolactiviteiten. Dit vereist duidelijke afspraken over het maken van beeldmateriaal. Zorg dat ouders alleen foto's en video's maken van kinderen wier ouders hiervoor specifiek toestemming hebben gegeven.

Het maken van foto's of video-opnamen van een leerling door (een medewerker van) Stichting 'Ieder kind telt' geschiedt altijd op basis van toestemming van ouders/voogden. Deze toestemming wordt in ieder geval eens per schooljaar aan ouders gevraagd. Ook bij de inschrijving van een leerling wordt hier toestemming voor gevraagd.

Het is op de Stichting 'Ieder kind telt' scholen gebruikelijk dat er tijdens de lessen video-opnamen worden gemaakt. Deze opnamen zijn bestemd om het lesgeven van de groepsleerkracht te verbeteren en worden niet buiten school gebruikt.

Af en toe worden er foto's video-opnamen gemaakt die gebruikt kunnen worden als voorlichtingsmateriaal. Als een kind hierop te zien is, kunnen deze opnamen alleen met toestemming van de ouder(s)/voogd(en) als zodanig worden gebruikt.

Online diensten

Voor het gebruik van online diensten door leerlingen binnen of buiten de school moeten ouders ook toestemming verlenen. Dit betekent dat wanneer leerlingen in de klas gebruik willen maken van een eigen (privé)account voor bijvoorbeeld WhatsApp of Pinterest, ouders

hier vooraf toestemming voor moeten geven. Dit betreft alleen online diensten die ook buiten de school om in het maatschappelijk verkeer gebruikt kunnen worden, dus niet voor e-mail, digitale leeromgevingen of leermiddelen waarvoor door de school zelf een account wordt verstrekt.

Uitwisseling persoonsgegevens

Wanneer je gegevens uit wil wisselen met externen, zoals bijvoorbeeld de logopedist, een arbo- of schoolarts, jeugdzorg of een schoolbegeleidingsdienst dan is het nodig om toestemming te vragen van ouders. Zorg dat je de toestemming registreert en hou daarbij ook rekening met de verdeling van het ouderlijk gezag.
Voor de uitwisseling van leerlinggegevens met het samenwerkingsverband of een andere school gelden aparte afspraken. Kijk hieronder in de tabel met welke partijen je gegevens mag uitwisselen en op welke manier.

Verstrekking aan	Doel	Uitwisseling toegestaan	Wijze waarop	Toestemming nodig?
Dienst Uitvoering Onderwijs	Bekostiging*	Ja	Koppeling ParnasSys	Nee
Educatieve uitgeverijen en Basispoort	Gebruik digitale leermiddelen	Ja	Koppeling ParnasSys	Nee (wel verwerkersovereenkomst)
Educatieve Apps	Onderwijs	Ja	Handmatige invoer	Ja, als ze ook na de schoolloopbaan gebruikt kunnen blijven worden door de leerlingen.
Basisscholen of scholen voor voortgezet onderwijs	Overdracht leerlingdossier (na aanmelding)*	Ja	Koppeling OSO	Nee (wel inzage)
Externe Onderwijsspecialisten	Zorgbegeleiding van een leerling	Ja	Verstrekken account	Ja
Stagiaires	Opleiden	Ja	Verstrekken account	Nee, wel stage-overeenkomst
Samenwerkingsverband	Toelaatbaarheidsverklaring afgeven*	Ja, zie ook: https://passendonderwijsenprivacy.nl	n.t.b.	Nee
TSO	Tussenschoolse opvang	Ja	n.t.b.	Ja
Activiteitencommissie	Innen ouderbijdrage	Ja	n.t.b.	Ja
GGD/JGZ	Bezoek schoolarts	Nee	n.v.t.	n.v.t.

Inspectie van het onderwijs	Toezicht*	Ja	Via Internet School Dossier (ISD)	Nee
Administratie- kantoor	Salarisadministratie en HR-management	Ja	n.t.b.	Nee
Leerplicht Gemeente	Controle verzuim	Ja	Verzuimloket	Nee

* Wettelijk verplicht

Gemeente en leerplichtambtenaren

De gemeente vraagt soms om informatie van leerlingen voor gemeentebeleid. Ook belt soms de leerplichtambtenaar voor een specifiek geval. Hoewel dit officiële instanties zijn, hebben zij niet altijd recht op informatie. De informatie die de gemeente nodig heeft en waar zij recht op heeft, krijgt zij via DUO en hoeft de school dus niet aan te leveren. Dit geldt dus ook voor de GGD. Overleg met de directeur, voordat je gegevens uitwisselt met andere organisaties.

Samenwerkingsverbanden

Voor de uitwisseling van leerlinggegevens met het samenwerkingsverband of een andere school gelden aparte afspraken. Hiervoor kun je terecht bij de zorgbegeleider. Kijk op https://passendonderwijsenprivacy.nl voor meer informatie over privacy en samenwerkingsverbanden.

Inspectie van het onderwijs

De inspectie mag alleen persoonsgegevens verwerken als dat voor haar wettelijke taken noodzakelijk is. In de voorbereiding van een schoolbezoek of bij het uitvoeren van haar toezichttaken vraagt de inspectie om documenten aan te leveren. Deze gegevens dienen zoveel mogelijk geanonimiseerd aangeleverd te worden. In uitzonderlijke gevallen heeft de inspectie voor het uitvoeren van hun toezicht- en handhavingsstaken wel persoonsgegevens nodig. Documenten die persoonsgegevens bevatten, moeten aangeleverd worden via het ISD (Internet Schooldossier). Het ISD kent een goede beveiliging. In het ISD kan aangevinkt worden dat het om persoonsgegevens gaat, zodat de Inspectie het op een juiste manier kan verwerken.

Vragen om informatie via de telefoon

Geef nooit zomaar gegevens door via de telefoon, als iemand belt om navraag te doen over een leerling of medewerker. Ook dan is het weer belangrijk om te controleren of diegene wel die gegevens mag krijgen.
Vraag altijd of de persoon het verzoek via de mail wil sturen. Dit geeft je de mogelijkheid om navraag te doen en uit te zoeken of de gegevens verstrekt mogen worden. Neem bij twijfel contact op met de schoolleider.

Burger Service Nummer (BSN)

Ons Nederlands recht schrijft voor dat je het BSN alleen mag verwerken als dit in de wet is bepaald óf als de doeleinden waarvoor je het verwerkt bij wet zijn bepaald.[1] Voor scholen betekent dit het volgende.

[1] Art. 46 Uitvoeringswet AVG

Een school mag/moet het BSN van een leerling verwerken:
1. Bij de toelating van een leerling tot de school;[2]
2. Door het nummer in de leerlingenadministratie van de school op te nemen;[3]
3. In het contact met de leerling (of zijn ouders);
4. Door het BSN aan de minister van OCW te verschaffen;
5. In het contact met deze minister over de bekostiging van de school;
6. In het contact met een gemeente in het kader van de Leerplichtwet;
7. In het contact met een andere school t.b.v. in- of uitschrijven en overleggen OKR;
8. Ter uitvoering van subsidieregelingen van het Europees Sociaal Fonds
9. In contacten met een andere school die valt onder de Wet op Expertise Centra t.b.v. de ondersteuning die deze school biedt;
10. Als eenmalige verwerking bij het aanmaken van een pseudoniem voor een leerling met het oog op het aanbieden van onderwijsvoorzieningen en begeleiding aan deze leerling;
11. Om het pseudoniem te bewaren in een leerlingadminstratiesysteem.

Een school mag het BSN van een leerling dus alleen in deze gevallen of voor deze doeleinden verwerken.

[2] Art. 40 b Wet op het primair onderwijs
[3] Voor punt 2 t/m 11 is de grondslag: art. 178a Wet op het primair onderwijs

Datalekken

Zijn er leerlinggegevens verloren gegaan? Is je laptop gestolen? Heb je last van een virus waardoor je niet meer bij je bestanden kunt? Of vertrouw je iets niet? Meld dit dan direct bij een leidinggevende. Als er persoonsgegevens beschadigd of verloren zijn, dan moet er mogelijk binnen 3 werkdagen een melding gedaan worden bij de Autoriteit Persoonsgegevens in het kader van meldplicht datalekken.

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

Voorbeelden van datalekken zijn:

- een e-mail die aan een verkeerd persoon geadresseerd is
- een kwijtgeraakte USB-stick
- inloggegevens die openbaar zijn geworden
- een gestolen iPad
- een gehackte computer

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

Ben je dus (een device met) persoonsgegevens kwijtgeraakt of heb je onrechtmatigheden geconstateerd met betrekking tot de toegang tot persoonsgegevens? Meld dit dan direct bij je leidinggevende en/of via privacy@iederkindtelt.nl

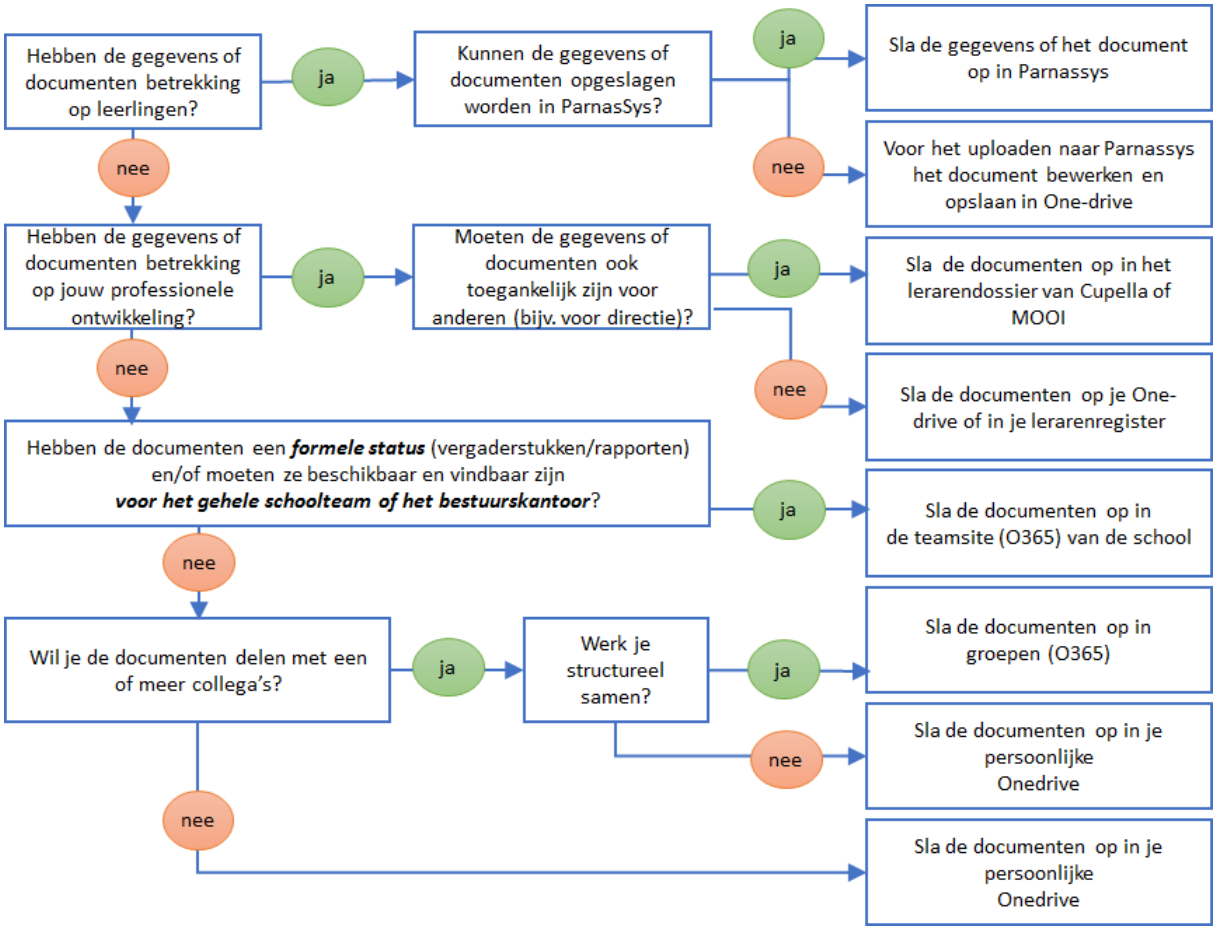
Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

In **bijlage E** is de volledige procedure melden datalekken opgenomen.

Document- en datamanagement

Om ervoor te zorgen dat we binnen de school onze documenten en gegevens (data) overzichtelijk en veilig opgeslagen hebben, zijn er afspraken over wat we waar bewaren. Op deze manier zijn documenten eenvoudiger terug te vinden, maar kunnen ze ook beter afgeschermd en geback-upt worden.

In het schema hieronder kun je nagaan op welke plek je gegevens en documenten op moet slaan.



Deel B

Informatie voor schoolleiders en leidinggevenden

Veelgestelde vragen

- Wat moet ik met ouders regelen rondom privacy?
- Welke afspraken moet ik maken met mijn medewerkers in het kader van privacy?
- Wat moet ik weten over datalekken?
- Wat moet ik weten als het gaat om het verlenen van toegang tot persoonsgegevens?
- Hoe lang moet ik persoonsgegevens bewaren?
- Welke afspraken maak ik over devices die in bruikleen worden gegevens?
- Wat moet ik weten over externe partijen die namens de school persoonsgegevens verwerken?
- Welke rollen en verantwoordelijkheden t.a.v. IBP zijn er binnen de schoolorganisatie belegd?
- Welke technische maatregelen moet ik geregeld hebben binnen de school?
- Hoe kan ik aantonen dat ik IBP op orde heb?

Ouders en privacy

Privacyreglement

Ouders hebben het recht om te weten welke gegevens er van hen en van hun kinderen worden verzameld door de school en voor welke doeleinden deze gegevens verzameld worden. Met het privacyreglement voldoet het bestuur aan zijn wettelijke informatieplicht, mits deze ook actief wordt aangeboden aan de ouders[4]. Daarom is het voor scholen belangrijk om het privacyreglement met ouders te communiceren.

In bijlage B en bijlage C is een tekst opgenomen die door alle scholen binnen het bestuur gebruikt wordt om ouders via de website en de schoolgids te wijzen op het privacyreglement van de school. Het kan in sommige gevallen nodig zijn om deze tekst uit te breiden indien er op school aanvullende bijzondere persoonsgegevens verwerkt worden. Ouders kunnen het reglement ook opvragen bij de directie van de school.

Toestemming

Voor het gebruik van foto- en filmopnames van leerlingen en medewerkers is toestemming vereist. Het handigste is om de toestemming voor het gebruik van foto-en filmopnames direct bij de inschrijving van een leerling of indiensttreding van een werknemer te regelen.
Om dit voor leerlingen te regelen is binnen ons bestuur een toestemmingsformulier beschikbaar gesteld. De tekst is te vinden in bijlage D. Hierop geven ouders aan of zij toestemming geven voor het gebruik van beeldmateriaal en voor welke doeleinden.
Als schoolleider is het belangrijk om ouders jaarlijks te herinneren (bijvoorbeeld via de nieuwsbrief en in de schoolgids) dat deze toestemming herroepen of alsnog verleend kan worden wordt. Maak ouders bewust van het feit dat film- en fotomateriaal dat wordt gemaakt in de school en tijdens schoolactiviteiten niet op sociale media geplaatst mag worden. Vraag ouders terughoudend te zijn wat betreft het maken van film- en fotomateriaal.

Wanneer je gegevens uit wil wisselen met externen, zoals bijvoorbeeld de logopedist, een arbo- of schoolarts, jeugdzorg of een schoolbegeleidingsdienst dan is het nodig om toestemming te vragen van ouders. Zorg dat je de toestemming registreert en hou daarbij ook rekening met de verdeling van het ouderlijk gezag.

[4] Ouders kan desgewenst ook gelezen worden als verzorgers.

Voorlichting en bewustwording onder medewerkers

Om informatiebeveiliging en privacy goed op orde te hebben is het nemen van maatregelen en het inrichten van procedures alleen niet voldoende. Het is minstens zo belangrijk dat iedereen binnen de organisatie op de hoogte is van deze maatregelen en procedures en dat er goede afspraken gemaakt worden met de medewerkers. Deze afspraken staan beschreven in het volgende hoofdstuk.

In dit hoofdstuk lees je wat er binnen [naam schoolbestuur] gedaan wordt en wat er van jou als schooldirecteur gevraagd wordt om medewerkers bewust te maken van het belang van informatiebeveiliging en privacy.

Medewerkers zullen de uitgangspunten van de AVG in hoofdlijnen moeten begrijpen om zelf de juiste afweging te maken als het gaat om het verwerken van persoonsgegevens. En zij zullen daarbij actief op de hoogte gehouden moeten worden van nieuwe ontwikkelingen rondom privacywetgeving. Bij nieuwe processen binnen de organisatie is het belangrijk om daarbij ook te kijken naar de impact op het IBP-beleid. Je kan hierbij denken aan het in gebruik nemen van een communicatie-applicatie, het aanschaffen van nieuwe (digitale) leermiddelen of het invoeren van groepsdoorbrekend werken. Is er sprake van nieuwe risico's, moeten er aanvullende maatregelen genomen worden of afspraken gemaakt worden?

Bovenschools

Tijdens een gezamenlijke studiedag kan er uitgebreid stilgestaan worden bij de nieuwe wetgeving en het IBP-beleid van [bestuur]. Voorafgaand aan de studiedag kunnen de scholen voorzien van voorlichtingsmateriaal voor zowel medewerkers als leerlingen en hun ouders.

Wanneer er nieuwe ontwikkelingen zijn met betrekking tot de AVG en het IBP-beleid van [naam schoolbestuur] zal de privacy officer dit in overleg met de functionaris voor de gegevensbescherming en het bevoegd gezag (bestuur) communiceren met de directeuren. Daarnaast zal er jaarlijks bovenschools een risicoanalyse gedaan worden samen met de directeuren. Waarin de situaties op de scholen meegenomen wordt. Waar mogelijk worden hieruit voortvloeiende maatregelen, procedures en afspraken bovenschools geregeld.

Tijdens bovenschoolse IB- en ICT-bijeenkomsten zal het onderwerp IBP ook regelmatig aan de orde komen.

Schooldirecteuren

Er wordt op school gestreefd naar een veilige werkplek waar met respect en aandacht voor ieders privacy gehandeld wordt. Als schooldirecteur heb je de taak om hierover zowel formeel als informeel het gesprek te voeren met je medewerkers.

Van directeuren wordt verwacht dat zij minimaal 1 keer per jaar uitgebreid stil staan bij het IBP-beleid op hun school, bijvoorbeeld tijdens een studiedag of teamvergadering. Er kan dan met het team gekeken worden naar mogelijke risico's en benodigde maatregelen. IBP-beleid op schoolniveau dient tevens opgenomen te zijn in het schoolplan. Hierin is duidelijk

aangegeven welke acties er op school ondernomen worden m.b.t. IBP en wie daarvoor verantwoordelijk is binnen het team.

Wanneer medewerkers nieuw zijn op school wordt in de inwerkperiode expliciet aandacht besteed aan de afspraken die er binnen [naam schoolbestuur] zijn rondom de verwerking van persoonsgegevens en het belang van informatiebeveiliging.

Afspraken met medewerkers

In dit handboek (deel A) zijn gedragsregels rondom informatiebeveiliging en privacy opgenomen die voor alle medewerkers binnen het bestuur gelden. Deze zijn hieronder in het kort weergegeven.

Het is belangrijk om medewerkers bewust te maken van het belang van deze regels rondom IBP en de gedragscode in te bedden in de schoolcultuur.

Laat de gedragsregels regelmatig terugkomen in gesprekken en tijdens overleggen. Besteed expliciet aandacht aan het hanteren van de Vuistregels Privacy bij het verzamelen en uitwisselen van gegevens.

A. Waar en hoe bewaar ik persoonsgegevens?

1. Verwerk persoonsgegevens zoveel mogelijk digitaal in de daarvoor aangewezen bewaarplaatsen.
2. Formuleer gegevens die je vastlegt over een persoon zorgvuldig en professioneel. Gebruik voor de verwerking van leerlinggegevens bij voorkeur een computer van school. Bij gebruik van een eigen device, de gegevens die lokaal zijn weggeschreven verwijderden na het afsluiten van de sessie.
3. Ga na welke afspraken er binnen de school gemaakt zijn voordat je persoonsgegevens uitwisselt met derden.
4. Informeer derden (ouders, hulpverleners etc.) wanneer je door hen aangeleverde informatie (zowel geschreven als mondeling) opslaat in het leerlingdossier.

B. Hoe en wat communiceer ik online?

1. Maak gebruik van een link naar het digitaal administratiesysteem om persoonsgegevens uit te wisselen met collega's.
2. Vraag ouders om toestemming om een (privé)account aan te maken voor online diensten.
3. Deel over leerlingen, ouders of collega's nooit informatie via sociale media.
4. Deel alleen kennis en informatie over de school als het geen vertrouwelijke of persoonlijke informatie betreft en andere betrokkenen en de naam van de school niet schaadt.
5. Ga voordat je foto's of video's publiceert waar leerlingen op te zien zijn na of ouders hiervoor toestemming hebben gegeven.
6. Gebruik de accounts die door de school worden beheerd als je met anderen wil communiceren via e-mail of sociale media.
7. Zet e-mailadressen altijd in de BCC-regel als je naar (grote) groepen mensen een bericht verstuurt. Verstuur mail berichten naar ouders het liefst via ParnasSys. Wanneer je een bericht stuurt met belangrijke en/of gevoelige informatie naar (een groep) ouders/verzorgers laat dit dan nalezen door een collega.

C. Hoe houd ik indringers op afstand?

1. Zorg er bij vertrouwelijke (telefonische) gesprekken voor dat er niet kan worden meegeluisterd.
2. Bewaar laptops of tablets altijd op een veilige plek, zeker tijdens vakantieperiodes.

3. Klik alleen op linkjes en open alleen bijlagen in e-mails van betrouwbare afzenders en pas op met het downloaden van bestanden.
4. Meld je altijd af als je de computer onbeheerd achterlaat. En zorg ervoor dat er op je werkplek geen gevoelige informatie zichtbaar of voor het grijpen ligt, ook bij de printer.
5. Zet je digibord op freeze als je wachtwoorden intoetst of persoonsgegevens in je scherm ziet staan. En zorg dat niemand meekijkt als jij je wachtwoord intoetst.
6. Laat je wachtwoorden van digitale (administratie)systemen met persoonsgegevens niet onthouden door de internetbrowser op openbare computers. En schrijf je logingegevens nooit op.
7. Houd je logingegevens altijd voor jezelf, ook al vragen anderen aan je om ze te delen.

Protocol melden datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplichting melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van deze melding kan leiden tot een fikse boete.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in de leerlingadministratie of digitale leermiddelen. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan moet de school met deze bewerkers aanvullende afspraken over het melden van datalekken.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten is dat persoonsgegevens verloren zijn gegaan. Er is persoonlijke informatie 'gelekt'. Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop de adresgegevens van klas 3b, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een bewerker voor de school. Er kan worden afgesproken dat een bewerker namens de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het schoolbestuur. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

De volledige procedure datalekken is te vinden in bijlage E.

Toegangsbeleid

Niet alle medewerkers hebben toegang nodig tot (alle) leerlinggegevens. Per rol is vastgesteld welke gegevens kunnen worden ingezien en gewijzigd, waarbij is gekeken wat die rol nodig heeft aan gegevens om zijn of haar werkzaamheden uit te kunnen voeren. Gegevens die daarbij niet noodzakelijk zijn, kan die rol ook niet inzien of wijzigen.

Uitgangspunten

1. Gegevens van leerlingen en medewerkers worden opgeslagen in de daarvoor aangewezen bewaarplaatsen (zie onderdeel Document- en datamanagement).
2. De afspraken met betrekking tot toegang tot en het verwerken van persoonsgegevens door de verschillende rollen binnen ons bestuur staan hieronder beschreven in een zogenaamde autorisatiematrix.
3. Alle accounts die worden verstrekt dienen te voldoen aan deze autorisatiematrix.
4. De directeur van de school is verantwoordelijk voor het verstrekken van de juiste toegang (lees: accounts met de juiste rollen en rechten). De directeur ziet er ook op toe dat de accounts worden ingetrokken na het beëindigen van een arbeids- of samenwerkingscontract of het wijzigen van functies. Daarnaast worden de accounts van systemen met persoonsgegevens periodiek gecontroleerd.
5. Naast het toepassen van de autorisatiematrix worden de volgende beveiligingsmaatregelen toegepast op systemen waarin persoonsgegevens worden gebruikt:
    - Inloggegevens worden verstuurd naar het e-mailadres van de medewerker dat beheerd wordt door (een school van) het bestuur.
    - Inloggegevens worden periodiek vernieuwd.
    - Er wordt technisch afgedwongen (waar mogelijk) om sterke wachtwoorden te gebruiken.

Autorisatiematrix

Er zijn 2 type autorisatiematrixen: Een matrix gericht op de systemen waarin gegevens van leerlingen worden verwerkt en een matrix gericht op de verwerking van gegevens van medewerkers.
De autorisatiematrixen hebben betrekking op de (externe) medewerkers die toegang moeten hebben tot de gegevens in de applicaties die onder de verantwoordelijkheid vallen van het bestuur. De matrixen gaan dus niet over de gegevens (uit de applicaties) die verstrekt worden aan derden, met uitzondering van ouders en leerlingen.

Functiegroepen
Om de autorisatiematrixen leesbaar te houden is gewerkt met functies en functiegroepen. De volgende functies vallen onder de functiegroepen die vermeld zijn in de matrixen.

Administratie	Facilitair	Financiële administratie (FA)	Personeel en Organisatie (P&O)	Groep-leerkracht	Kwaliteit
Secretariaat	Netwerk-beheerder	OBT/ Akorda	OBT/ Akorda Secretariaat	Betreffende groepsleerkracht	IB-er
Directeur					Directeur

Adm. medewerker					

Autorisatiematrix leerlinggegevens

Categorieën persoonsgegevens	Mag ingezien worden door de volgende functiegroepen:	Mag geregistreerd en gewijzigd worden door de volgende functiegroepen	Mag verwijderd worden door de volgende functiegroepen	Mag uitgewisseld worden door de volgende functiegroepen
Contactgegevens huisarts	*Administratie, groepsleerkracht, kwaliteit*	*Administratie*	*Administratie*	*Administratie*
Contactgegevens leerling	*Administratie, groepsleerkracht, kwaliteit*	*Administratie*	*Administratie*	*Administratie*
Contactgegevens ouder	*Administratie, groepsleerkracht, kwaliteit*	*Administratie*	*Administratie*	*Administratie*
Contactgegevens vorige school	*Administratie, groepsleerkracht, kwaliteit*	*Administratie*	*Administratie*	*Administratie*
Geslacht	*Administratie, groepsleerkracht, kwaliteit*	*Administratie*	*Administratie*	*Administratie*
Identificerende gegevens	*Administratie, groepsleerkracht, kwaliteit*	*Administratie*	*Administratie*	*Administratie*
Inschrijfgegevens	*Administratie, groepsleerkracht, kwaliteit*	*Administratie*	*Administratie*	*Administratie*
Kopie id bewijs	*Administratie*	*Administratie*	*Administratie*	*Administratie*
Nationaliteit en geboorteplaats	*Administratie*	*Administratie*	*Administratie*	*Administratie*
Naw-gegevens huisarts	*Administratie*	*Administratie*	*Administratie*	*Administratie*
Naw-gegevens leerling	*Administratie*	*Administratie*	*Administratie*	*Administratie*
Naw-gegevens ouders	*Administratie*	*Administratie*	*Administratie*	*Administratie*
Onderwijs-begeleidings-gegevens	*Groepsleerkracht* Kwaliteit*	*Groepsleerkracht, kwaliteit*	*Kwaliteit*	*Groepsleerkracht en kwaliteit*
Overeenkomsten	*Administratie, groepsleerkracht* kwaliteit*	*Administratie kwaliteit*	*Administratie kwaliteit*	*Administratie kwaliteit*
Resultaatgegevens	*Groepsleerkracht*, kwaliteit*	*Groepsleerkracht* kwaliteit*	*Groepsleerkracht* kwaliteit*	*Groepsleerkracht* kwaliteit*
Sancties	*Groepsleerkracht* kwaliteit*	*Kwaliteit*	*Kwaliteit*	*Kwaliteit*

School- en loopbaangegevens	*Administratie groepsleerkracht* kwaliteit*	*Administratie groepsleerkracht* kwaliteit*	*Administratie groepsleerkracht* kwaliteit*	*Administratie Groepsleerkracht* kwaliteit*
Zorgbegeleidingsgege-vens	*Groepsleerkracht* Kwaliteit*	*Groepsleerkracht* kwaliteit*	*Groepsleerkracht* kwaliteit*	*Groepsleerkracht* kwaliteit*

N.B. Alle functies die zijn gemarkeerd met een * hebben alleen toegang tot de gegevens van leerlingen die zij lesgeven/begeleiden. Personen die zijn gemarkeerd met een ** hebben alleen toegang tot de eigen gegevens.

Autorisatiematrix gegevens medewerkers

Categorieën persoonsgegevens	Mag ingezien worden door de volgende functies	Mag opgevraagd, toegevoegd en gewijzigd worden door de volgende functiegroepen	Mag verwijderd worden door de volgende functiegroepen	Mag uitgewisseld/ gekoppeld worden door de volgende functiegroepen
Contactgegevens medewerker	Administratie Groepsleerkracht**	Administratie	*Administratie*	*Administratie*
NAW-gegevens medewerker	*Administratie Fin administratie P&O Groepsleerkracht***	*Administratie*	*Administratie*	*Administratie*
Financien – declaraties (reiskosten)	*Administratie Fin. Administratie Groepsleerkracht***	*Administratie*	*Administratie*	*Administratie*
Financien – facturen	*Administratie Fin administratie Groepsleerkracht***	*Administratie*	*Administratie*	*Administratie*
Verzuimgegevens medewerkers	*Administratie P&O*	*Administratie*	*Administratie*	*Administratie*
Algemene overeenkomsten	*Administratie Fin administratie*	*Administratie*	*Administratie*	*Administratie*

N.B. Alle functies die zijn gemarkeerd met een * hebben alleen toegang tot de gegevens van medewerkers waaraan zij leiding geven. Personen die zijn gemarkeerd met een ** hebben alleen toegang tot de eigen gegevens.

Bewaartermijnen

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

Het bestuur hanteert mede op basis hiervan de bewaartermijnen voor persoonsgegevens zoals hieronder aangegeven.

Wanneer de bewaartermijn verstreken is moeten de betreffende gegevens vernietigd worden.

Gegevens	Maximale bewaartermijn (wettelijk verplicht)	Verantwoordelijke
Gegevens over verzuim en afwezigheid	5 jaar nadat een leerling is uitgeschreven	Directeur
Gegevens in- en uitschrijving (noodzakelijk voor berekening van bekostiging)	5 jaar nadat een leerling is uitgeschreven	Directeur
Gegevens die nodig zijn om te berekenen hoeveel bekostiging de school krijgt	7 jaar na afloop van het schooljaar waarop de bekostiging betrekking heeft	Directeur
Gegevens in het leerlingdossier	2 jaar nadat een leerling is uitgeschreven	Directeur
Gegevens met betrekking tot bezwaar-, klachten- of gerechtelijke procedure.	Maximaal 5 jaar nadat leerling is uitgeschreven.	Bestuurder/ Directeur
Medische gegevens in het leerlingdossier	2 jaar nadat een leerling is uitgeschreven	Directeur
Gegevens met betrekking tot bezwaar-, klachten- of gerechtelijke procedure.	2 jaar nadat een leerling is uitgeschreven	Directeur
Camerabeelden t.b.v. toezicht	Maximaal 4 weken, tenzij er een incident is vastgelegd.	Directeur
Gegevens in personeelsdossier met betrekking tot fiscale	5 jaar na uitdiensttreding	Bestuurder/ Directeur

bewaarplicht		
Overige gegevens in het personeelsdossier	2 jaar na uitdiensttreding	P&O
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk door personeel en leerlingen	Maximaal 6 maanden	Directeur i.s.m. / ICT-netwerkbeheerder
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, maximaal 2 jaar na uitdiensttreding voor benoemde collega.	Directeur/ P&O

N.B.
ParnasSys verwijdert niet de gegevens . De verantwoordelijke moet hier dus zelf een actie op zetten.

Afspraken over mobiele devices in bruikleen en privé-devices

Het bestuur en/of de school leent afhankelijk van de functie of aard van de werkzaamheden mobiele devices uit aan haar medewerkers. Dit kan gaan om een smartphone, tablet of een laptop. De devices zijn voorzien van beveiliging, zodat gegevens goed beschermd zijn. De devices zijn naast antivirus o.a. voorzien van back-up functionaliteit, encryptie (versleuteling van gegevens) en worden na inname weer opgeschoond.

Aanvullend hierop wil de school nog een aantal afspraken schriftelijk vastleggen over het gebruik van het device wanneer deze in bruikleen wordt gegeven aan een medewerker. Deze afspraken zijn vastgelegd in bijlage F van dit handboek.

Gebruik privé-devices

Mobiele devices in eigendom van de medewerker kunnen gebruikt worden voor schoolwerkzaamheden indien ze voorzien zijn van de volgende beveiligingseisen, zodat persoonsgegevens goed beschermd zijn.

- Het device is voorzien van een wachtwoord of code.
- Het device is voorzien van antivirussoftware.
- E-mail en andere apps of online toepassingen van [naam schoolbestuur] moeten afgeschermd worden met een apart wachtwoord.
- E-mail en andere apps of online toepassingen mogen niet toegankelijk zijn voor andere gebruikers.
- Wachtwoorden mogen niet onthouden worden in de browser.
- Er worden geen bestanden lokaal opgeslagen, maar alleen op de daarvoor aangewezen bewaarplaatsen van [naam schoolbestuur].
- De devices waarop persoonsgegevens worden verwerkt, worden niet gebruikt in een openbaar Wifi-netwerk, gebruik dan 4G.

Verwerkersovereenkomsten

In de privacywetgeving is bepaald dat het schoolbestuur als gegevensverantwoordelijke afspraken moet maken met alle leveranciers van de school die leerling gegevens verwerken in zogenaamde Verwerkersovereenkomsten. Het gaat hierbij bijvoorbeeld om uitgevers van digitaal lesmateriaal, leveranciers van toetsen, onderwijsadviesdiensten, etc.

Een uitzondering hierop vormt de uitwisseling van gegevens met de overheid (DUO) in het kader van bekostiging of toezicht of het Samenwerkingsverband in het kader van passend onderwijs.

De verwerkersovereenkomsten worden waar mogelijk bovenschools afgesloten. Hiervoor is in een inventarisatie gedaan van de lopende contracten van de scholen binnen het bestuur.

Wanneer een school een contract afsluit met een nieuwe leverancier zal er een nieuwe verwerkersovereenkomst gesloten moeten worden. De school is verplicht om nieuwe contracten door te geven aan het bestuur.

Wanneer het gaat om een leverancier die alleen een contract heeft met een individuele school, is de school zelf verantwoordelijk voor het afsluiten van de verwerkersovereenkomst. Wanneer het een contract met meerdere scholen betreft, dan wordt dit bovenschools geregeld.

Voor het afsluiten van verwerkersovereenkomsten wordt gebruik gemaakt van de meest actuele model verwerkersovereenkomst, die te vinden is via https://www.privacyconvenant.nl

Via het bestuurskantoor is een overzicht op te vragen van de leveranciers waar het bestuur op dit moment een verwerkersovereenkomst mee heeft. Voor vragen over het afsluiten van verwerkersovereenkomsten of het doorgeven hiervan, kan men terecht bij het bestuurskantoor.

Vragen of klachten over privacy

Het is belangrijk om klachten of vragen over privacy serieus te nemen. Om deze goed te beantwoorden is het nodig om kennis en expertise te hebben op het gebied van privacy.

Vandaar dat we binnen het bestuur hier een centraal punt voor in hebben gericht. Dit is de Functionaris Gegevensbescherming (FG)

Wettelijk hebben de personen (betrokkenen) van wie het bestuur persoonsgegevens verzamelen bepaalde rechten. Deze rechten zijn:

- Inzage en overdracht – een kopie van alle gegevens die over die persoon zijn verzameld
- Rectificatie – als blijkt dat de gegevens die zijn verzameld onjuist of onvolledig zijn, dan heeft die persoon het recht om deze gegevens te laten aanvullen of corrigeren
- Wissen – het is verplicht om gegevens te wissen als de persoon die om inzage heeft gevraagd dit vraagt. Dit is niet altijd het geval, soms heeft de school bijvoorbeeld een wettelijke plicht om bepaalde informatie te verwerken en kan zij dit niet zomaar verwijderen. Dit zal per geval moeten worden bekeken.

Als je zelf inzage wilt hebben in de gegevens die over jou zijn verzameld of je krijgt de vraag van een leerling of een ouder, dan kan dat op de volgende manier.

- Als **medewerker** kun je jouw vraag om inzage stellen aan de directeur.
- **Een ouder** die jou deze vraagt stelt, kun je doorverwijzen naar de directeur.

Rollen en verantwoordelijkheden

Binnen het vaststellen en uitvoeren van het IBP-beleid zijn verschillende rollen en verantwoordelijkheden vastgesteld binnen het bestuur. Deze zijn beschreven in het IBP-beleidsplan.

Dit handboek is bedoeld om praktische uitvoering te geven aan het IBP-beleid, met name ten aanzien van de organisatorische maatregelen. Voor de technische maatregelen voor informatiebeveiliging en privacy dienen afzonderlijke afpraken opgesteld te worden.

In het verlengde van de rollen en verantwoordelijkheden in het IBP-beleidsplan, zijn de volgende rollen en verantwoordelijkheden bepaald ten aanzien van het vaststellen van de inhoud en (de controle op) de toepassing van dit handboek.

Onderwerp	Verantwoordelijk voor	Rol/functie
Privacyreglement	Vaststellen	Bestuurder / GMR vaststellen
	Communicatie met ouders/ personeel.	Directeur/ P&O medewerker
Gebruik beeldmateriaal en online diensten	Toestemming vragen aan ouders en registreren	Directeur/ secretariaat
Uitwisseling persoonsgegevens	Bepalen met welke partijen persoonsgegevens uitgewisseld mogen worden en op welke wijze.	Directeur
	Toestemming vragen aan ouders en registreren	Directeur
Gedragscode	Vaststellen	Bestuur/ GMR
	Bewustwording en toezien op toepassing gedragscode	Directeur en secretariaat
	Toepassen gedragscode	Personeel
	Opstellen en toepassen protocol voor leerlingen	Werkgroep Privacy
Document- en datamanagement	Toepassen van technische beveiligingsmaatregelen (back-up, encryptie, etc.)	Directeur, ICT-er i.s.m. netwerkbeheer
	Vaststellen bewaarplaatsen	Directeur en secretariaat
	Vaststellen bewaartermijnen	Bestuur
	Vernietiging persoonsgegevens conform bewaartermijnen	Directeur P&O
Toegangsbeleid Verwerkersovereenkomsten	Verstrekken en intrekken accounts conform autorisatiematrixen	Directeur en secretariaat

	Toepassen technische beveiligingsmaatregelen (o.a. automatisch vernieuwen en sterkte wachtwoord)	(Bovenschools) ICT-er
	Doorgeven nieuwe verwerkers (leveranciers) aan bestuurssecretariaat	Directeur en ICT-er
	Afsluiten verwerkersovereenkomsten voor meerdere scholen	(Zie privacyconvenant.nl) Bestuurder regelt dit met alle partijen.
	Afsluiten verwerkersovereenkomsten voor individuele scholen	Directeur (meldingsplicht bij bestuur)
Datalekken	Protocol vaststellen	Werkgroep Privacy
	Datalekken doorgeven aan meldpunt	De ontdekker van het lek.
	Verzamelen meldingen en benodigde informatie	Bestuurder
	Afwegen, melden aan Functionaris Gegevensbescherming en registreren.	Bestuurder
	Afweging maken tot melding Autoriteit Persoonsgegevens	FG
	Melding maken bij Autoriteit Persoonsgegevens	FG
Devices in bruikleen	Afsluiten gebruikersovereenkomst voor devices die in bruikleen worden gegeven.	Bestuurder en directeur
Handboek Privacy	Controle en toezicht op toepassing handboek	Bestuurder i.s.m. met FG en directeuren

Checklist beveiliging ICT

Fysieke beveiliging en continuïteit van ict

- ☐ Persoonsgegevens worden uitsluitend verwerkt in een gesloten, fysiek beveiligde omgeving met bescherming tegen bedreigingen van buitenaf.
- ☐ Persoonsgegevens worden uitsluitend verwerkt op apparatuur waarbij maatregelen zijn genomen om de apparatuur fysiek te beveiligen en de continuïteit van de dienstverlening te verzekeren.
- ☐ Er worden periodiek back-ups gemaakt ten behoeve van de continuïteit van de dienstverlening. Deze back-ups worden vertrouwelijk behandeld, bewaard in een gesloten omgeving en na het verstrijken van de bewaartermijn vernietigd.
- ☐ De locaties waar gegevens worden verwerkt worden periodiek getest, onderhouden en periodiek beoordeeld op veiligheidsrisico's

De netwerk-, server- en applicatiebeveiliging

- ☐ De netwerkomgeving waarbinnen gegevens worden verwerkt is strikt beveiligd. Daarbij worden verkeersstromen gescheiden en zijn maatregelen geïmplementeerd tegen misbruik en aanvallen.
- ☐ De omgeving waarbinnen persoonsgegevens worden verwerkt wordt gemonitord.
- ☐ Op systemen worden periodiek de laatste (beveiligings)patches en updates geïnstalleerd.
- ☐ Penetratietests en vulnerability assesssments worden periodiek uitgevoerd.
- ☐ Niet (meer) gebruikte informatie wordt verwijderd.
- ☐ Op wachtwoorden worden cryptografische maatregelen toegepast om deze gegevens veilig op te slaan.
- ☐ Er wordt voor inlogprocessen gebruik gemaakt van versleutelde verbindingen. De uitwisseling van persoonsgegevens aan derden in opdracht van <naam schoolbestuur> vindt versleuteld plaats.

Netwerkcomponenten

- ☐ De netwerkcomponenten binnen de scholen van <naam schoolbestuur> hebben enkel tot doel dat er gebruik kan worden gemaakt van de digitale omgeving via Unilogic, internet, copiers en printers en WIFI. Alle wifi-punten worden automatisch geüpdatet.
- ☐ Alle netwerkpunten (switches en routers) worden geüpdatet indien nodig. Alle netwerkcomponenten die password protected ingesteld kunnen worden zijn beveiligd.

Controle en toezicht

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

#	Maatregelen met betrekking tot privacy en informatiebeveiliging	Ja*/ Nee	Waaruit blijkt dit? *(cursief = voorbeeldvulling)*
1	Het **privacyreglement** wordt door de school jaarlijks onder de aandacht gebracht van ouders en medewerkers.	ja	*Opgenomen in het jaarrooster via nieuwsbrief of mail*
2	Voor de publicatie van **foto- en filmbeelden** en **online diensten** is door de school vooraf **toestemming** vastgelegd.	ja	*Formulier (digitaal)*
3	Met alle leveranciers die namens de school persoonsgegevens verwerken is een **verwerkersovereenkomst** afgesloten.	ja	*Bestuurlijk geregeld: database in Office 365*
4	Voor de uitwisseling van persoonsgegevens met derden, niet zijnde verwerkers, is **toestemming vastgelegd**. (bijv. SOT)	ja	*Toestemmingsformulier (Bijlage D)*
5	Het **protocol datalekken** is bij de medewerkers bekend. Men weet wat er van hen verwacht wordt. (Protocol wordt gedeeld via het SharePoint)	ja	*Ja, vraag medewerkers steekproefsgewijs*
6	Toegang tot software en systemen met persoonsgegevens op school worden verleend conform de **vastgestelde toegangsmatrixen**.	ja	*Per bestuur dit regelen. Matrix is op alle scholen gelijk. Directeur controleert*
7	De afspraken **over de bewaarplaatsen van gegevens en informatie** (Document- en datamanagement) worden nageleefd.	ja	*Protocol wordt jaarlijks verstrekt en doorgenomen*
8	Er wordt middels een **gedragscode** en een **protocol voor leerlingen** structureel en regelmatig aandacht besteed aan de zorgvuldige verwerking van persoonsgegevens.		*Per bestuur en per school Aandacht in lesprogramma*
9	Bij **uitdiensttreding** worden alle accounts ingetrokken en apparatuur ingenomen.	ja	*Looplijstje*
10	Voor alle door de school/ bestuur uitgegeven apparatuur aan medewerkers zijn **gebruikers-overeenkomsten** afgesloten.	ja	*Getekend contract bij directeur/ secretariaat*
11	**Fysieke ruimtes** op school met persoonsgegevens van gevoelige aard (op papier of op server) **zijn beveiligd** tegen onbevoegde toegang.	ja	*Kasten zijn op slot*
12	**Er wordt voldaan aan de checklist beveiliging ICT**		

Bijlagen

A. Privacyreglement

Inleiding
Informatie en ict zijn noodzakelijk in de ondersteuning van het onderwijs. Omdat we met persoonsgegevens (van onszelf, leerlingen en anderen) werken, is privacywetgeving daarop van toepassing. Deze wetgeving bepaalt niet alleen onder welke voorwaarden persoonsgegevens gebruikt mogen worden, maar geeft ook aan dat er passende technische en organisatorische maatregelen genomen moeten worden om de persoonsgegevens te beschermen.

Dit protocol beschrijft hoe binnen ons bestuur wordt omgegaan met de verwerkingen van persoonsgegevens en de beveiliging van de informatie.
Dit protocol is onderdeel van het privacy handboek voor medewerkers. Hierin staan naast dit protocol praktische afspraken over onder andere gegevensopslag, omgang met sociale media en internet en toestemming voor beeldmateriaal van leerlingen.

Met dit document wordt voldaan aan de wettelijke informatieplicht conform **Algemene Verordening Gegevensbescherming** (AVG) die in 2018 is ingegaan.

Dit document beschrijft het privacy protocol in concrete en begrijpelijke bewoordingen.
Het is bedoeld als centrale informatiebron voor alle betrokkenen (leerlingen, hun ouders/verzorgers, personeelsleden, etc.) en beschrijft per categorie het type verwerkingen, waarom die worden uitgevoerd, welke persoonsgegevens worden verwerkt en aan wie die gegevens worden verstrekt.

Dit document wordt jaarlijks herzien door de Privacy Officer.

1. Privacy van leerlingen en hun ouders

Om de doelstelling van de school waar te maken is het van belang goed te weten wie de leerling is, wat zijn of haar talenten en uitdagingen zijn en hoe het onderwijs voor deze leerling het beste kan worden verzorgd. Om hier een beeld van te krijgen worden persoonlijke gegevens van die leerling op school verzameld en bewaard. In dit hoofdstuk is te lezen om welke verzamelingen dit gaat, waarom die gegevens worden gebruikt, wie ze gebruikt en aan wie ze worden verstrekt.

1.1 Om welke gegevens gaat het?

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

Persoonsgegevens

De gegevens die worden verzameld en opgeslagen zijn:

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

Deze gegevens worden zoveel mogelijk digitaal opgeslagen.

1.2 Wat is het doel van de verzameling van deze gegevens?

Deze gegevens worden verzameld om:

- Overzicht te hebben van de leerlingen die onderwijs volgen
- Overzicht te hebben van de aard, organisatie en verloop van dat onderwijs per leerling en de behaalde studieresultaten
- Te communiceren met leerlingen en/of hun ouders/ verzorgers
- Persoonlijke (waaronder medische) omstandigheden van een leerling ende gevolgen

daarvan voor het volgen van onderwijs bij te houden
- Financieel beheer uit te kunnen voeren
- Aan de wettelijke eisen rond monitoring en verantwoording naar toezichthoudende instanties en zorginstellingen te kunnen voldoen
- Toegang tot de systemen te krijgen
- De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het bewaken van de consistentie en betrouwbaarheid van de opgeslagen gegevens te verzorgen
- De continuïteit en goede werking van de systemen te waarborgen

1.3 Wie hebben toegang tot de leerlinggegevens en hoe worden deze beveiligd?
Binnen de school hebben de volgende type medewerkers toegang tot (een deel van) de gegevens:
- Directeur-bestuurder, de directie en het MT
- Onderwijzend personeel
- Onderwijsondersteunend personeel (OOP: administratief, zorgcoördinator, IB)

Niet alle rollen hebben tot alle gegevens toegang. Per rol is vastgesteld welke gegevens kunnen worden ingezien en gewijzigd, waarbij is gekeken wat die rol nodig heeft aan gegevens om zijn of haar werkzaamheden uit te kunnen voeren. Gegevens die daarbij niet noodzakelijk zijn, kan die rol ook niet inzien of wijzigen.

Gegevens met betrekking tot administratie, inschrijving, onderwijsbegeleiding en zorg worden in ParnasSys opgeslagen. Voor ParnasSys is een toegangsbeleid opgesteld waarin is vastgelegd welke functies tot welke gegevens toegang mogen hebben. Dit beleid wordt jaarlijks gecontroleerd. Op dit moment gebruiken we nog de standaardrolverdeling van ParnasSys. Indien er nog papieren dossiers van leerlingen aanwezig zijn worden deze bewaard in een afgesloten ruimte/kast. Hiertoe hebben alleen medewerkers toegang die deze gegevens nodig hebben bij het uitvoeren van hun werkzaamheden.

In het privacy handboek is een overzicht opgenomen van de verschillende functies en welke gegevens zij kunnen inzien en/of wijzigen.

Inloggen bij ParnasSys is alleen voorbehouden aan medewerkers die in dienst zijn van het bestuur. Met de leveranciers als ParnasSys zijn zogenaamde verwerkersovereenkomsten (conform het model van de PO-raad) afgesloten, waarin ook afspraken zijn gemaakt over beveiliging en back-up van de data die in ParnasSys wordt opgeslagen.

De uitwisseling met de overheid en andere scholen gebeurt ook middels ParnasSys. Dit systeem voldoet om deze reden ook aan de nationale standaarden op het gebied van beveiliging die de overheid heeft bepaald.

Voor digitale leermiddelen en toetsen worden systemen van diverse leveranciers of uitgeverijen gebruikt. Met deze partijen worden of zijn verwerkersovereenkomsten afgesloten. Onderdeel hiervan is dat zij ook voldoen aan de nationale standaarden en voorzieningen met betrekking tot de veilige uitwisseling van persoonsgegevens. In dit kader zal op termijn gebruik worden gemaakt van de nummervoorziening die het mogelijk maakt om alleen nog maar gepseudonimiseerde gegevens met deze partijen uit te wisselen.

Een overzicht van leveranciers met wie een overeenkomst is afgesloten over de uitwisseling van persoonsgegevens is op te vragen bij de betreffende school.

1.4 Aan wie worden deze gegevens verstrekt?
De gegevens mogen in beginsel niet aan derden worden doorgegeven of door anderen worden ingezien zonder toestemming van de ouders, tenzij de school verplicht is om bepaalde persoonsgegevens te verstrekken, die noodzakelijk zijn voor de uitvoering van een wettelijke plicht. Toestemming van ouders vindt schriftelijk plaats en wordt opgeslagen in het leerling dossier.

Bij het uitwisselen van gegevens wordt altijd gecheckt of aan de vijf privacy-vuistregels wordt voldaan:

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

De gegevens worden verstrekt aan de volgende externe partijen:

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

1.5 Inzage en wijzigen
Wanneer men de persoonsgegevens wil inzien of wijzigen, dan kan men hiervoor een afspraak maken met de directeur van de betreffende school.

1.6 Bewaartermijnen
De persoonsgegevens van leerlingen worden uiterlijk 2 jaren na de uitschrijving van een leerling verwijderd, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan de wettelijke bewaarplicht.

2. Privacy van medewerkers

Niet alleen van leerlingen worden persoonsgegevens verwerkt binnen Het bestuur, maar ook van onze medewerkers. Soms zijn dat gegevens die direct samenhangen met de arbeidsverhouding tussen het bestuur en medewerkers, maar ook worden persoonsgegevens van onze medewerkers verwerkt in systemen die in gebruikt worden bij het geven en begeleiden van onderwijs. De informatie over persoonsgegevens van medewerkers is ook van toepassing op stagiaires.
In dit hoofdstuk is te lezen om welke verzamelingen het gaat, waarom die gegevens worden gebruikt, wie ze gebruikt en aan wie ze worden verstrekt.

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

2.2 Wat is het doel van de verzameling van deze gegevens?
Deze gegevens worden verzameld om:
- Onderwijs te geven en leerlingen te begeleiden en volgen, waaronder:
  - Opslag van leer- en toetsresultaten
  - Het terugontvangen van leer- en toetsresultaten om te verwerken in het leerlingvolgsysteem

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

Voor de organisatie van het onderwijs en begeleiding van leerlingen wordt gebruikt gemaakt van digitale systemen, waarin gegevens over hun prestaties en welbevinden worden vastgelegd. In deze systemen worden ook gegevens van onderwijzend personeel vastgelegd, gericht op het kunnen maken van een koppeling tussen leerling en leerkracht en om de opgeslagen gegevens van de leerlingen in te kunnen zien, aan te vullen en te wijzigen.

Voor het verzorgen van het onderwijs wordt, naast boeken, ook gebruik gemaakt van digitale onderwijsmiddelen. In deze onderwijsmiddelen, die worden afgenomen van externe leveranciers, worden persoonsgegevens verwerkt die nodig zijn voor de toegang tot en het gebruik van deze digitale producten en diensten. Voorbeelden van deze digitale

onderwijsmiddelen zijn, digitale (aanvullingen op) lesmethodes, toetssystemen en apps. Ook in deze systemen worden persoonsgegevens van onderwijzend personeel opgeslagen.

Tevens worden onderwijsondersteunende ICT-middelen, zoals iPads of andere (draagbare) computersystemen ingezet. Voor systeembeheer, beveiliging, logging en monitoring wordt software op deze middelen geïnstalleerd die persoonsgegevens verzamelen.

2.3 Wie hebben toegang tot de personeelsgegevens en hoe worden deze beveiligd?
Binnen de school hebben de volgende type medewerkers toegang tot (een deel van) de gegevens:

- Directeur-bestuurder, de directie en het MT (systemen voor organisatie en begeleiding onderwijs en formatieplanning)
- Administratief personeel (systemen voor organisatie en begeleiding onderwijs en formatieplanning)
- Stafmedewerker bestuursbureau
- Medewerkers salarisadministratie en financiën
- Personeelsadviseurs
- Leidinggevende van de betreffende medewerker
- P&O, bedrijfsvoering en financiën
- ICT-ondersteunend personeel

Niet alle rollen hebben tot alle gegevens toegang. Per rol is vastgesteld welke gegevens ingezien en gewijzigd kunnen worden, waarbij is gekeken wat die rol nodig heeft aan gegevens om zijn of haar werkzaamheden uit te kunnen voeren. Gegevens die daarbij niet noodzakelijk zijn, kan die rol ook niet inzien of wijzigen.

Voor personeelsgegevens die in dezelfde systemen worden verwerkt als die van leerlingen, gelden dezelfde maatregelen als in hoofdstuk 1.3. zijn genoemd.

Via OBT/ Akorda worden verzuimgegevens geregistreerd. Ook hiervoor geldt dat er binnen het bestuur een toegangsbeleid is opgesteld dat jaarlijks wordt gecontroleerd. Met beide partijen worden ook verwerkersovereenkomsten afgesloten. Toegang tot medische gegevens komt tot stand tussen de Arbodienst en medische specialisten (Arboarts/arbeidsdeskundige) zonder tussenkomst van het bestuur.

2.4 Aan wie worden deze gegevens verstrekt?
De *NAW*-gegevens worden verstrekt aan de volgende externe partijen:

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

2.5 Inzage en wijziging
Alle medewerkers binnen het bestuur hebben een eigen inlog voor het digitale personeelsdossier. Wanneer men vragen heeft over de persoonsgegevens of deze wil wijzigen dan kan men terecht bij de administratie van het bestuur. Wanneer men de persoonsgegevens wil inzien of wijzigen in de onderwijssystemen van de school, dan kan men hiervoor terecht bij de directeur van de betreffende school.

2.6 Bewaartermijnen
De persoonsgegevens van medewerkers worden uiterlijk 2 jaren na de beëindiging van het dienstverband van de medewerker verwijderd, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan de wettelijke bewaarplicht.

3. Privacy van derden
In sommige gevallen worden gegevens van derden opgeslagen, die geen leerling, ouder of medewerker zijn. Denk bijvoorbeeld aan sollicitanten en extern ingehuurd personeel.
In dit hoofdstuk is te lezen om welke verzamelingen dit gaat, waarom die gegevens worden gebruikt, wie ze gebruikt en aan wie ze worden verstrekt.

3.1. Sollicitanten
In een sollicitatieproces worden persoonsgegevens verwerkt van sollicitanten. Deze paragraaf beschrijft hoe binnen ons bestuur met deze gegevens wordt omgegaan.

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

Deze gegevens worden verzameld om:
- De geschiktheid van een sollicitant te beoordelen voor een functie die vacant is of kan komen
- De veiligheid binnen de organisatie te borgen
- De door de sollicitant gemaakt onkosten af te handelen
- De uitvoering of toepassing van een andere wet te borgen

Binnen het bestuur hebben alleen medewerkers die betrokken zijn bij de sollicitatieprocedure toegang tot de persoonsgegevens van de sollicitanten.

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

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

Inzage en wijziging
Alle medewerkers binnen het bestuur hebben een eigen inlog voor het digitale personeelsdossier. Wanneer men vragen heeft over de persoonsgegevens of deze wil wijzigen, dan kan men hiervoor terecht bij de afdeling P&O.

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

Persoonsgegevens
De gegevens die worden verzameld en opgeslagen zijn:
- Naam, voornamen, geslacht, geboortedatum, adresgegevens en soortgelijke voor communicatie bedoelde gegevens
- Bedrijfsgegevens en bankrekeningnummer van de extern ingehuurde medewerker
- Kopie verstrekte VOG
- De gegevens voor de organisatie en begeleiding van onderwijs zoals vermeld in paragraaf 2.1.

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

Binnen de school hebben de volgende type medewerkers toegang tot de gegevens:
- Medewerkers salarisadministratie en financiën
- Personeelsadviseurs
- Opdrachtgever van de betreffende externe medewerker
- Hoofd P&O, bedrijfsvoering en financiën
- ICT-ondersteunend personeel

Deze gegevens worden verstrekt aan uitzendbureaus en detacheringsbureaus waarmee door het bestuur wordt samengewerkt.

Bijzonderheden

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

Inzage en wijziging
Wanneer men de persoonsgegevens wil inzien of wijzigen, dan kan men hiervoor terecht bij de afdeling personeelszaken.

3.3. Vrijwilligers
Vrijwilligers, met name ouders van (oud)leerlingen, worden op de verschillende scholen ingezet om te helpen bij schoolactiviteiten zoals sportdagen en excursies.
Van de vrijwilligers worden alleen gegevens verzameld en opgeslagen die nodig zijn om contact met hen te onderhouden en vergoeding te kunnen betalen. Het betreft naam, adres, telefoonnummer, e-mailadres en bankrekeningnummer.

Voor inzage en wijziging kan de betreffende vrijwilliger terecht bij de administratie van de school waar hij of zij vrijwilligerswerk verricht.

3.4 Oud-leerlingen
Voor het onderhouden van contacten met en het verzenden van informatie aan oud-leerlingen worden de volgende gegevens opgeslagen:

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

4. Datalekken
Wanneer de kans bestaat dat er persoonsgegevens in handen zijn gekomen van derden die geen toegang zouden moeten hebben tot die gegevens of wanneer de mogelijkheid bestaat dat er persoonsgegevens verloren zijn gegaan dient dit direct gemeld te worden bij het bevoegd gezag. Het bevoegd gezag is verantwoordelijk voor eventuele melding van een datalek bij de Autorisatie Persoonsgegevens, indien er onterecht geen melding gedaan wordt kan dit leiden tot fikse boetes. De volledige procedure melden datalekken is opgenomen in het privacy handboek.

5. Klachten
Indien men van mening is dat het privacy protocol niet op de juiste wijze wordt nageleefd binnen het bestuur kan er een klacht worden ingediend bij fg@iederkindtelt.nl
Wanneer deze klacht voor de betrokkene niet leidt tot een acceptabele oplossing kan men zich wenden tot het bestuur.

B. Tekst voor op de website en/of in de schoolgids

Privacy en leerlinggegevens

De gegevens die over leerlingen gaan, noemen we persoonsgegevens. In het privacyreglement van het bestuur is beschreven hoe de school omgaat met persoonsgegevens, en wat de rechten zijn van ouders en leerlingen. Dit reglement is met instemming van de GMR vastgesteld.

Wij maken alleen gebruik van persoonsgegevens als dat nodig is voor het leren en begeleiden van onze leerlingen, en voor de organisatie die daarvoor nodig is. De meeste gegevens ontvangen wij van ouders bij de inschrijving op onze school. Daarnaast registreren leerkrachten en ondersteunend personeel gegevens over leerlingen, bijvoorbeeld cijfers en vorderingen. Soms worden er bijzondere persoonsgegevens geregistreerd als dat nodig voor de juiste begeleiding van een leerling, zoals medische gegevens (denk aan dyslexie of ADHD). De leerlinggegevens worden opgeslagen in ons (digitale) administratiesysteem ParnasSys. Dit programma is beveiligd en toegang tot die gegevens is beperkt tot medewerkers van de stichting die de gegevens strikt noodzakelijk nodig hebben voor de uitvoering van hun werkzaamheden.

Tijdens de lessen maken wij gebruik van digitale leermiddelen. Hiervoor wordt een beperkte set met persoonsgegevens uitgewisseld met leveranciers om bijvoorbeeld een leerling te identificeren als die inlogt.

Wij hebben met leveranciers duidelijke afspraken gemaakt over de gegevens die ze van ons krijgen. De leverancier mag de leerlinggegevens alleen gebruiken als wij daar toestemming voor geven. Een lijst van de leveranciers waar de school afspraken mee heeft gemaakt, is op te vragen bij de school.

Daarnaast kan het nodig zijn dat wij gegevens uitwisselen met andere externe partijen, denk aan zorginstanties. Deze zijn vermeld in het privacyreglement. Als voor de uitwisseling geen wettelijke verplichting bestaat, dan vragen wij u vooraf toestemming om met deze partijen gegevens te mogen uitwisselen.

Bij de inschrijving van uw kind(eren) vragen wij u om toestemming voor het gebruik van foto- en videomateriaal, het delen van uw contactgegevens met andere ouders en het gebruik van sociale media door uw kind(eren). U hebt te allen tijde het recht om deze toestemming te wijzigen. U kunt dit kenbaar maken via een mail aan de directeur.

De school vraagt ouders nadrukkelijk om terughoudend te zijn met het maken van foto’s en video’s binnen de school. Het is voor ouders niet toegestaan om foto’s/video’s die gemaakt zijn op school te delen via sociale media of te gebruiken voor commerciële doeleinden.

C. Tekst voor op de website (Responsible disclosure)

Bij <naam school> vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is.

Wij vragen je een bijdrage te leveren aan de veiligheid van ict-systemen en het beheersen van de kwetsbaarheid van ict-systemen. Dat kun je doen door de door jou ontdekte kwetsbaarheden op verantwoorde wijze bij <naam school> te melden. Als je een zwakke plek in één van onze systemen hebt gevonden horen wij dit graag zo snel mogelijk, zodat we aanvullende (beveiligings)maatregelen kunnen treffen.

Wij vragen je:

- Je bevindingen te melden via privacy@<naam school.nl>.
- De door jou ontdekte kwetsbaarheid niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of (persoons)gegevens van derden in te kijken, te verwijderen of aan te passen.
- Je bevinding/probleem niet met anderen te delen totdat de kwetsbaarheid is verholpen en alle (vertrouwelijke) gegevens die zijn verkregen door de kwetsbaarheid direct na het verhelpen daarvan te wissen.
- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden.
- Voldoende informatie te geven om de kwetsbaarheid te reproduceren zodat wij deze zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

Wij zeggen toe dat:

- We reageren zo spoedig mogelijk op jouw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing.
- Als je je aan bovenstaande voorwaarden houdt, wij geen aangifte van een strafbaar feit zullen doen of andere juridische stappen tegen je ondernemen betreffende de melding.*
- Wij jouw melding vertrouwelijk behandelen en je persoonsgegevens zonder jouw toestemming niet zullen delen met derden of verder zullen verwerken, tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Melden onder een pseudoniem is mogelijk.
- Wij je op de hoogte houden van de voortgang van het verhelpen van de kwetsbaarheid.
- In berichtgeving over de gemelde kwetsbaarheid wij je, indien je dit wenst, zullen vermelden als ontdekker van de kwetsbaarheid. Wij streven ernaar alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

* Let op: het feit dat <naam school> geen aangifte tegen jou zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar jouw handelen gehouden kan worden dan wel dat je strafrechtelijk kunt worden veroordeeld.

D. Toestemmingsformulier

Toelichting in het kader van privacywetgeving

De gegevens die u heeft ingevuld op het inschrijfformulier, worden opgeslagen in de leerlingadministratie van onze school. Uiteraard worden deze gegevens vertrouwelijk behandeld. Op onze administratie is de Algemene Verordening Gegevensbescherming van toepassing. Dit betekent onder andere dat de gegevens door ons worden beveiligd, en dat de toegang tot de administratie is beperkt tot alleen personeel die de gegevens strikt noodzakelijk nodig heeft. U heeft als ouder het recht om de door ons geregistreerde gegevens in te zien (voor zover die informatie betrekking heeft op uw kind). Als de gegevens niet kloppen, dan mag u van ons verwachten dat wij – op uw verzoek - de informatie verbeteren of aanvullen.
Een aantal vragen in dit inschrijfformulier zijn wij wettelijk verplicht aan u te stellen. Zo vragen wij naar uw opleidingsniveau. Dit heeft te maken met de wettelijke 'gewichtenregeling': het aantal leerkrachten aan onze school is mede afhankelijk van het totaal van het 'leerlinggewicht' van onze leerlingen.
Voor meer informatie over de omgang met de privacy van uw kind(eren), verwijzen wij u naar ons privacyreglement.

Toestemming

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

Foto- en videomateriaal

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

Adressenlijst

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

Online diensten

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

Hierbij verklaart ondergetekende, ouders/verzorger van ……, dat:

1. foto's en video's WEL gebruikt mogen worden:

- ❑ op het ouderportaal van de school
- ❑ in de (digitale) nieuwsbrief
- ❑ in de schoolkalender
- ❑ in de schoolgids
- ❑ op de website van de school
- ❑ in folders en flyers ter promotie van de school
- ❑ op sociale-media account van de school namelijk Klasbord
- ❑ Facebook
- ❑ Twitter
- ❑ Instagram

(kruis aan waar u toestemming voor geeft)

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

(* streep door wat niet van toepassing is)

	Ouder/verzorger 1	Ouder/verzorger 2
Naam:	_____	_____
Datum:	_____	_____
Plaats:	_____	_____
Handtekening:	_____	_____

E. Formulier uitwisseling derden

De ouders/verzorgers van (*doorstrepen wat niet van toepassing is)*

_____ (*Naam leerling)*

Geven toestemming aan: _____ (*Naam school)*

om de volgende gegevens: _____

te verstrekken aan: _____ (*Naam school/ instantie*)
Bijvoorbeeld: Logopedie, arts, Maatschappelijk werk, andere school bijvoorbeeld bij een overdracht.

Voor de volgende doeleinde(n): _____

_____

_____

	Ouder/verzorger 1	Ouder/verzorger 2
Naam:	_____	_____
Datum:	_____	_____
Plaats:	_____	_____

F. Protocol datalekken

Inhoudsopgave

Inleiding

Deze procedure maakt integraal onderdeel uit van het privacybeleid van de ons bestuur en is vastgesteld door het college van bestuur.

De procedure bestaat uit 5 onderdelen voor afzonderlijke doelgroepen, te weten:
A. Medewerkers en leerlingen (meldingen aan ict-coördinator of schoolleider)
B. Ict-coördinator of Schoolleider (meldingen aan bovenschoolse Privacyfunctionaris)
C. Privacyfunctionaris (meldingen aan Autoriteit Persoonsgegevens)
D. Communicatiemedewerkers (informeren betrokkenen)

Er wordt periodiek (minstens een keer per jaar) gecontroleerd of deze procedure inclusief de onderstaande beschreven stappen adequaat zijn geïmplementeerd.

Waarom deze procedure?

Beveiligingsincidenten kunnen leiden tot informatie en/of gegevens die verloren gaan of onbedoeld gewijzigd worden. Dit kan gevolgen hebben voor de kwaliteit en continuïteit van het onderwijs.

Daarnaast kunnen vertrouwelijke gegevens door beveiligingsincidenten op straat komen te liggen of in verkeerde handen vallen. Voor de verwerking van persoonsgegevens zijn regels vastgelegd in de Algemene Verordening Gegevensbescherming (AVG). Het niet zorgvuldig omgaan met vertrouwelijke gegevens kan leiden tot boetes en imagoschade.

Als een beveiligingsincident betrekking heeft op persoonsgegevens, moet er mogelijk binnen 72 uur melding worden gemaakt aan de Autoriteit Persoonsgegevens (voorheen College bescherming persoonsgegevens).

Definities

Wat is een beveiligingsincident?

Een beveiligingsincident is een gebeurtenis waarbij gegevens:
1. verloren zijn geraakt
2. gestolen zijn
3. beschadigd zijn
4. onbedoeld gewijzigd zijn
5. onrechtmatig toegankelijk zijn voor derden

Wat is een datalek?

Er is sprake van een datalek als er bij een opgetreden beveiligingsincident persoonsgegevens betrokken zijn.

Wat zijn persoongegevens?

Alle gegevens die (evt. gecombineerd met andere gegevens) tot een persoon herleid kunnen worden.

Voorbeelden persoonsgegevens

- Naam
- BSN
- Pasfoto
- Geboortedatum
- Adres
- IP-adres
- Etc.

Deel A. Medewerkers en leerlingen

Onderstaande teksten zijn opgenomen in de schoolgids en/of intranet van de scholen binnen ons bestuur.

Persoonsgegevens gelekt? Meld ze direct!

Als er sprake is van gestolen computers of opslagmedia, virussen of kwijtgeraakte logingegevens waardoor persoonsgegevens toegankelijk zijn voor anderen, meld dit dan zo snel mogelijk bij de ict-coördinator of schoolleiding van de school.

Op deze manier hopen we op <naam school> veilig en probleemloos met ict te kunnen werken. Klik hier voor meer informatie over hoe wij omgaan met privacy en zorgen voor een veilig schoolklimaat.

Voorbeelden

- computer of software die niet werkt of bruikbaar is
- kwijtgeraakte USB-stick
- gestolen laptop
- inbraak door een hacker
- DDOS aanval
- malware- of virusbesmetting
- gestolen logingegevens
- onbeveiligde serverruimte.

Nog 3 belangrijke tips:

1. Deel je logingegevens nooit met anderen en laat ze niet meekijken.
2. Als je een link in je mail niet vertrouwt, klik er dan niet op.
3. Mocht je computer besmet zijn met een virus, sluit de computer dan zo snel mogelijk af en verbreek de internet- of netwerkverbinding, om besmetting te voorkomen.

Deel B. Ict-coördinator of schoolleider

Stap 1 - Analyseer en beoordeel (binnen 8 uur na melding)

Heeft de melding betrekking op persoonsgegevens?
Meld dit direct via fg@iederkindtelt.nl bij de functionaris gegevensbescherming binnen ons bestuur.

Wat is een datalek?
Er is sprake van een datalek als er bij een opgetreden beveiligingsincident Persoonsgegevens betrokken zijn.

Is er sprake van opzettelijk misbruik of strafbare feiten, zoals diefstal, hacken of DDOS?
Neem (ook) contact op met de schooldirecteur in verband met te nemen sancties en/of het doen van aangifte.

Stap 2 - Inventariseer en registreer

Indien er een melding wordt gedaan van een beveiligingsincident, dan worden de volgende gegevens geregistreerd:

Naam:
Datum:
Tijdstip:
Omschrijving incident:
Soort gegevens:
Omvang gegevens: (aantal personen)
Betrokkenen:
Locatie:
Type hardware (tagcode):
Naam software:

Prioriteit: (indien datalek: hoog)
Back-up aanwezig?: ja/nee
Zijn de gegevens geëncrypt?: ja/nee

Stap 3 – Neem herstelmaatregelen

Is er sprake van diefstal, verlies of beschadiging?
Dan moet het systeem vervangen worden en/of de back-up teruggeplaatst worden (indien aanwezig). Neem hiervoor contact op met de ict-leverancier van de school.

Is er sprake van onrechtmatige toegang?
Dan dient de toegang afgesloten te worden door fysieke beveiliging, een wijziging in de configuratie van het netwerk of in de accounts van computers, netwerkapparatuur of

applicaties, zoals wachtwoorden. Pas dit zelf aan de software of neem hiervoor contact op met de ict-leverancier van de school.

Is er sprake van DDOS aanval op servers die in beheer zijn van de school?
Dan dient relevante netwerk apparatuur afgesloten of opnieuw geconfigureerd te worden, eventueel in overleg met leveranciers of externe beheerders. Neem hiervoor contact op met de ict-leverancier van de school of de leverancier van het betreffende softwarepakket.

Is er sprake van malware of antivirus aanvallen?
Dan dient de computer of apparatuur uit het netwerk genomen, opgeschoond en hersteld te worden. Indien nodig dienen back-ups teruggeplaatst te worden. Neem hiervoor contact op met de ict-leverancier van de school.

Stap 4 – Neem preventieve maatregelen en registreer deze bij de melding

De melding kan pas afgesloten worden als de herstelmaatregelen zijn uitgevoerd en er preventieve maatregelen zijn genomen en beschreven om het risico op toekomstige incidenten te vermijden of te verkleinen.

De herstelmaatregelen en preventieve maatregelen worden geregistreerd bij de melding.

N.B. De registratie van meldingen wordt meegenomen in de periodieke evaluatie van het privacybeleid van ons bestuur. In de evaluatie wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

Deel C. Privacyfunctionaris

Dit onderdeel is opgenomen in het procedurehandboek van de bovenschoolse Privacyfunctionaris. Dit betreft een rol die op bovenschools niveau is belegd en belast is met onder andere de volgende taken en verantwoordelijkheden:

- (Laten) uitvoeren risicoanalyses
- (Laten) opstellen / bijwerken beleidsplan
- (Laten) opstellen, evalueren en controleren jaarplan
- Rapporteren (relevante) incidenten en datalekken aan directeur/bestuurder

Stap 1 - Controleer en registreer

Controleer of al gegevens zijn geregistreerd over het beveiligingsincident. Vul deze registratie aan met de informatie die uit de volgende stappen naar voren komt.

Stap 2 – Bepaal of er sprake is van een datalek (binnen 8 uur na melding)

Zijn er bij het incident persoonsgegevens verloren gegaan?
Er is geen kopie of back-up aanwezig van de persoonsgegevens

Is er bij het incident sprake van onrechtmatige verwerking van persoonsgegevens? En kan dit niet uitgesloten worden?
Onbevoegden hebben onrechtmatig toegang kunnen krijgen tot de persoonsgegevens

Indien Ja op één van beide → Ga naar stap 3
Indien Nee op beide →Er is geen sprake van een datalek, overleg met systeembeheer over preventieve maatregelen

N.B. Schakel indien nodig een externe deskundige in en informeer de betrokken leverancier(s)! Zie bewerkersovereenkomst voor de afspraken in het kader van datalekken met leveranciers.

Stap 3 – Bepaal of er sprake is van meldplicht

Zijn er persoonsgegevens van gevoelige aard gelekt of leidt de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

Indien Ja → Ga naar stap 4
Indien Nee → Er is geen sprake van meldplicht, overleg met systeembeheer over preventieve maatregelen

Gegevens van gevoelige aard:
Godsdienst of levensovertuiging, ras, politieke gezindheid, ras, gezondheid, seksuele leven, lidmaatschap vakvereniging, strafrechtelijke gegevens of over onrechtmatig of hinderlijk gedrag, financiële gegevens of over de economische situatie, gegevens die kunnen leiden tot

stigmatisering (schoolprestaties, relatieproblemen), gebruikersnamen en wachtwoorden, gegevens die kunnen worden gebruikt bij identiteitsfraude (BSN)

Nadelige gevolgen:
Misbruik in het criminele circuit van grote databestanden, ingrijpende beslissingen die op basis van (gewijzigde) gegevens worden genomen, gevolgen die binnen ketens van gegevensverwerking kunnen optreden.

Stap 4 – Informeer het college van bestuur en bepaal of betrokkenen ook geïnformeerd dienen te worden.

Ontbreken er technische beschermingsmaatregelen waardoor het datalek (waarschijnlijk) nadelige gevolgen kan hebben voor leerlingen, ouders of personeel?
De gegevens zijn niet voorzien van encryptie of de encryptie is verouderd.

Indien Ja → Ga naar de volgende vraag
Indien Nee → Ga naar stap 5 en informeer het college van bestuur

Zijn er zwaarwegende redenen om de melding aan leerlingen, ouders of personeel achterwege te laten?
Het informeren van de leerlingen, ouders of personeel kan negatieve gevolgen hebben voor de veiligheid van anderen.

Indien Ja → Ga naar stap 5 en informeer het college van bestuur
Indien Nee → Ga naar stap 5 en informeer het college van bestuur en de communicatiemedewerker (zie deel D procedure Melden beveiligingsincidenten en datalekken)

Stap 5 – Meld het datalek bij de Autoriteit (binnen 72 uur na melding)

Verzamel alle benodigde informatie (zie bijlage A voor vragenlijst)

Na toestemming van het college van bestuur wordt door de Privacyfunctionaris een melding gedaan via http://datalekken.autoriteitpersoonsgegevens.nl of (indien de website niet beschikbaar is) via telefoonnummer 088 - 180 52 55.

De melding wordt minimaal 3 jaar bewaard. Informeer indien nodig de leverancier over de melding.

Deel D. Communicatiemedewerker (niet van toepassing)

Dit onderdeel is opgenomen in het procedurehandboek van de communicatiemedewerker.

Informeer de betrokkenen (binnen 1 week na melding) via de daarvoor vastgestelde communicatiemiddelen indien er sprake is van een datalek

De communicatiemedewerker wordt van een datalek op de hoogte gesteld door de Privacyfunctionaris. Deze verstrekt ook de benodigde gegevens ten behoeve van de communicatie.

In de kennisgeving aan de betrokkene wordt in ieder geval vermeldt:
Een algemene omschrijving van de aard van het incident, de contactgegevens om meer informatie over de inbreuk te verkrijgen, en de maatregelen die genomen zijn en/of door betrokkene genomen moeten worden om negatieve gevolgen te beperken.

Bij grootschalige datalekken dient er ook een persbericht in overleg met het college van bestuur opgesteld te worden.

G. Model Gebruikersovereenkomst

De werkgever : <naam>

En de werknemer:
< Naam >
< Geboortedatum >
< Adres >

Verklaren dat zij een gebruikersovereenkomst mobiele telefonie, laptop5
voor onbepaalde duur zijn aangegaan, in aanmerking nemende dat:

- werkgever aan werknemer een mobiele telefoon of laptop (hierna: de apparatuur) heeft verstrekt ten behoeve van de uitoefening van de werkzaamheden van de dienstbetrekking;
- de apparatuur eigendom is van werkgever en in bruikleen wordt gegeven aan werknemer;
- deze overeenkomst de nadere gebruiksvoorwaarden bepaalt waaronder werknemer de apparatuur kan gebruiken.

1. Aard en uitvoering

Het type apparatuur en het abonnement worden door werkgever vastgesteld en aangeschaft.

2. Rechten en plichten van werknemer

a) Werknemer verklaart de apparatuur in goede staat te hebben ontvangen en zal deze niet aan derden ter beschikking stellen, verpanden noch op enige andere wijze vervreemden.
b) Werknemer is verantwoordelijk voor het in goede en representatieve staat houden van de apparatuur.
c) Het is werknemer verboden de apparatuur te gebruiken voor activiteiten die in strijd zijn met de bedrijfsdoelstellingen of het imago van werkgever kunnen schaden.

3. Gebruik van de apparatuur door werknemer

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

4. Gebruik van de apparatuur in de auto

Het is werknemer verboden te telefoneren in de auto zonder gebruikmaking van een carkit dan wel een handsfreeset. Niet handsfree bellen zal onder alle omstandigheden worden aangemerkt als bewust roekeloos handelen. Werkgever zal geen aansprakelijkheid aanvaarden voor zaak- of letselschade als gevolg hiervan, tevens zijn boeten voor rekening van werknemer.

5. Termijn van gebruik, beëindiging dienstverband en functieverandering

Werknemer dient de apparatuur binnen de afgesproken bruikleentermijn dan wel bij beëindiging van het dienstverband of functieverandering op eerste verzoek in volledige staat te retourneren. Bij verzuim hiertoe, verbindt werknemer zich tot betaling van de rest(boek) waarde van de apparatuur aan werkgever.

6. Diefstal en beschadiging

a) Werknemer dient alle zorgvuldigheid in acht te nemen ter voorkoming van beschadiging, diefstal of verlies van de apparatuur.
b) In geval van schade of diefstal van de apparatuur is werknemer verplicht dit zo spoedig mogelijk, doch uiterlijk binnen 24 uur bij werkgever te melden. Werknemer dient verder het gebruik onmiddellijk te laten blokkeren via de klantenservice van de provider of de interne contactpersoon. Als contractant draagt werkgever het risico voor misbruik na diefstal, mits aan het hiervoor gestelde is voldaan.
c) Werknemer kan aansprakelijk worden gesteld voor schade aan de apparatuur ontstaan door verwijtbare nalatigheid of onachtzaamheid.

7. Bewustzijn

a) Werknemer is op de hoogte dat werkgever informatie omtrent het gebruik van de mobiele telefoon kan aanleveren aan de werkgever.
b) Werknemer verklaart zich akkoord dat, indien gehandeld in strijd met de bepalingen van deze gebruikersovereenkomst mobiele telefonie, de naheffingsaanslagen loonheffing en een bedrag ter grootte van de correctie nota's werknemersverzekeringen inclusief eventuele boetes en rente die als gevolg van dit handelen worden opgelegd aan werkgever, zullen worden verhaald op werknemer.
c) Door ondertekening van deze overeenkomst verklaart werknemer dat hij gevolgen van deze overeenkomst en het onderliggende beleid mobiele telefonie heeft begrepen en zich daarmee akkoord verklaart.

Aldus overeengekomen en getekend te <plaats>, <datum>.

<naam werkgever>
Namens deze:

<ondertekening werknemer> <ondertekening werkgever>

H. ICT en social media leerlingen

A. Internet en e-mail

We vinden het van groot belang dat je als leerling zo veilig mogelijk online kan werken. Om hiervoor te zorgen, zijn de volgende gedragsregels van belang:

1. Ik gebruik het internet om informatie te zoeken over een onderwerp of werkstuk voor school. Ik gebruik een internetbrowser die de leerkracht aanreikt.
2. Ik vraag toestemming van mijn leerkracht als ik…
    a. een online game wil spelen
    b. persoonlijke gegevens (naam, adres en je telefoonnummer) moet invullen op een website
    c. bestanden wil downloaden of delen
    d. een e-mail wil versturen
3. Ik deel geen wachtwoorden met anderen.
4. Ik ga voorzichtig om met mails die ik niet vertrouw of waarvan ik de afzender niet ken. Bij twijfel klik ik geen linkjes aan.
5. Ik vertel direct aan mijn meester of juf als ik informatie tegenkom die ik niet prettig vind of waarvan ik weet dat dat niet hoort.
6. Ik weet bij welke instanties/personen ik op school en buiten school terecht kan als ik iets onprettigs heb meegemaakt op het internet waarbij ik me niet veilig voel.
7. Ik bekijk informatie op internet kritisch.
8. Ik ken de gevolgen van het delen van informatie die niet echt is.

B. Sociale media

Binnen de school maken de leerlingen geen gebruik van Social Media.
Buiten de school gelden de volgende gedragsregels om te zorgen dat de mogelijkheden van sociale media worden gebruikt zonder andere personen of de school te schaden:

9. Ik plaats geen foto’s of verhalen over een ander (leerling, juf of meester, school, ouders of anderen van buiten de school) op sociale media als een ander dit niet goed vindt.
10. Ik plaats geen kwetsende foto’s, verhalen of opmerkingen op sociale media. Ook gebruik ik geen grove taal.
11. Ik doe niet mee aan pesten via de Whats app. Als ik nare berichten ontvang van iemand, dan vertel ik dit thuis. In overleg met je ouder(s) kun je het ook op school melden bij je leerkracht.
12. Als ik iemand niet begrijp via Whats app of andere berichten, dan vraag ik rechtstreeks aan diegene.
13. Ik ga zorgvuldig om met mijn eigen identiteit. Ik besef dat ik altijd terug te vinden ben op internet.

C. ICT-apparatuur

De ICT-apparatuur op school (chromebook, 3d-printer, digibord, etc.) is kostbaar, daarom dien je hier voorzichtig mee om te gaan. De volgende gedragsregels zijn daarom van belang:

14. Ik gebruik alleen ICT-apparatuur en software waar ik toestemming voor heb gekregen van de meester of juf. Dat geldt ook voor meegebracht smartphones, etc.

15. Ik ga voorzichtig om met de dure ICT-apparatuur van de school die ik mag gebruiken.
16. Ik gebruik geen meegebrachte USB-sticks van thuis in ICT-apparatuur van de school.

D. Schermtijd

17. Ik ben me bewust van de wereld buiten de online wereld en de leerkracht en ik houden de tijd in de gaten als ik achter de computer/laptop of tablet zit.

I. Geheimhoudingsovereenkomst *(digitaal) laten ondertekenen door elke werknemer*

Ondergetekende:

Voorletters en achternaam:
Functie binnen Stichting 'Ieder kind telt':

Hierna te noemen: Werknemer

Overwegende:

- dat werknemer een dienstverband in het kader van de cao po heeft met Stichting 'Ieder kind telt' (hierna te noemen het bestuur).
- dat werknemer voor de uitvoering zijn of haar functie de beschikking moet hebben over informatie en/ of persoonsgegevens, door het bestuur verzameld in haar hoedanigheid als verantwoordelijke in de zin van de algemene verordening gegevensbescherming.
- dat het bestuur wil benadrukken dat zij de zorgvuldige omgang met deze gegevens van groot belang vindt en daarom voorwaarden stelt aan het ter beschikking stellen van deze gegevens aan werknemer.
- dat het bestuur tevens moet voldoen aan haar wettelijke verplichting tot het treffen van technische en organisatorische beveiligingsmaatregelen ten aanzien van deze informatie en/ of persoonsgegevens.
- dat deze verklaring gezien kan worden als regels ten behoeve van een goede gang van zaken, zoals bedoeld in artikel 19.2 van de cao po.
- dat werknemer door het ondertekenen van deze verklaring erkent dat het bestuur deze informatie en/of persoonsgegevens als geheim en vertrouwelijk beschouwt en dat werknemer het bestuur schade kan berokkenen door onzorgvuldige omgang met en/ of het onrechtmatig aan derden ter beschikking stellen van deze informatie.

verklaart dat

- de werknemer de informatie en/ of persoonsgegevens alleen zal gebruiken voor de duur van het dienstverband en uitsluitend voor de werkzaamheden binnen de functie van de werknemer.
- de werknemer de informatie en/ of persoonsgegevens niet zonder voorafgaande toestemming van het bestuur verstrekt aan derden.
- de werknemer uiterste zorg besteedt aan een deugdelijke en veilige opslag van de informatie en/of persoonsgegeven, ter voorkoming van verlies en/of enige vorm van onrechtmatige verwerking, en hiertoe de richtlijnen en instructies opvolgt die het bestuur verstrekt en voorschrijft.
- het voorgaande geldt ook voor door of namens het bestuur verstrekte toegang aan werknemer tot ict-systemen en/of ter beschikking gestelde apparatuur.
- de werknemer zich verplicht alle door of namens het bestuur verstrekte informatie en/of persoonsgegevens te retourneren aan het bestuur, zodra daarom verzocht wordt. de werknemer zal geen kopieën van de informatie bewaren.

- de werknemer erkent dat het bestuur te allen tijde rechthebbende en eigenaar blijft van de verstrekte informatie en/of persoonsgegevens.
- de afspraken in deze verklaring ook na beëindiging van het dienstverband geldig blijven.

ondertekening:

plaats:
datum:
naam:
handtekening:

J. Verwerkersovereenkomsten

Leveranciers waarvoor een verwerkersovereenkomst is afgesloten:

☐Actacom
☐Aerobe / RedOrBlue B.V.
☐Aimfor
☐Alles-in-1
☐AMN
☐Ars Scribendi Uitgeverij B.V.
☐Bareka Online Rekentoetsen
☐Basisacademie B.V.
☐BasisOnline
☐Basisschool-apps
☐Bazalt Educatieve Uitgaven
☐BeatsNbits
☐bettermarks NL
☐Blink
☐BLOON
☐Boekgeheim
☐BOLAS
☐Bomberbot
☐Boom uitgevers / Uitgeverij Edu'Actief
☐Boom uitgevers Amsterdam
☐Bordfolio
☐Bosos
☐Brightcenter
☐Briter
☐Brite Wireless Expertise Buro
☐BruutTAAL
☐Bureau Educatief PeuterPlusPlan
☐Bureau ICE
☐CED-Groep
☐Cito
☐ChildPoint
☐Cloudwise B.V.
☐Codename Future
☐Cupella
☐Dageraad
☐DataCare BV
☐Dedact
☐Delta Apps
☐Delubas Educatieve Uitgeverij
☐De Digitale Topschool
☐De Rolf groep
☐De Stoeltjesdans
☐Diataal B.V.
☐DigiDUIF
☐Dotcomschool
☐Driestar Educatief
☐Digikeuzebord
☐Drie-O Automatisering BV
☐Drillster B.V.
☐D. van Dongen advies
☐Educus
☐EduHint B.V.
☐Eisma Edumedia
☐Elerna
☐EURObizz Academy
☐EXOVA
☐Focus Onderwijs B.V.
☐Get There MijnSchool
☐Groot's Onderwijsadvies
☐Gynzy
☐HetSchoolvoorbeeld.nl
☐Heutink ICT
☐Heutink Primair Onderwijs BV
☐Iddink Voortgezet Onderwijs bv
☐iDEALnet
☐IDFocus BV
☐Instruct
☐Intertaal
☐IntraQuest
☐Inzichtelijk Onderwijs
☐IRRUS
☐ISO Groep Automatisering B.V.
☐Isy School B.V.
☐Italko
☐itslearning Nederland
☐Jongbloed Educatief
☐Jimmy Company B.V.
☐Junior Einstein BV
☐Kennisnet

☐KIC
☐Koninklijke Van Gorcum
☐Kwintessens
☐Kwizl
☐LC-Data
☐LearningStone
☐Leerpodium
☐Leeruniek
☐LesLab Coöperatie U.A.
☐LessonUp
☐Liquid Development C.V.
☐Lvscv.nl
☐LWEO
☐Maandtaak (AP-taalproductie)
☐Magnaview
☐Malmberg
☐MaxClass
☐Mijnschoolinfo
☐MIEGROEP Automatisering
☐Muiswerk Educatief
☐Nederlandse Kleurenschool
☐Nils &Paul
☐nnine
☐Noordhoff Uitgevers
☐Oefenweb.nl
☐Onderwijs Transparant BV
☐Onlineklas
☐Onderwijspraktijk Harry Janssens
☐Ontwikkelcentrum
☐OpenEdu
☐OsingadeJong educatieve diensten
☐OVD Educatieve Uitgeverij B.V.
☐ParnasSys
☐Pearson
☐Peppels B.V.
☐Peuter-Kleuterpraktijk Ellen Voogt
☐Presentis B.V.
☐Projects4Learning
☐Prowise B.V.
☐Qompas
☐Quarantainenet
☐Raet
☐Ratho B.V.
☐RealOpen IT
☐ReadSpeaker B.V.
☐Reinders Oisterwijk BV
☐Rovict B.V.
☐RTTI-online B.V.
☐Safe School
☐Scholen met Succes
☐Schoolpoort B.V.
☐Schoolmaster BV
☐Schoolplanner
☐SchouderCom
☐Skool
☐SLB Diensten B.V.
☐Slim
☐Slimleren.nl
☐Smart2Scool
☐SnapIT
☐Snappet
☐SOMtoday b.v.
☐SPEYK
☐Stichting Basispoort
☐Studyflow
☐Summario
☐SWIS Suite, Praktikon
☐Switch IT Solutions bv, Studywise
☐Teachers Channel
☐The Implementation Group (TIG)
☐Thiememeulenhoff
☐Topicus
☐TripleWict
☐Tumult
☐Uitgever Essener
☐Uitgever Zwijsen
☐Uitgeverij Betelgeuze
☐Uitgeverij Deviant b.v.
☐Uitgeverij Malmberg BV
☐Uitgeverij Stoffels BV
☐Unilogic BV
☐VanBuurtICT
☐Van Dijk Educatie bv
☐Van Dijk Educatie, Digitaal Leren
☐Van Tricht uitgeverij
☐Veilig Verkeer Nederland

☐Visiria Uitgeversmaatschappij
☐VO-digitaal
☐VO-content
☐Volution, DataByte BV
☐VSA Vogels Software en Advies
☐VWC
☐Vitasys B.V.
☐Web2work B.V.
☐WIS Services BV
☐WizeNoze B.V.
☐Woordhelder
☐Yubu B.V.
☐Zermelo Software B.V.
☐ZuluBook
☐ZuluDesk
☐Zwijssen
☐…
☐…
☐…

Colofon

Auteurs: Tonny Plas en O21, Gouda 2018
tonnyplas.nl
o21.nu