Handboek

Informatiebeveiliging en privacy

Versie	1.0
Goedgekeurd directieoverleg	
Goedgekeurd GMR	
Goedgekeurd RvT	
Goedgekeurd CvB	
Bestand	
Bestand datum laatst opgeslagen	20-9-2019 16:20:00

Inhoudsopgave

Inhoud

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.

In dit 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 die voorschrijft, maar ook op basis van de normen en waarden die wij vanuit onze visie op onderwijs met elkaar delen en uitdragen.

Het handboek is onderverdeeld in twee delen voor afzonderlijke doelgroepen:

Deel A - Alle medewerkers
Dit deel bevat de algemene informatie die voor alle medewerkers van Wonderwijs 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. In dit deel wordt o.a. antwoord gegeven op de volgende 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?
- Waar moet ik op letten bij het uitwisselen van gegevens met andere partijen?
- 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?

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 op mijn school goed geregeld is? In dit deel wordt o.a. antwoord gegeven op de volgende 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 afspreken met medewerkers in het kader van geheimhouding?
- Wat moet ik weten over datalekken?
- Wat moet ik weten over cameratoezicht?
- 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?

Deel A

Infomatie voor alle medewerkers

Deel A – Infomatie voor alle medewerkers

Gedragsregels privacy

Privacy op school gaat over de bescherming van gegevens van personen. Dit wordt geregeld in de Algemene Verordening Gegevensbescherming (voorheen de Wet Bescherming Persoonsgegevens).

Binnen Wonderwijs 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, zie bijlage A.

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

De afspraken zijn verdeeld in twee onderdelen:

A. Waar en hoe verwerk ik persoonsgegevens?
B. 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 verwerk ik persoonsgegevens?

1. **Privacywetgeving**
   Ken de belangrijkste begrippen en uitgangspunten van privacy en de wet. Wij gebruiken hiervoor de 5 vuistregels voor privacy van Kennisnet. Om persoonsgegevens te mogen verwerken (verzamelen, uitwisselen, etc.) kent de AVG een aantal uitgangspunten. Deze voorwaarden gelden voor elke school en zijn samengevat tot 5 vuistregels:

   a. *Doel en doelbinding*
      Persoonsgegevens worden altijd verzameld met een vooraf vastgesteld en concreet doel. Zoals: onderwijs geven en begeleiden, leerlingen, voldoen aan de wet. Persoonsgegevens mogen alleen worden verwerkt om het vooraf vastgestelde doel te bereiken. Bijvoorbeeld: Een telefoonnummer voor noodgevallen.

   b. *Grondslag*
      Persoonsgegevens mogen alleen verwerkt worden als de AVG hier een grond voor noemt. 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.

c. *Dataminimalisatie*
De persoonsgegevens die de school verwerkt, moeten redelijkerwijs nodig zijn om het doel te bereiken. De gegevens moeten in verhouding staan tot het doel en het doel kan niet met minder dan deze verzamelde gegevens worden bereikt. Het gaat er dus om dat scholen uitsluitend gegevens verzamelen die écht nodig zijn om het doel te bereiken.

d. *Transparantie en rechten van de betrokkene*
De betrokkene (dus: degene van wie de persoonsgegevens worden verwerkt) is vooraf in begrijpelijke taal geïnformeerd over wat er precies aan informatie wordt verwerkt en wat het doel daarvan is. De betrokkenen moeten op de hoogte worden gesteld van hun rechten als het gaat om de verwerking van persoonsgegevens door de school/de stichting.

e. *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?

2. Uitwisselen gegevens
Als je gegevens uitwisselt, houd dan rekening met bovenstaande punten. Kijk hier voor een overzicht van partijen met wie je gegevens mag uitwisselen en de wijze waarop dat moet gebeuren. In bepaalde gevallen heb je ook toestemming nodig. Verstuur persoonsgegevens bij voorkeur niet als bijlage per mail, verstuur in plaats hiervan een link met de online bewaarplaats van de benodigde gegevens. Wonderwijs heeft met verschillende partijen verwerkersovereenkomsten afgesloten. Deze lijst vind je hier terug.

3. Bewaren van persoonsgegevens
Persoonsgegevens worden opgeslagen op de daarvoor aangewezen plaatsen. Leerlinggegevens worden alleen in het leerlingadministratiestysteem, op het schoolnetwerk of op de door de school gefaciliteerde Cloud omgeving opgeslagen. Er worden geen persoonsgegevens op USB-sticks bewaard. Bekijk voor meer info hierover het onderdeel Document- en datamanagement.

4. **Rechten ouders**
   Ouders hebben rechten als het gaat om de privacy van hun kind. Denk aan recht op inzage, correctie of verwijdering van de persoonsgegevens. Formuleer gegevens over een persoon met zorgvuldigheid.

5. **Publiceren beeldmateriaal**
   Foto's, video's of persoonlijke informatie van en over leerlingen (en ouders) publiekelijk delen? Zorg altijd dat je schriftelijke toestemming hebt van de ouders. Lees verderop in dit handboek (bijlage D) hoe dit wordt geregeld. Bij inschrijving van de nieuwe leerling wordt standaard om deze toestemming gevraagd en vervolgens wordt aan het begin van ieder schooljaar in de nieuwsbrief gecommuniceerd dat men zijn of haar keuze te allen tijde mag wijzigen. De schooldirecteur verzekert zich ervan dat de leerkracht weet welke leerlingen wel en niet op foto's mogen staan. De leerkrachten dienen dit te weten.

6. **Beveiligingseisen computer**
   Het downloaden en bewerken van persoonsgegevens wordt alleen gedaan op computers van school.

B. Hoe houd ik "indringers" op afstand?

7. **Account en wachtwoord**
   Je wachtwoord en account zijn privé en worden niet gedeeld met anderen. Dit betekent:
   a. Als je weggaat bij je computer vergrendel je je computer (Windowstoets + L)
   b. Laat anderen nooit onder je account werken en houd je logingegevens altijd voor jezelf, ook al vragen anderen aan je om ze te delen.
   c. Schrijf je wachtwoord nooit op, maar gebruik een wachtwoordkluis. Lees hieronder meer info over wachtwoordkluizen.

8. **Mobiele devices**
   Bewaar laptops of tablets altijd op een veilige en afgesloten 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. Op school worden mobiele devices in een afgesloten ruimte in de laptopkar opgeborgen.

9. **Phisingmail**
   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 (ransomeware). Mocht je vermoeden dat je slachtoffer bent geworden van phishing activiteiten, meld dit bij je leidinggevende.

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

11. **Zorgvuldigheid gevoelige informatie**
    Meld je altijd af als je de computer onbeheerd achterlaat en zorg ervoor dat onder andere op de werkplek of bij de printer geen gevoelige informatie zichtbaar of voor het grijpen ligt. Met de combinatie van de Windows- en L-toets kun je jouw account makkelijk vergrendelen. 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.

12. **Bewaren devices**
    Bewaar het apparaat dat je van school in bruikleen krijgt/hebt gekregen altijd op een veilige, afgesloten plek, zeker tijdens vakantieperiodes.

13. **Afschermen wachtwoorden**
    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.

14. **Gebruik wachtwoordkluisjes**
    Laat je wachtwoorden van digitale (administratie)systemen met persoonsgegevens niet onthouden door je internetbrowser en schrijf je logingegevens nooit op.
    Maak bijvoorbeeld gebruik van wachtwoordkluisjes, zoals LastPass of True Key. 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.

Gebruik sociale media

Sociale media kunnen een waardevolle toevoeging zijn op de manier waarop wij met collega's, ouders, leerlingen en anderen communiceren. Zo bieden ze talrijke mogelijkheden tot interactie zoals het ouderportaal, posts, blogs en fora.
Wonderwijs is zich ervan bewust dat veel collega's, zowel privé als zakelijk, participeren in sociale media. Het is daarom belangrijk dat de invloed van sociale media niet wordt onderschat en op een verantwoorde wijze wordt gebruikt. Want alles wat online wordt gezegd – of het nu in woorden of met beelden is – kan Wonderwijs beïnvloeden.

1. **Identificeer jezelf**
   Een belangrijk principe is openheid en eerlijkheid. Als je online schrijft over Wonderwijs, gebruik dan je echte naam, vermeld voor wie je werkt en wat je functie is.

2. **Neem de bestaande richtlijnen in acht**
   Zorg ervoor dat jou online activiteiten niet botsen met de regels van Wonderwijs op het gebied van gedrag, privacy, vertrouwelijkheid en de richtlijnen voor pers en publiciteit. Het is voor medewerkers van Wonderwijs niet toegestaan standpunten en/of overtuigingen uit te dragen die in strijd zijn met de missie en visie van de organisatie en/of school. Als je uit naam van Wonderwijs sociale media gebruikt volg dan de huisstijl, zoals het logo.

3. **Zet je expertise in**
   Zorg ervoor dat je deskundig bent in de onderwerpen waarover je schrijft. Zeker als het te maken heeft met Wonderwijs en de dienstverlening. Baseer je op objectieve en controleerbare feiten.

4. **Neem verantwoordelijkheid**
   Elke medewerker is persoonlijk verantwoordelijk voor zijn of haar onlinegedrag en de content die hij of zij op internet plaatst. Doe dit op een verantwoorde wijze. Schrijf niet negatief over anderen. Als je verwijst naar relevante partijen, plaats dan waar mogelijk een link naar hun website. Indien je over gevoelige of omstreden onderwerpen schrijft, zorg dan dat je hiervoor van tevoren toestemming hebt.

5. **Wees kritisch**
   Wonderwijs beschouwt het niet als zijn taak om alle online bijdragen van medewerkers te controleren. Het is dan ook belangrijk dat je zelfkritisch nadenkt over de mogelijke impact die een online bijdrage kan hebben, niet alleen op jezelf, maar ook op Wonderwijs. Deel alleen kennis en informatie over de organisatie en/of school als het geen vertrouwelijke of persoonlijke informatie betreft en andere betrokkenen en de naam van de organisatie en/of school niet schaadt. Wel worden online publicaties over Wonderwijs gemonitord. Mochten we daarbij een ongeoorloofde publicatie tegenkomen, dan kan je leidinggevende je verzoeken de publicatie van internet te verwijderen of aan te passen. Als het niet mogelijk is een vermelding te plaatsen, dan distantieert Wonderwijs zich van de publicatie.

6. **Gebruik bronvermelding**
   Zorg altijd voor een duidelijke bronvermelding wanneer je naar andere publicaties en/of onderzoeken verwijst. Respecteer auteurs- en portretrechten, trademarks en copyrights op muziek, video, tekst en foto's e.d.

7. **Alleen op persoonlijke titel**
   Uitspraken van medewerkers op internet kunnen misbruikt of onjuist geïnterpreteerd worden. Communiceer dan ook uitsluitend op persoonlijke titel en niet als woordvoerder van Wonderwijs tenzij je hiervoor toestemming hebt.

8. **Geen perscontact zonder overleg**
   Er is een mogelijkheid dat je via sociale netwerken in contact komt met journalisten. Voor online mediacontacten gelden dezelfde regels als voor offline perscontacten. Raadpleeg altijd je leidinggevende voor communicatie over Wonderwijs.

9. **Communiceer respectvol**
   Online discussies maken soms emoties los. Blijf altijd fatsoenlijk, professioneel en respecteer andermans mening, cultuur, normen en waarden. Waak voor taalgebruik dat als beledigend of kwetsend kan worden ervaren. Wees voorzichtig met het aangaan van discussies.

10. **Vergeet niet: Google onthoudt alles**
    Alles wat je online publiceert blijft lang bestaan. Houd dit in gedachten voordat je iets op internet plaatst.

11. **Bij twijfel neem contact op**
    Als je twijfels hebt over een post, commentaar of reactie op het internet neem dan contact op met je leidinggevende. Indien nodig, corrigeer snel.

12. **Deel geen informatie over personen**
    Doe dit, in plaats van via social media, vooral in persoon of desnoods via de telefoon. Wat je communiceert via social media kan gemakkelijk anders worden geïnterpreteerd door de lezer als je hier niet alert op bent.

    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 I is een voorbeeld opgenomen van dergelijke afspraken. Van iedere school wordt verwacht dat ze een dergelijk protocol hebben en toepassen.

Privacyreglement

Het privacyreglement maakt duidelijk (transparant) aan de personen van wie gegevens worden verzameld (ook wel betrokkenen genoemd), waarvoor de verzamelde gegevens nodig zijn en welke gegevens dit zijn (doel en doelbinding uit de vuistregels).

Ook is hierin te lezen wie binnen de school 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.wonderwijs.nl/privacy . Het reglement is ook als bijlage A toegevoegd bij dit handboek.

Ouders worden via het inschrijfformulier, de schoolgids en via de website van de scholen gewezen op het privacyreglement, waarvan de laatste versie altijd op www.wonderwijs.nl/privacy staat.

Toestemming beeldmateriaal en online diensten

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.

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

- Ouders in algemene zin op het terrein van Wonderwijs 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) Wonderwijs 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 scholen binnen Wonderwijs mogelijk 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 en video-opnamen gemaakt die gebruikt kunnen worden als voorlichtingsmateriaal. Als een leerling hierop te zien is, kunnen deze opnamen alleen met toestemming van de ouder(s)/voogd(en) als zodanig worden gebruikt.

Onlinediensten

Voor het gebruik van onlinediensten 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, 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 gegevens van leerlingen 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 & Basispoort	Nee
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
Samenwerkingsverband	Toelaatbaarheidsverklaring afgeven*	Ja, zie ook: https://passendonderwijsenprivacy.nl	Door Passenderwijs verstrekken van schrijflink	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
Administratiekantoor	Salarisadministratie en HR-management	Ja	Verstrekken account bij Groenendijk	Nee
Leerplicht Gemeente	Controle verzuim	Ja	Verzuimloket	Nee

* Wettelijk verplicht

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? Dan ben je verplicht dit zo snel mogelijk te melden door gebruik te maken van het datalekkenformulier op www.wonderewijs.nl of bij privacy@wonderwijs.nl.

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:
Algemeen

- Inloggegevens (computer, ParnasSys, Google account, BasisPoort) zijn openbaar geworden/verstrekt aan iemand anders
- Een e-mail die aan een verkeerd persoon geadresseerd is
- Een kwijtgeraakte USB-stick
- Een gestolen iPad
- Een gehackte computer
- Kwijtgeraakte documenten

In de klas

- In de pauze, naar gym blijft de computer ingelogd achter, waardoor iemand anders bij gevoelige informatie kan.
- Leerkracht (bovenbouw) verlaat de klas en leerling kan bij informatie.
- Leerkracht typt wachtwoord zichtbaar op digibord

Thuis

- Kind (huisgenoot) werkt op onder hetzelfde account op computer/laptop/tablet/telefoon en kan op deze wijze vertrouwelijke e-mails lezen of in ParnasSys (omdat wachtwoord is opgeslagen).

Beoordelen datalek

Het bevoegd gezag van de school is verantwoordelijk voor de bescherming van persoonsgegevens van leerlingen en personeel en moet in samenspraak met de privacy officer bepalen of er een melding gedaan moet worden bij de Autoriteit Persoonsgegevens. Om dit beoordelen dient het beslismodel in hoofdstuk ‘protocol melden datalekken’ gevolgd te worden.

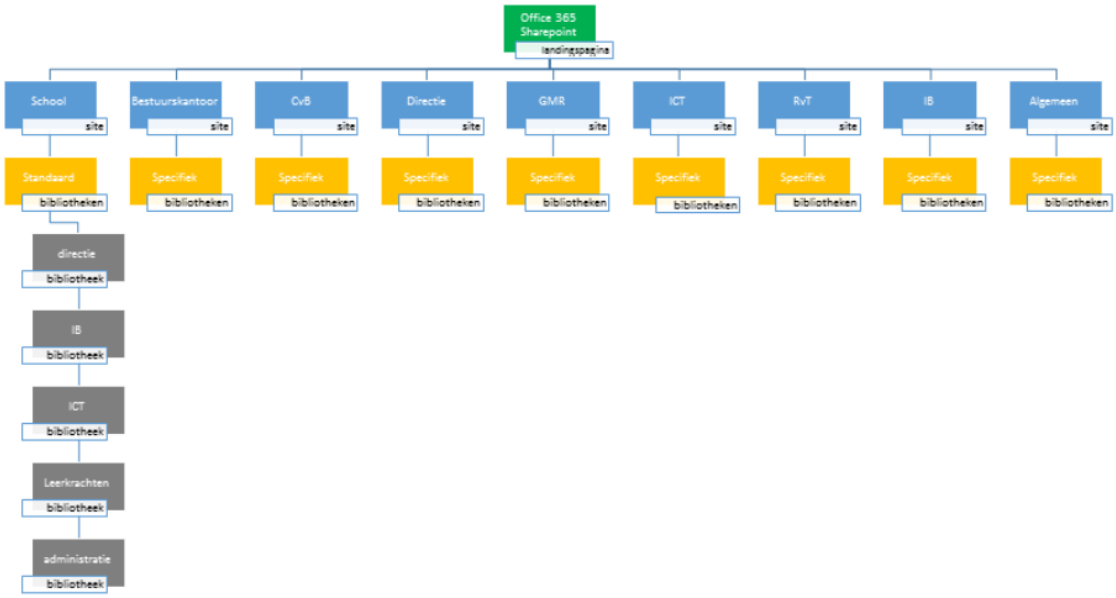
Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

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. Overleg in geval van twijfel met de privacy officer (of functionaris gegevensbescherming) van Wonderwijs via privacy@wonderwijs.nl .

Structuur Sharepoint omgeving Wonderwijs



Deel B

Informatie voor directeuren

Deel B – Informatie voor directeuren

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 van Wonderwijs aan zijn wettelijke informatieplicht, mits deze ook actief wordt aangeboden aan de ouders[1]. 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 van Wonderwijs 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 schoolleiding.

Toestemming

Voor het gebruik van foto- en filmopnames van leerlingen en medewerkers is schriftelijke 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 Wonderwijs 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. Dit betekent ook dat wanneer toestemming wordt ingetrokken, het materiaal van het betreffende medium moet worden verwijderd.

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.

Dit betekent ook dat wanneer toestemming wordt ingetrokken, het materiaal van het betreffende medium moet worden verwijderd.

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

Protocol melden datalekken

Het Protocol informatiebeveiligingsincidenten en datalekken is gebaseerd op het model van Kennisnet.

Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het tijdig melden, oplossen en het voorkomen van beveiligingsincidenten en datalekken in de toekomst.

Gebruikte termen

- Beveiligingsincident: een beveiligingsincident is een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- Datalek: Een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- Betrokkene: De persoon van wie de persoonsgegevens zijn gelekt.

Wet- en regelgeving 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 groep 3, 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.

Rollen en verantwoordelijkheden

Er zijn tenminste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of datalek succesvol af te handelen:

1. **Ontdekker (medewerker)**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt (Formulier op website of via privacy@wonderwijs.nl)**; een aanspreekpunt binnen de school waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder (bovenschool ICT-coördinator)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus (externe ict-dienstverlener)**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

Stappenplan

1. **Ontdekken**
   De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt dit het bij het Meldpunt (formulier op website).

2. **Inventariseren**
   Het Meldpunt bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt daarna vastgelegd:
   - Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
   - Datum/periode van het beveiligingsincident
   - Aard van het beveiligingsincident
   - Wanneer van toepassing (bij een datalek):
     - Omschrijving van de groep betrokkenen
     - Aantal betrokkenen
     - Type persoonsgegevens in kwestie
     - Worden de gegevens binnen een keten gedeeld

3. **Beoordelen**
   Wanneer het Meldpunt voldoende informatie heeft verzameld, en een datalek vermoedt, stuurt deze de Melder een verzoek om de verzamelde informatie te

bekijken. De Melder beoordeelt in overleg met de bestuurder de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.

Classificatieniveaus
Hieronder een uitwerking van classificatieniveaus.

Classificatieniveau	Vertrouwelijkheid
"Geen"	Openbaar
"Laag"	Bedrijfsvertrouwelijk
"Midden"	Vertrouwelijk
"Hoog"	Geheim

- GEEN
  - Schoolgids
  - Nieuwsbrief
  - Website
- LAAG
  - Algemene vergaderstukken
  - Werkbladen van methoden
  - Algemeen leerlingwerk (werkstukken, schriftelijk werk)
- MIDDEN
  - Toetsen, beoordeeld werk
  - Registratiebladen
  - Toetsgegevens en periodieke rapporten van kinderen
- HOOG
  - Dossiergegevens van personeelsleden
  - Verslagen van functionerings- en beoordelingsgesprekken
  - Dossiergegevens van kinderen:
  - Onderzoeksverslagen van kinderen
  - Groeidocumenten
  - Notities, handelingsplannen in ParnasSys
  - Wachtwoorden

De volgende informatie wordt vastgelegd door de Melder:

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- Wordt het datalek aan betrokkenen gemeld? Waarom niet?
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', houd je rekening met het type gegevens, en met de hoeveelheid gegevens. Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, moet er gemeld worden.

Van die ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is bijvoorbeeld sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn maar ook wanneer de gelekte gegevens "gevoelig" zijn zoals bijvoorbeeld bijzondere persoonsgegevens over gezondheid, over de financiële of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene (denk aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).

4. Repareren
   De Technicus wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus van Wonderwijs legt onderstaande vast:
   - Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.
   - Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?

5. Melden
   Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Melder dit binnen twee werkdagen doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken:
   https://datalekken.autoriteitpersoonsgegevens.nl

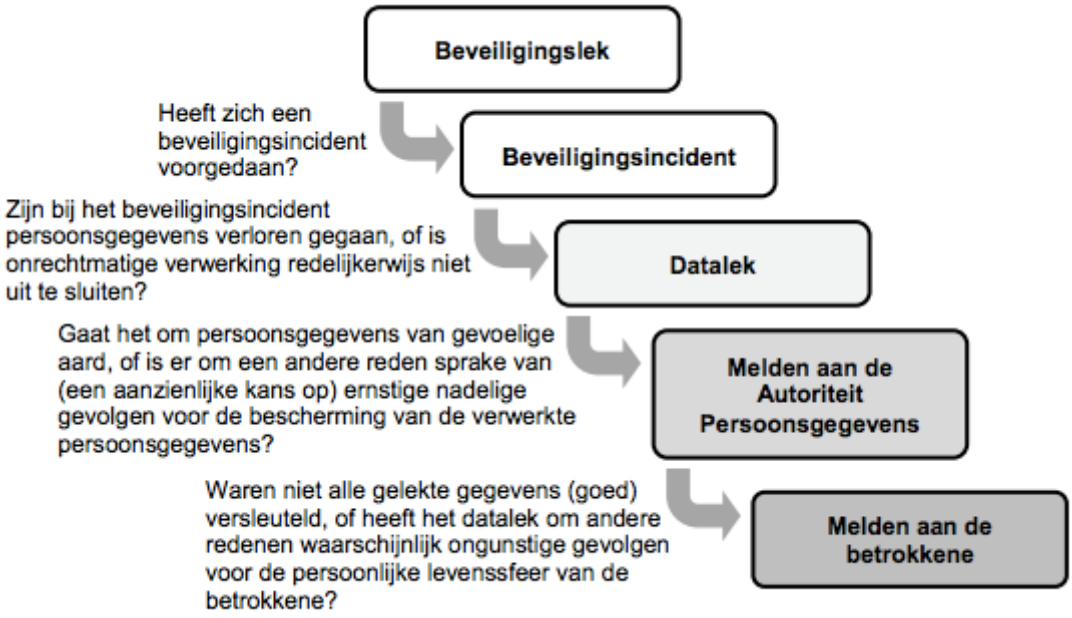
6. Vastleggen
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door het Meldpunt waarmee het incident is afgesloten. Het Meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.

7. Informeren betrokkene: leerling en/of zijn ouders
   Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers en de ouders van leerlingen (aangezien zij jonger zijn dan 16 jaar). In principe kan ervan worden uitgaan dat lekken van gevoelige aard

gemeld moeten worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelekt, maar die zijn beveiligd of versleuteld en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat toch niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

Monitoring beveiligingsincidenten en datalekken.
Alle beveiligingsincidenten en datalekken worden geregistreerd in een overzicht.

Bijgaand beslismodel kan worden gebruikt om te achterhalen of zich een datalek heeft voorgedaan en of dit moet worden gemeld. De privacy officer (of functionaris gegegevensbescherming) overlegt met de bestuurder:



Bron: autoriteitpersoonsgegevens.nl

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

- Gegevens van leerlingen en medewerkers worden opgeslagen in de daarvoor aangewezen bewaarplaatsen (zie onderdeel Document- en datamanagement).
- De afspraken met betrekking tot toegang tot en het verwerken van persoonsgegevens door de verschillende rollen binnen Wonderwijs staan hieronder beschreven in een zogenaamde autorisatiematrix.
- Alle accounts die worden verstrekt dienen te voldoen aan deze autorisatiematrix.

- De locatieleider of directeur van de school is verantwoordelijk voor het verstrekken van de juiste toegang (lees: accounts met de juiste rollen en rechten). De locatieleider of 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.
- Naast het toepassen van de autorisatiematrix worden de volgende beveiligingsmaatregelen toegepast op systemen waarin persoonsgegevens worden gebruikt:
    - Inloggegevens worden via het e-mailadres van Wonderwijs verstrekt aan de medewerker en nooit gedeeld met anderen.
    - Inloggegevens worden periodiek (minstens 1x per jaar) 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 Vechtstreek en Venen. De matrixen gaan dus niet over de gegevens (uit de applicaties) die verstrekt worden aan derden, met uitzondering van ouders en leerlingen.

Autorisatiematrix met betrekking tot Parnassys

Voor de leerlinggegevens én de gegevens van medewerkers in Parnassys wordt gebruik gemaakt van een autorisatiematrix die ontwikkeld is door Parnassys. Deze is gebaseerd op de rollen en de bijhorende rechten.

Deze autorisatiematrix is terug te vinden op het kennisportaal van Parnassys onder de titel ‘Rollen en rechten Parnassys schoolomgeving’. (zie ook dit document).

Autorisatiematrix gegevens medewerkers in Groenendijk en onderliggende applicaties

Voor het verwerken van gegevens in de applicaties die Groenendijk gebruikt worden ook verschillende rollen en rechten gehanteerd. In Groenendijk worden alleen gegevens van medewerkers opgeslagen. Het gaat hier om gegevens omtrent het salaris, het personeelsdossier en het verzuim- en reïntegratiedossier.

In bijgaande autorisatiematrix wordt weergegeven wie toegang heeft tot individuele dossiers en wordt onderscheid gemaakt in de volgende rollen: onderwijzend en onderwijsondersteunend personeel **OP/OOP (betreft alle medewerkers)**, directeur **D**, HRM-adviseur **HRM**, financiën **F**, bestuurssecretariaat **S**, bestuur **CvB**

	Mag ingezien worden door	Mag opgevraagd, toegevoegd en gewijzigd worden door	Mag verwijderd worden door
Management Informatie Onderwijs	**D, F, S, CvB**	-	-
Performance management	**OP/OOP, D, HRM, F, S, CvB**	**D, HRM, F, S, CvB**	**HRM**
Personeelsdossier (salaris)	**OP/OOP, D, HRM, F, CvB**	-	-
Self service medewerkerskaart, Vervangingen, ontslag, ziekte (meldingen), verlof, registratie overig.	**D, HRM, CvB**	**D, HRM, CvB**	**D, HRM, CvB**
Verzuimanager	**D, HRM, CvB**	**D, HRM, CvB Arbodienst**	**D, HRM, CvB, Arbodienst**
Mijn Dossier (eigen salaris)	**OP/OOP, HRM**	**HRM**	

Autorisatiematrix toegang werkplekken
In de Sharepoint worden gegevens met een laag risico opgeslagen die met name betrekking hebben op kunnen uitoefenen van de werkzaamheden die horen bij de functie.

In Sharepoint worden gegevens opgeslagen zoals leerlingenlijsten, toetsregistratie die niet ingevoerd kan worden in ParnasSys en bijvoorbeeld weekoverzichten voor individuele leerlingen.

Bij onderstaande matrix wordt gebruik gemaakt van de onderstaande rollen.

Rollen
College van Bestuur **CvB**, directeur **D**, medewerker bestuurskantoor **BS**, Intern Begeleider **IB**, onderwijzend personeel **OP**, onderwijsondersteunend personeel/ stagiaires **OOP**, ICT-coach/ ICT'er **ICTC**,

	Mag ingezien worden door	Mag opgevraagd, toegevoegd en gewijzigd worden door	Mag verwijderd worden door
Sharepoint			
Domein Sharepoint/Office 365			

Intranet			
Intranet Wonderwijs nieuws	CvB, D, BS, IB, OP, OOP, ICTC	CvB, BS, ICTC	CvB, BS, ICTC
Intranet School nieuws	CvB, D, BS, IB, OP, OOP, ICTC	D	D
Toegang verstrekken werkgroep school op intranet	CvB, D, ICTC	D, ICTC	D, ICTC
Bestuurskantoor			
Toegang en beheer tot domein bestuurskantoor	CvB, BS, ICTC	CvB, BS, ICTC	CvB, BS, ICTC
School(server)			
Toegang tot admin account en beheer Sharepoint schoolniveau	CvB, D, IB, OP, OOP, ICTC	OICT	OICT

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.

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

Gegevens	Bewaartermijn
Gegevens over verzuim en afwezigheid	Maximaal 5 jaar nadat een leerling is uitgeschreven
Gegevens in- en uitschrijving (noodzakelijk voor berekening van bekostiging)	Maximaal 5 jaar nadat een leerling is uitgeschreven
Gegevens die nodig zijn om te berekenen hoeveel bekostiging de school krijgt	Minimaal 7 jaar na afloop van het schooljaar waarop de bekostiging betrekking heeft
Gegevens in het leerlingdossier	Maximaal 2 jaar nadat een leerling is uitgeschreven en 3 jaar als er sprake is van een verwijzing naar het speciaal onderwijs.
Medische gegevens in het leerlingdossier	n.t.b.
Gegevens met betrekking tot bezwaar-, klachten- of gerechtelijke procedure.	Maximaal 5 jaar nadat leerling is uitgeschreven
Camerabeelden t.b.v. toezicht	Maximaal 4 weken, tenzij er een incident is vastgelegd.
Gegevens in personeelsdossier met betrekking tot fiscale bewaarplicht	Maximaal 5 jaar na uitdiensttreding

Overige gegevens in het personeelsdossier	Maximaal 2 jaar na uitdiensttreding
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk door personeel en leerlingen	Maximaal 6 maanden
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.

Afspraken over mobiele devices in bruikleen

De school leent afhankelijk van de functie of aard van de werkzaamheden mobiele device 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 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.

Verwerkersovereenkomsten

In de privacywetgeving is bepaald dat het schoolbestuur als Gegevensverantwoordelijke afspraken moet maken met alle leveranciers van de school die leerlinggegevens 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 2018 een inventarisatie gedaan van de lopende contracten van de scholen binnen Wonderwijs.

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 zelfverantwoordelijk voor het afsluiten van de verwerkers-overeenkomst. Wanneer het een contract met meerdere scholen betreft, dan wordt dit bovenschools geregeld. De school dient in alle gevallen afstemming te zoeken met het bestuurssecretariaat.

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

Rollen en verantwoordelijkheden

Binnen het vaststellen en uitvoeren van het IBP-beleid zijn verschillende rollen en verantwoordelijkheden vastgesteld binnen Wonderwijs.

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

De volgende rollen en verantwoordelijkheden zijn 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	CvB en GMR (instemming)
	Communicatie met ouders	Directeur
Gebruik beeldmateriaal en online diensten	Toestemming vragen aan ouders en registreren	Directeur
Uitwisseling persoonsgegevens	Bepalen met welke partijen persoonsgegevens uitgewisseld mogen worden en op welke wijze.	Directieoverleg
	Toestemming vragen aan ouders en registreren	Directeur
Gedragscode	Vaststellen	CvB en GMR (instemming)
	Bewustwording en toezien op toepassing gedragscode	Directeur
	Toepassen gedragscode	Alle medewerkers
	Vaststellen protocol voor leerlingen	CvB
	Toepassen protocol voor leerlingen	Directeur
Documentbeheer	Toepassen van technische beveiligingsmaatregelen (backup, encryptie, etc.)	ICT-coach
	Vaststellen bewaarplaatsen	Directie
	Vaststellen bewaartermijnen	CvB
	Vernietiging persoonsgegevens conform bewaartermijnen	Directeur en CvB (voor het bestuurskantoor)
Toegangsbeleid	Verstrekken en intrekken accounts conform autorisatiematrixen	Directie en CvB (voor het bestuurskantoor)

	Toepassen technische beveiligingsmaatregelen (o.a. automatisch vernieuwen en sterkte wachtwoord)	ICT-coach
Verwerkersovereenkomsten	Doorgeven nieuwe verwerkers (leveranciers) aan bestuurssecretariaat	Directeur
	Afsluiten verwerkersovereenkomsten voor meerdere scholen	Bestuurssecretariaat
	Afsluiten verwerkersovereenkomsten voor individuele scholen	Directeur
Datalekken	Protocol vaststellen	CvB en GMR (instemming)
	Datalekken doorgeven aan Meldpunt	Medewerkers (Ontdekkers)
	Verzamelen meldingen en benodigde informatie	Privacy officer/FG (Meldpunt) i.o.m. externe ICT-dienstverlener (Technicus)
	Melden en registreren	Privacy officer/FG
	Afweging maken tot melding Autoriteit Persoonsgegevens	FG i.o.m. Bestuurder
	Melding maken bij Autoriteit Persoonsgegevens	Functionaris Gegevensbescherming
Devices in bruikleen	Afsluiten gebruikersovereenkomst voor devices die in bruikleen worden gegeven.	Directeur en CvB (voor bestuurskantoor)
Handboek Privacy	Controle en toezicht op toepassing handboek	CvB

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 Wonderwijs vindt versleuteld plaats.

Netwerkcomponenten

- ☐ De netwerkcomponenten binnen de scholen van Wonderwijs 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 door de directeuren gerapporteerd aan het CvB.

#	Maatregelen met betrekking tot privacy en informatiebeveiliging	Ja*/ Nee	Waaruit blijkt dit?
1	Het privacyreglement wordt door de school jaarlijks onder de aandacht gebracht van ouders en medewerkers.		
2	Voor de publicatie van foto- en filmbeelden en online diensten is door de school vooraf toestemming vastgelegd.		
3	Met alle leveranciers die namens de school persoonsgegevens verwerken is een verwerkersovereenkomst afgesloten.		
4	Voor de uitwisseling van persoonsgegevens met derden, niet zijnde verwerkers, is toestemming vastgelegd.		
5	Het protocol datalekken is bij de medewerkers bekend. Men weet wat er van hen verwacht wordt.		
6	Toegang tot software en systemen met persoonsgegevens op school worden verleend conform de vastgestelde toegangsmatrixen.		
7	De afspraken over de bewaarplaatsen van gegevens en informatie (Document- en datamanagement) worden nageleefd.		
8	Er wordt middels een gedragscode en een protocol voor leerlingen structureel en regelmatig aandacht besteed aan de zorgvuldige verwerking van persoonsgegevens.		
9	Bij uitdiensttreding worden alle accounts ingetrokken en apparatuur ingenomen.		
10	Voor alle door de school uitgegeven apparatuur aan medewerkers zijn gebruikersovereenkomsten afgesloten.		
11	Fysieke ruimtes op school met persoonsgegevens van gevoelige aard (op papier of op server) zijn beveiligd tegen onbevoegde toegang.		
12	Er wordt voldaan aan de checklist beveiliging ICT		

Bijlagen

A. Privacyreglement Wonderwijs

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 Wonderwijs 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 en 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.

1. Privacy van leerlingen en hun ouders

Om deze doelstelling waar te maken is het van belang goed te weten wie deze leerling is, wat zijn of haar talenten en uitdagingen zijn en hoe het onderwijs voor deze leerling het beste kan worden verzorgd. Om hier een beeld van te krijgen worden persoonlijke gegevens van die leerling op school verzameld en bewaard. 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 leerlingdossier.

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 in ParnasSys 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 en de 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:

- Leden van de directie en het MT
- Onderwijzend personeel
- Onderwijsondersteunend personeel (OOP: onderwijsassistenten, administratief, IB, ICT-coördinator, SMW, logopedist, orthopedagoog)

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.
Daarnaast wordt in enkele gevallen een papieren dossier bijgehouden. Dit dossier bevindt zich 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 tot ParnasSys is alleen voorbehouden aan medewerkers die in dienst zijn van Wonderwijs. Met de leverancier van ParnasSys is een zogenaamde verwerkersovereenkomst (conform de modelovereenkomst) 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 leerlingendossier.

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, leden van het ondersteuningsteam (OT), orthopedagoog) op grond van toestemming door de ouders/verzorgers.
- Externe partijen die in opdracht van de school en met toestemming van de ouders ondersteunen bij het bieden van aanvullende zorg voor de leerling.
- Verwerkers in de zin van leveranciers van onderwijsmiddelen die in opdracht van de school zorgen voor toegang en beheer van de digitale systemen die bij de begeleiding en zorg voor leerlingen worden gebruikt en waarmee een verwerkersovereenkomst is afgesloten.
-

- De Inspectie van het Onderwijs op grond van een wettelijke verplichting inzake onderwijskwaliteit.

1.5 Inzage en wijzigen

Wanneer men de persoonsgegevens wil inzien of wijzigen, dan kan men hiervoor een afspraak maken met de directeur of locatieleider van de betreffende school.
Ouders krijgen het dossier niet mee, maar hebben wel recht op een kopie.

1.6 Bewaartermijnen

Wonderwijs hanteert de bewaartermijnen voor leerlingengegevens zoals hieronder aangegeven, tenzij de wet anders voorschrijft.

Document/gegevens	*Verplichte bewaartermijn*	*Vastgelegd in*
Gegevens over verzuim en afwezigheid	Maximaal 5 jaar nadat leerling is uitgeschreven	Bekostigingsbesluit WPO
Gegevens in- en uitschrijving (noodzakelijk voor berekening van bekostiging)	Maximaal 5 jaar nadat leerling is uitgeschreven	Artikel 9 Bekostigingsbesluit WPO
Overige gegevens leerlingendossier, waaronder: • Verwerkingen van persoonsgegevens ter uitvoering van de **Leerplichtwet** • Verwerking van persoonsgegevens voor het verstrekken van de vergoeding van de kosten verbonden aan het leerlingenvervoer • Verwerkingen van beoefenaren van individuele beroepen in de gezondheidszorg	Maximaal 5 jaar nadat leerling is uitgeschreven	Vrijstellingsbesluit WBP
Indien sprake is van een **bezwaar-, klachten- of gerechtelijke procedure**, dienen de persoonsgegevens **uiterlijk vijf jaar** te worden verwijderd nadat de desbetreffende leerling is uitgeschreven.	Maximaal 5 jaar nadat leerling is uitgeschreven	Vrijstellingsbesluit WBP

2. Privacy van medewerkers

Niet alleen van leerlingen worden persoonsgegevens verwerkt binnen Wonderwijs, maar ook van onze medewerkers. Soms zijn dat gegevens die direct samenhangen met de arbeidsverhouding tussen Wonderwijs 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
- Bedrijf medische 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:

- Leden van de directie en het MT (systemen voor organisatie en begeleiding onderwijs en formatieplanning)
- Administratief personeel (systemen voor organisatie en begeleiding onderwijs en formatieplanning)
- HRM-adviseur en medewerker personele administratie,
- Medewerkers salarisadministratie en financiën
- Leidinggevende van de betreffende medewerker
- Beleidsmedewerker financiën en controller
- 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.

Voor de personeels- en salarisadministratie (opm. de psa is belegd bij Groenendijk Onderwijsadministratie) wordt een registratiesysteem gebruikt. De arbodienst stelt de RAET-verzuimmanager ter beschikking. Via de Verzuimmanager worden verzuimgegevens geregistreerd. Ook hiervoor geldt dat er binnen Wonderwijs een toegangsbeleid is opgesteld dat jaarlijks wordt gecontroleerd. Met beide partijen worden ook verwerkersovereenkomsten afgesloten. Toegang tot medische gegevens komt tot stand tussen RAET-verzuimmanager en medische specialisten (Arboarts/arbeidsdeskundige) zonder tussenkomst van Wonderwijs. De Arboarts is de gegevensverantwoordelijke.

2.4 Aan wie worden deze gegevens verstrekt?

De gegevens worden verstrekt aan de volgende externe partijen:

- Bewerkers in de zin van leveranciers van onderwijsmiddelen 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 van Wonderwijs 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 Wonderwijs, te bereiken via telefoonnummer: 0481-350003
Wanneer men de persoonsgegevens wil inzien of wijzigen in de onderwijssystemen van de school, dan kan men hiervoor terecht bij de afdeling administratie 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. Dit is ingeregeld in het PDOL-systeem via Groenendijk Onderwijsadministratie. De bewaartermijnen worden hierin per soort document aangeven.

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 Wonderwijs 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
- 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 uitvoering of toepassing van een andere wet te borgen

Binnen Wonderwijs 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 Wonderwijs 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 van Wonderwijs 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 personeelszaken van Wonderwijs, te bereiken via telefoonnummer: 0481-350003.

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 Wonderwijs hebben de volgende type medewerkers toegang tot de gegevens:
- Medewerkers salarisadministratie en financiën;
- HRM-adviseur en medewerkers personeelsadministratie;
- Opdrachtgever van de betreffende externe medewerker;
- Beleidsmedewerker financiën en controller;

Deze gegevens worden verstrekt aan uitzendbureaus en detacheringsbureaus waarmee door Wonderwijs 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 administratie van Wonderwijs, te bereiken via telefoonnummer: 0481-350003.

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. Het betreft naam, adres, telefoonnummer en/of e-mailadres.
Voor inzage en wijziging kan de betreffende vrijwilliger terecht bij de administratie van de school waar hij of zij vrijwilligerswerk verricht.

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 Wonderwijs kan er een klacht worden ingediend bij privacy@wonderwijs.nl .

Wanneer deze klacht voor de betrokkene niet leidt tot een acceptabele oplossing kan men zich wenden tot het bestuur van Wonderwijs via bestuur@wonderwijs.nl .

Bijlage 1 bij privacyreglement

Categorieën persoonsgegevens die binnen Wonderwijs verwerkt worden.

1. Leerlingen

Geen andere persoonsgegevens van een leerling worden verwerkt dan:

a. naam, voornamen, voorletters, geslacht, geboortedatum, adres, postcode, woonplaats;
b. het persoonsgebonden nummer;
c. nationaliteit en geboorteplaats;
d. gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling;
e. gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor het onderwijs;
f. gegevens betreffende de aard en het verloop van het onderwijs, alsmede de behaalde studieresultaten;
g. gegevens met het oog op de organisatie van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen;
h. gegevens met het oog op het berekenen, vastleggen en innen van de ouderbijdrage of de bijdrage voor TSO;
i. andere dan de onder a tot en met i bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een wettelijke regeling.

2. Ouders, voogden, verzorgers van leerlingen

Geen andere persoonsgegevens van ouders, voogden, verzorgers van leerlingen worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens;
b. nationaliteit en geboorteplaats;
c. hoogst genoten opleiding; behaald diploma; diplomajaar; naam en plaats van de instelling waar het diploma is behaald;
d. beroep;
e. relatie tot het kind;
f. burgerlijke staat.

3. Sollicitanten

Geen andere persoonsgegevens van sollicitanten worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer, e-mailaccount en soortgelijke voor communicatie benodigde gegevens, alsmede bank- en girorekeningnummer van de betrokkene;
b. een administratienummer dat geen andere informatie bevat dan bedoeld onder a;
c. nationaliteit en geboorteplaats;
d. gegevens betreffende gevolgde en te volgen opleidingen, cursussen en stages;
e. gegevens betreffende de functie waarnaar gesolliciteerd is;
f. gegevens betreffende de aard en inhoud van de huidige dienstbetrekking, alsmede betreffende de beëindiging ervan;
g. gegevens betreffende de aard en inhoud van de vorige dienstbetrekkingen, alsmede betreffende de beëindiging ervan;
h. andere gegevens met het oog op het vervullen van de functie, die door de betrokkene zijn verstrekt of die hem bekend zijn;
i. andere dan de onder a tot en met i bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet.

4. Medewerkers

Geen andere persoonsgegevens van medewerkers worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer, e-mailaccount en soortgelijke voor communicatie benodigde gegevens, alsmede bank- en girorekeningnummer van de betrokkene;
b. een administratienummer dat geen andere informatie bevat dan bedoeld onder a;
c. nationaliteit en geboorteplaats;
d. gegevens als bedoeld onder a, van de ouders, voogden of verzorgers van minderjarige werknemers;
e. gegevens betreffende gevolgde en te volgen opleidingen, cursussen en stages;
f. gegevens betreffende de functie of de voormalige functie, alsmede betreffende de aard, de inhoud en de beëindiging van het dienstverband;
g. gegevens met het oog op de administratie van de aanwezigheid van de betrokkenen op de plaats waar de arbeid wordt verricht en hun afwezigheid in verband met verlof, arbeidsduurverkorting, bevalling of ziekte, met uitzondering van gegevens over de aard van de ziekte;
h. gegevens die in het belang van de betrokkenen worden opgenomen met het oog op hun arbeidsomstandigheden;
i. gegevens, waaronder begrepen gegevens betreffende gezinsleden en voormalige gezinsleden van de betrokkenen, die noodzakelijk zijn met het oog op een overeengekomen arbeidsvoorwaarde;

j. gegevens met oog op het organiseren van de personeelsbeoordeling en de loopbaanbegeleiding, voor zover die gegevens bij de betrokkenen bekend zijn;
k. andere dan de onder a tot en met j bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet.

B. Tekst voor in de schoolgids

Privacy en leerlinggegevens

Ter bescherming van de privacy van leerlingen, hun ouders en medewerkers betracht Wonderwijs de grootst mogelijke zorgvuldigheid. Van medewerkers, ouders en leerlingen wordt daarom verwacht dat zij zich houden aan onderstaande maatregelen.

Hoe gaan wij om met de informatie van en over leerlingen
Over de ingeschreven leerlingen verzamelt de school alle informatie die noodzakelijk is om hen zo goed mogelijk kunnen begeleiden bij het doorlopen van de schoolloopbaan en om zo nodig extra ondersteuning te kunnen bieden. Deze informatie wordt (digitaal) opgeslagen in het leerlingdossier (alle geregistreerde informatie over een leerling).

Omdat wij deze gegevens over leerlingen verzamelen, vallen we onder de Algemene Verordening Gegevensbescherming. Deze wet is bedoeld om ervoor te zorgen dat de gegevens over personen zorgvuldig worden gebruikt (geheimhoudingsplicht) en wordt misbruik ervan tegen gegaan. Het leerlingdossier is alleen toegankelijk voor de begeleiders van een leerling ín de school en het bevoegd gezag.

In de school wordt regelmatig over leerlingen gesproken, bijvoorbeeld in de rapportvergadering, de leerlingbespreking en het interne zorgoverleg. Dit overleg is nodig om de vorderingen van de leerlingen te volgen, problemen te signaleren en afspraken te maken over de begeleiding. Voor leerlingen die extra begeleiding of ondersteuning nodig hebben, wordt samengewerkt met externe deskundigen. Als we een leerling willen bespreken met deze externen wordt daarvoor eerst aan ouders/verzorgers toestemming gevraagd.

Bij onze scholen is een (groot) aantal disciplines nauw betrokken bij de ontwikkeling en ondersteuning van onze leerlingen. Dit betekent echter niet dat onze scholen alle gegevens in haar bezit hebben. Het gaat hierbij om:

- de medische dossiers vallen onder het beheer van de schoolarts
- de overige gegevens, zoals verslagen van onderzoek en besprekingen, vallen onder het beheer van de directie. Alle dossiers mogen slechts onder toezicht worden ingezien. Ouders hebben uiteraard het recht deze in te zien.
- de schooldossiers worden twee jaar na het schoolverlaten van de leerling vernietigd.
- het beschikbaar stellen van dossiergegevens aan derden kan slechts plaatsvinden na toestemming van ouders/wettelijk vertegenwoordigers.
- de school kan slechts na toestemming van ouders overgaan tot het opvragen van dossiergegevens bij derden.

Zie voor verdere gegevens over de Algemene Verordening Gegevensberscherming
https://autoriteitpersoonsgegevens.nl

Hoe gaan wij om met informatie van en over ouders

Over de ouders van ingeschreven leerlingen verzamelt de school alle informatie die noodzakelijk is om hen zo goed mogelijk kunnen begeleiden bij het doorlopen van de school en om zo nodig extra zorg te kunnen bieden. Deze informatie wordt (digitaal) opgeslagen in het leerlingdossier.

Hoe gaan wij om met informatie van en over medewerkers
Over de medewerkers die bij ons werkzaam zijn en zijn geweest verzamelt het schoolbestuur alle informatie die noodzakelijk is voor hun aanstelling en bezoldiging. Deze informatie wordt (digitaal) opgeslagen in het personeelsdossier (alle geregistreerde informatie over het personeelslid).

Hoe gaan wij om met sociale media
Met een betrekking tot de omgang met sociale media is een 'gedragscode voor het gebruik van sociale media' opgesteld dat alle medewerkers hebben ontvangen. Op alle scholen binnen Wonderwijs worden leerlingen onderwezen in de omgang met sociale media.

Hoe gaan wij om met het maken en gebruiken van foto's en video's.
Het is op Wonderwijs scholen mogelijk 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. Toestemming van ouders is eveneens vereist als hun kind gefilmd wordt voor privédoeleinden. Hierbij valt te denken aan ouders die willen filmen tijdens bijvoorbeeld het vieren van een verjaardag op school. Dan dient er vooraf toestemming te zijn van de directie van onze school.

Het maken van foto's of video-opnamen van een leerling door (een medewerker van) Wonderwijs geschiedt altijd op basis van toestemming van ouders/voogden. Deze toestemming wordt in ieder geval eens per schooljaar bij ouders getoetst. Bij de inschrijving van een leerling wordt toestemming voor het gebruik van foto's en video-opnamen voor genoemde doeleinden gevraagd.

Wat vragen wij van ouders
Voorzieningen zoals bijvoorbeeld digitale camera's, mobiele telefoons en tablets zorgen ervoor dat ouders op schoolbijeenkomsten veel foto's en video-opnames kunnen maken. Wij kunnen dat niet verbieden. Wij vragen echter voorafgaand aan dergelijke events of ouders eraan willen denken dat lang niet alle ouders van leerlingen en medewerkers het op prijs stellen dat deze beelden op sociale media geplaatst worden. En verzoeken hen om alleen opnames waar uitsluitend hun eigen kind op staat via sociale media te verspreiden.

C. Tekst voor op de website (Responsible disclosure)

Bij Wonderwijs 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 Wonderwijs 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@wonderwijs.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 zo spoedig mogelijk op jouw melding reageren 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.

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 AVG 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 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 op www.wonderwijs.nl/privacy .

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

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

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

Sociale media

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

Formulier toestemming publicatie foto’s en video’s

[Plaats], [maand] [jaar]

Beste ouder/verzorger,

Op onze school laten wij u met foto’s en video’s zien waar we mee bezig zijn. Opnames worden gemaakt tijdens verschillende gelegenheden. Bijvoorbeeld tijdens activiteiten, schoolreisjes en lessen. Ook uw zoon/dochter kan op deze foto’s (en soms in video’s) te zien zijn.

Natuurlijk gaan we zorgvuldig om met foto’s en video’s. Wij plaatsen geen foto’s waardoor leerlingen schade kunnen ondervinden. We plaatsen bij foto’s en video’s geen namen van leerlingen. Toch vinden we het belangrijk om uw toestemming te vragen voor het gebruik van foto’s en video’s van uw zoon/dochter. Het is goed mogelijk dat u niet wilt dat foto’s van uw kind op internet verschijnen.

Met deze brief vragen we daarom uw toestemming voor het gebruik van beeldmateriaal van uw zoon/dochter. Wilt uw deze brief of antwoordstrook met uw kind meegeven naar school?

Uw toestemming geldt alleen voor foto’s en video’s die door ons, of in onze opdracht worden gemaakt. Het kan voorkomen dat andere ouders foto’s maken tijdens schoolactiviteiten. De school heeft daar geen invloed op, maar wij gaan ervan uit dat deze ouders ook terughoudend zijn bij het plaatsen van foto’s en video’s op internet.

Wilt u uw toestemming samen met uw zoon/dochter bespreken? We merken dat oudere leerlingen soms zelf een keuze willen maken om foto’s te gebruiken. Als u uw keuze thuis bespreekt, dan weten ze zelf waarom het gebruik van foto’s en video’s wel of niet mag.

Als we foto’s en video’s willen laten maken voor onderzoeksdoeleinden, bijvoorbeeld om een les van de stagejuf op te nemen, zullen we u daar apart over informeren en zo nodig om toestemming vragen. Ook als we beeldmateriaal voor een ander doel willen gebruiken, nemen we contact met u op.

U mag natuurlijk altijd terugkomen op de door u gegeven toestemming. Ook mag u op een later moment alsnog toestemming geven.

Alvast bedankt voor uw medewerking!

Met vriendelijke groet,

[naam ondertekenaar]

Hierbij verklaart ondergetekende, ouders/verzorger van ..... groep .....

dat foto's en video's door <schoolnaam> gebruikt mogen worden*:

☐ in de schoolgids, de schoolbrochure en schoolkalender.
☐ op de website van de school.
☐ in de (digitale) nieuwsbrief.
☐ op sociale-media accounts van de school (Twitter, Facebook) ter promotie van de school.

☐ Ik geef toestemmen dat de naam, adres en telefoonnummer gedeeld mag worden met andere ouders voor een klassenlijst.

* aankruisen waarvoor u toestemming geeft

Datum: .....

Naam ouder/verzorger: .....

Handtekening ouder/verzorger: .....

Toelichting gebruik formulier toestemming

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

In het toestemmingsformulier is aparte toestemming opgenomen voor verschillende categorieën. De wetgever eist dat een ouder een goedgeïnformeerde beslissing kan nemen, die ook specifiek is. Het vragen van toestemming 'voor gebruik van foto's door de school' is dat zeker niet. Als school mag je je het dus niet zo formuleren: 'als u niet wilt dat we foto's van uw kind gebruiken, moet u dat maar zeggen'. Dit is een 'opt-out', en dit is in strijd met de wet.

Foto's maken door ouders op school

Het kan voorkomen dat ouders het vervelend vinden dat andere ouders foto's maken van hun kinderen.

Meestal overleggen deze ouders samen over het maken en gebruik van die foto's. Soms komen ouders er samen niet uit en dan wordt de school gevraagd om iets te regelen.

De school wil voor álle kinderen een veilige omgeving zijn, en niet een plek waar kinderen (en hun ouders) bang hoeven te zijn steeds te worden gefotografeerd. Het maken van foto's en

video’s op school kan moeilijk worden verboden, maar kan wel aan banden worden gelegd. Door bijvoorbeeld verwachtingen uit te spreken naar ouders over fotograferen tijdens een schoolactiviteit, of door ouders in de nieuwsbrief te vragen terughoudend te zijn met het maken en publiceren van foto’s. Mocht dat niet het gewenste effect hebben, dan kan de schoolregels voor het maken van foto’s op school vastleggen in het privacyreglement of in een aparte gedragscode of een protocol. Een schoolgebouw is niet zomaar een openbare plaats waar iedereen toegang toe heeft. De school kan aan het verlenen van toegang dus voorwaarden verlenen zoals de (extreme) regel dat fotograferen van leerlingen tijdens de les of in klas alleen is toegestaan door docenten.

Toestemming geven door één of twee ouders

Als leerlingen jonger zijn dan 16 beslissen de wettelijk vertegenwoordigers (de ouders) over de privacy. De wet gaat ervan uit dat je als school mag vertrouwen op de mededelingen van één ouder. Als dat vertrouwen terecht is, dan is de andere ouder ook gebonden aan die mededeling. Bij het ondertekenen van de toestemmingsverklaring, mag de school dus vertrouwen op de toestemming als één ouder die geeft. Alleen als de school weet dat de andere ouder (die niet getekend heeft) tegen de toestemming is, mag de school niet uitgaan van die ene ondertekening. Dan moet de school van beide ouders toestemming hebben. Vooral bij gescheiden ouders kan het verstandig zijn om de toestemming van beide ouders te vragen. Voor het intrekken van toestemming is de mededeling van één ouder ook voldoende.

Bij twijfel is het beter om te vertrouwen op twee handtekeningen, of om de foto dan maar niet te gebruiken.

E. Beleid ambulant werken & mobiele bereikbaarheid

Inleiding

De huidige technologische ontwikkelingen en vragen vanuit de organisatie maken dat een eenduidige harmonisatie van regelingen en secundaire arbeidsvoorwaarden noodzakelijk is. Onderdeel van deze (secundaire) arbeidsvoorwaarden vormt de mogelijkheid van het door Wonderwijs ter beschikking stellen van mobiele devices en mobiele telefoons.

Momenteel beschikken een medewerkers, uit verschillende functiegroepen, over een mobiel device die door Wonderwijs in bruikleen is gegeven.

Fiscale regelgeving

Computers (incl. laptops en tablets), mobiele communicatiemiddelen en dergelijke apparatuur verstrekken kan, mits ze voldoen aan het noodzakelijkheidscriterium. Ook hier geldt dat werknemer de voorziening teruggeeft of de restwaarde betaalt als hij de voorziening niet meer nodig heeft voor de dienstbetrekking. Deze vergoedingen of verstrekkingen mogen niet worden gebruikt in een cafetariasysteem. Een werkgever kan wel een budget vaststellen waarmee de werknemer bijvoorbeeld een telefoon mag kopen. Als de werknemer dan een duurder device wil mag dat. In dat geval moet de werknemer een eigen bijdrage betalen uit zijn nettoloon. Vergoedingen en verstrekkingen voor telefoon en vergelijkbare communicatiemiddelen vallen binnen de WKR. Het verstrekken van vergoedingen heeft wel invloed op de vrije ruimte.

Vergoedingen, verstrekkingen en terbeschikkingstellingen worden toegepast conform hetgeen hierboven is beschreven. Alles wat de werknemer vergoedt, verstrekt of ter beschikking wordt gesteld voor zijn dienstbetrekking, is loon. Bepaalde vergoedingen, verstrekkingen en terbeschikkingstellingen zijn geen loon of geen belast loon.

Contract

Het is verplicht een gebruikersovereenkomst te sluiten met medewerkers die een mobiele telefoon of laptop in bruikleen krijgen. Medewerkers tekenen voor ontvangst en voor de voorwaarden die in het contract en dit beleid zijn gesteld. In onderstaand voorbeeld (zie bijlage F) zijn alle bepalingen opgenomen die op het in bruikleen geven/ nemen van een mobiele telefoon, tablet of laptop van toepassing zijn.

F. Model Gebruikersovereenkomst

De werkgever: Stichting Wonderwijs

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

Verklaren dat zij een gebruikersovereenkomst mobiele telefonie of laptop 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 en deze weer ingeleverd dient te worden bij beëindiging uitvoering taken waarvoor het device nodig is of bij beëindiging dienstverband;
- 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 eventuele 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 laptop of mobiele telefoon ter beschikking gesteld met een eventueel 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 boetes 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 eigen initiatief 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. 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 informatie omtrent het gebruik van de mobiele telefoon aangeleverd kan worden aan de werkgever.
b) Werknemer verklaart zich akkoord dat, indien gehandeld in strijd met de bepalingen van deze gebruikersovereenkomst mobiele telefonie en laptops, 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>

G. Cameratoezicht

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

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

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

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

Bewaartermijn beelden

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

Bekijken van beelden
Toestemming voor het bekijken van opgeslagen en/of actuele camerabeelden kan alleen gegeven worden door de schoolleiding.

Beheer systeem
ICT-coach (met toestemming van het CvB) is alleen gerechtigd benodigde software te installeren en te controleren op het functioneren van het systeem.

Informatie aan ouders

- Ouders van een leerling die een incident meldt dat het bekijken van camerabeelden noodzakelijk maakt, worden hiervan door de schoolleiding op de hoogte gesteld.
- Indien een leerling – in het belang van het oplossen van een incident – wordt verzocht camerabeelden te bekijken, worden ouders hiervan op de hoogte gesteld. Ouders kunnen het bekijken van de beelden desgewenst bijwonen.
- Ouders van een leerling die na het bekijken van de camerabeelden als “dader” wordt geïdentificeerd, worden hiervan door de schoolleiding op de hoogte gesteld en hebben het recht de beelden binnen de bewaartermijn uit dit protocol te bekijken.
- Camerabeelden die een incident registeren, dat aangifte bij de politie noodzakelijk maakt, kunnen desgevraagd door de politie worden bekeken. Betrokken leerlingen en ouders worden hierover geïnformeerd.

H. ICT en Social media protocol 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.
2. Ik vraag toestemming van mijn meester of juf, 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 en kan beoordelen of het echt of nep is.
8. Ik ken de gevolgen van het delen van informatie die niet echt is.

B. Sociale media
Binnen 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 op school of thuis.
12. Als ik iemand niet begrijp via de Whats app of andere berichten, dan vraag ik dit 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 (laptop, tablet, digibord etc.) is niet goedkoop, 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 onlinewereld en ik houd de tijd in de gaten als ik achter de computer/laptop of tablet zit.

I. Geheimhoudingsovereenkomst

Ondergetekende:

Naam:
Rol/ functie binnen Wonderwijs
Organisatieonderdeel:

Hierna te noemen: Werknemer

Overwegende:

- dat werknemer een dienstverband in het kader van de cao po heeft met Stichting Wonderwijs (hierna te noemen Wonderwijs)
- dat werknemer voor de uitvoering zijn of haar functie de beschikking moet hebben over informatie en/ of persoonsgegevens, door Wonderwijs verzameld in haar hoedanigheid als verantwoordelijke in de zin van de algemene verordening gegevensbescherming.
- dat Wonderwijs 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 Wonderwijs tevens moet voldoen aan haar wettelijke verplichting tot het treffen van technische en organisatorische beveiligingsmaatregelen ten aanzien van deze informatie en/ of persoonsgegevens.
- dat werknemer door het ondertekenen van deze verklaring erkent dat Wonderwijs deze informatie en/of persoonsgegevens als geheim en vertrouwelijk beschouwt en dat werknemer Vechtstreek en Venen 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 Wonderwijs 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 Wonderwijs verstrekt en voorschrijft.
- het voorgaande geldt ook voor door of namens Wonderwijs verstrekte toegang aan werknemer tot ICT-systemen en/of ter beschikking gestelde apparatuur.
-

- de werknemer zich verplicht alle door of namens Wonderwijs verstrekte informatie en/of persoonsgegevens te retourneren aan Wonderwijs zodra daarom verzocht wordt. De werknemer zal geen kopieën van de informatie bewaren.
- de werknemer erkent dat Wonderwijs 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:.....