IBP

Handboek informatiebeveiliging en privacy

Datum	:	11 november 2019
Herzien	:	20/02/2020
Status	:	Definitief
Versie:	:	0.01
CvB	:	21/01/2020, 23/06/2020
KD-PO	:	18/02/2020
KD-VO	:	17/02/2020
PMR	:	12/03/2020 (ter kennisname)
MR	:	01/04/2020 (ter kennisname)
GMR	:	01/04/2020 (ter kennisname)
RvT	:	N.v.t.
Bron	:	CED-groep
Bewerkt	:	Agnes Kurpershoek, Kwaliteit & Beleid

willem
van oranje
scholen
groep

Inhoud

Vaststelling

Dit handboek kan worden aangehaald als Handboek Informatiebeveiliging en Privacy Willem van Oranje Scholengroep.
Het handboek is herzien op 20 februari 2020.

Het handboek is vastgesteld door het College van Bestuur van Willem van Oranje Scholengroep op 23 juni 2020.

De heer J.M. de Bruin
Voorzitter College van Bestuur

1. Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van informatiebeveiliging en privacy (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.
Hiervoor is er binnen Willem van Oranje Scholengroep een IBP-beleidsplan opgesteld. Het IBP-beleidsplan is vastgesteld door de GMR en MR en is te vinden op de portal van de Scholengroep. Onder het IBP-beleidsplan vallen ook het privacyreglement, de gedragscode ICT en internet en het reglement cameratoezicht.

Dit handboek is bedoeld als informatiebron voor alle medewerkers van Willem van Oranje Scholengroep.
Hierin staan de afspraken die we met elkaar gemaakt hebben over informatiebeveiliging en privacy. Hierbij hebben wij naast de wettelijke basis, ook onze visie op onderwijs en onze normen en waarden als uitgangspunt genomen.

2. Gedragscode

Voor een veilig schoolklimaat is het belangrijk dat de afspraken rondom informatiebeveiliging en privacy door alle werknemers worden nageleefd en uitgedragen. Daarom is er een Gedragscode ICT en Internet opgesteld waaraan alle medewerkers van Willem van Oranje Scholengroep zich dienen te houden.

De Gedragscode ICT en Internet is vastgesteld door het College van Bestuur na instemming van de GMR en MR en op te vragen bij privacy@wvoranje.nl. Een exemplaar is ook opgenomen op de site van de Scholengroep.

3. De basis van de privacy wetgeving

Privacy is een lastig en vaag begrip. Privacy op school gaat over de bescherming van gegevens over leerlingen, hun ouders en medewerkers. Dit wordt geregeld in de Algemene Verordening Gegevensbescherming (AVG). Als we praten over de AVG dan praten we over persoonsgegevens.

3.1 Wat zijn persoonsgegevens?

Een persoonsgegeven is informatie die direct iets over een persoon zegt of op een bepaalde manier herleidbaar is naar die persoon. Een andere manier om de term persoonsgegevens te omschrijven is: de gegevens waarmee je een specifiek persoon binnen een bepaalde groep kunt aanwijzen. Dat zijn bijvoorbeeld een naam, een adres en een geboortedatum. Bij een veelvoorkomende naam, zullen er meestal wat gegevens moeten worden gecombineerd om een specifieke persoon aan te wijzen. Dat verandert niets aan het feit dat een naam altijd een persoonsgegeven is. In **bijlage I - Persoonsgegevens** is schematisch weergegeven welke typen persoonsgegevens mogelijk zijn.

3.2 Grondslagen voor verwerking van persoonsgegevens

Persoonsgegevens mogen niet zomaar worden bewaard, verspreid, bewerkt etc. Dat mag alleen als er een grondslag op van toepassing is. Een grondslag is simpel gezegd een gegronde reden op basis waarvan er bevoegdheid is om met de persoonsgegevens aan de slag te gaan. De AVG-wet noemt 6 grondslagen. Er moet altijd minimaal 1 grondslag van toepassing zijn voor er überhaupt iets gedaan mag worden met persoonsgegevens!

Om persoonsgegevens te mogen verzamelen, is dus een grondslag nodig. Deze grondslagen zijn:

1. **Toestemming** van de betrokkene
   Foto's, gebruik digitale middelen (sociale media), begeleiding leerling door externe onderwijsspecialist;
2. Noodzakelijk voor de **uitvoering van de overeenkomst**
   Met de ouders/verzorgers. Bijvoorbeeld voor de TSO (tussenschoolse opvang) van kinderen, personeel - de arbeidsovereenkomst;
3. Noodzakelijk voor voldoen aan een **wettelijke verplichting**
   Bijvoorbeeld voor bekostiging, inspectie, overdrachtsdossier;
4. Een **vitaal belang** te beschermen
   De gegevensverwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen, bijvoorbeeld allergie;
5. Vervulling taak van **algemeen belang** of openbaar gezag
   Bijvoorbeeld de uitwisseling van informatie met samenwerkingsverbanden (let op: geen BSN);
6. **Gerechtvaardigd belang**
   Zoals het goed laten werken van digitale leermiddelen. Bijvoorbeeld voor educatieve uitgeverijen.

3.3 Vuistregels bij verzamelen en verstrekken van persoonsgegevens

Als er een grondslag is en dus persoonsgegevens verwerkt mogen worden, dan zijn de volgende vuistregels van belang:

1. Doelbepaling doelbinding
Worden de persoonsgegevens alleen gebruikt voor dat doel dat vooraf is vastgelegd?
Persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld.
De belangrijkste doelen zijn voor het onderwijs:

- de organisatie of geven van onderwijs;
- het leren en begeleiden van leerlingen/studenten;
- het verstrekken of ter beschikking stellen van leermiddelen;
- het bekend maken van informatie over de hierboven genoemde organisatie en leermiddelen; het bekend maken van informatie over leerlingen, deelnemers of studenten (bijv. de eigen website);
- het bekend maken van de activiteiten van de instelling of het instituut op de eigen website;
- het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen;
- het behandelen van geschillen;
- het doen uitoefenen van accountantscontrole;
- de uitvoering of toepassing van een andere wet.

2. Dataminimalisatie
Worden die gegevens gebruikt die noodzakelijk zijn om het vastgestelde doel te verwezenlijken? Is het mogelijk met minder of bijvoorbeeld anonieme gegevens te werken? Worden de gegevens niet langer bewaard dan nodig?

3. Transparant
Zijn de leerlingen of hun ouders vooraf helder geïnformeerd over het doel van de gegevensverwerking? Is uitgelegd welke gegevens worden gebruikt en met wie deze worden gedeeld? Deze informatievoorziening vindt ongevraagd plaats.

4. Juistheid
Kloppen de gebruikte persoonsgegevens nog steeds? De persoonsgegevens moeten correct zijn en blijven.

5. Opslagbeperking
Worden de gegevens niet te lang bewaard? Worden de bewaartermijnen gehanteerd?

6. Integriteit en vertrouwelijkheid
Staan de gegevens op de juiste plaats en zijn ze voor de juiste mensen beschikbaar? Hebben er niet te veel mensen toegang tot deze gegevens?

7. Verantwoordingsplicht
Kan de dataverantwoordelijke (bestuurder) aan deze regels te voldoen? En kan de bestuurder dit aantonen?

Binnen Willem van Oranje Scholengroep is afgesproken dat er altijd een check is of aan deze vuistregels voldaan wordt bij het verzamelen en verstrekken van persoonsgegevens. Hiervoor wordt het volgende schema gebruikt.

Zijn het **persoonsgegevens**?

Is er een **grondslag** voor verzamelen?

Doelbepaling Doelbinding → uitdrukkelijk omschreven

Dataminimalisatie → alleen wat nodig is voor het **doel**

Transparant → zijn betrokkenen **geïnformeerd**?

Juistheid → zo nodig **actualiseren**

Opslagbeperking → bij voorkeur anoniem

Integriteit en vertrouwelijkheid → beveiliging

Verantwoordingsplicht → voldoen aan de **AVG-verplichting**

4. Privacyreglement en verklaring

Het privacyreglement is een document waarin nauwkeurig en op een begrijpelijke manier beschreven is welke persoonsgegevens binnen de organisatie worden verwerkt en met welk doel.

Ook is hierin te lezen wie toegang heeft tot deze gegevens, hoe de gegevens zijn beveiligd en met wie ze uitgewisseld mogen worden. Met het reglement voldoet het bestuur aan haar wettelijke informatieplicht, mits deze ook actief wordt aangeboden aan de leerlingen, ouders en medewerkers. Alle betrokkenen moeten daarom het privacyreglement kunnen inzien. Het privacyreglement heeft instemming van de GMR en MR en is vastgesteld door het College van Bestuur. Het privacyreglement is opgenomen op de website van Willem van Oranje Scholengroep.

Leerlingen en ouders moeten (tijdens de aanmelding) geïnformeerd worden over de gegevens die verzameld worden door de school en wat er met die gegevens gedaan wordt. Dit is opgenomen in de privacy verklaring/toelichting. De privacyverklaring heeft instemming van de GMR en MR en is vastgesteld door het College van Bestuur en opgenomen op de website van Willem van Oranje Scholengroep.

Medewerkers, leerlingen en ouders kunnen het reglement en de verklaring inzien op de website https://willemvanoranjescholengroep.nl. Op de sites van de scholen wordt verwezen naar dit adres zodat altijd de actuele informatie beschikbaar is.

5. Toestemming foto's/video's en online diensten

5.1 Richtlijn voor het gebruik en toestemming beeldmateriaal

Privacy wordt in Nederland beschermd door de Algemene Verordening Gegevensbescherming. Foto's en video's van leerlingen en medewerkers zijn persoonsgegevens en vallen daarmee onder deze wet. Daarom gelden er aangescherpte eisen voor het gebruik van beeldmateriaal. Het gaat om alle vormen van gebruik, zoals:

- foto's die de school in de nieuwsbrief plaatst;
- foto's die worden gedeeld of op sociale media geplaatst;
- een video die vertoont wordt op de website van de school.

De Autoriteit Persoonsgegevens (AP) is in Nederland toezichthouder op de uitvoering van de privacywetgeving. De AP heeft een aantal richtlijnen opgesteld voor het juist gebruik van beeldmateriaal op school.

Als een school foto's of video's van leerlingen gebruikt, dan is daar altijd toestemming van ouders voor nodig. Als de leerling 16 jaar of ouder is, moet de leerling daar zelf toestemming voor geven. Hierbij gelden de volgende voorwaarden:

De toestemming moet in **vrijheid** worden gegeven. Hiermee wordt bedoeld dat ouders en leerlingen altijd moeten kunnen weigeren, zonder dat daar sancties aan zijn verbonden. De inschrijving van een leerling op school mag bijvoorbeeld niet afhankelijk zijn van de toestemming om beeldmateriaal te gebruiken.
De toestemming moet '**ondubbelzinnig zijn'**. Dit betekent dat toestemming altijd nodig is. Als er geen reactie is op de vraag, mag niet worden aangenomen dat de ouders of de leerling het goed vinden dat beeldmateriaal gebruikt wordt. Wie zwijgt, stemt dus niet toe. Ook mag de toestemming niet verborgen zijn in de voorwaarden bij inschrijving of in de schoolregels. Toestemming moet namelijk altijd aangetoond kunnen worden.
De toestemming is **specifiek**. Dit houdt in dat het duidelijk is voor de leerling en zijn ouders waar toestemming voor wordt gegeven. Bij het vragen van toestemming is duidelijk hoe het beeldmateriaal wordt gebruikt: bijvoorbeeld op de website, nieuwsbrief of sociale media, en wat het doel is (bijvoorbeeld informeren van de ouders en leerlingen of promotie van de school).
Toestemming die eenmaal is gegeven, mag op **ieder moment worden ingetrokken**. En natuurlijk wordt het beeldmateriaal niet gebruikt als er (nog) geen toestemming is gegeven.

De beleidsregels van de AP benadrukken dat scholen het vragen om toestemming serieus moeten nemen. Ook al leidt dat tot extra administratieve rompslomp. Tenminste jaarlijks zal gewezen moeten worden op de toestemming die wel of niet is gegeven. Door het hele jaar heen moet het mogelijk zijn de toestemmingen aan te passen.

N.B.: Alle hierboven genoemde regels gelden ook voor de relatie school en medewerker.

5.2 Fotograferen door ouders, leerlingen of omstanders

Uiteraard zijn er in de school ook ouders, leerlingen of omstanders die foto's of video's maken bijvoorbeeld bij feestelijke gelegenheden. De school moet een veilige omgeving zijn voor alle leerlingen (en hun ouders) en medewerkers en zij moeten niet het risico lopen ongewenst gefotografeerd te worden.
Wanneer er activiteiten georganiseerd worden op een externe locatie, zoals bij een excursie, sportdag of schoolreis, is het echter lastig om het maken van beeldopnames te verbieden.

Willem van Oranje Scholengroep vraagt daarom de ouders, leerlingen, medewerkers en omstanders terughoudend te zijn met fotograferen. Ook wordt gevraagd aan ouders, leerlingen en medewerkers dat zij geen foto's van anderen op hun eigen sociale media plaatsen.

5.3 Online diensten

Voor het gebruik van online diensten door leerlingen binnen of buiten de school moeten bij leerlingen jonger dan 16 jaar ook ouders toestemming verlenen. Dit betekent dat wanneer leerlingen in de klas gebruik willen maken van een eigen (privé) account voor bijvoorbeeld Whatsapp of Pinterest, ouders hier vooraf toestemming voor moeten geven.

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

6. Rechten van betrokkenen en klachten over privacy

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

Hiervoor is een **procedure** opgesteld.
Het verzoek komt doorgaans binnen bij de leraar. Deze speelt het verzoek direct door aan de directeur of de Privacy Officer. De directeur of de Privacy Officer neemt het verzoek in behandeling. Bij vragen kan de directeur of de Privacy Officer terecht bij de Functionaris voor Gegevensbescherming (FG).

Betrokkenen kunnen een verzoek indienen bij de school of bij de verwerkingsverantwoordelijke (schoolbestuur). Betrokkenen kunnen verzoeken doen, die zijn gebaseerd op de volgende rechten:

1. Recht op informatie
2. Recht op inzage in de gegevens
3. Recht op kopie van de gegevens
4. Recht op correctie en aanvulling (rectificatie)
5. Recht op vergetelheid (wissen van gegevens)
6. Recht om gegevens over te (laten) dragen (dataportibiliteit)
7. Recht op beperking van de verwerking
8. Recht om bezwaar te maken tegen de verwerking van gegevens

Als inzage gewenst is in de gegevens die zijn verzameld, dan kan dat op de volgende manier.

- Een **medewerker** kan de vragen stellen aan de **directeur of Privacy Officer**.
- Een **leerling, ouder** of andere gezaghebbende die een vraag stelt, wordt doorverwezen naar de **directeur of Privacy Officer**.

In alle gevallen kan er ook altijd rechtstreeks contact opgenomen worden met de Functionaris voor Gegevensbescherming. De contactgegevens staan op de website van Willem van Oranje Scholengroep.

Voor de directeuren en de Privacy Officer is de uitgebreide procedure rechten van betrokkenen beschikbaar en een overzicht van welke ouder recht heeft op welke informatie (gezagkwesties). Tevens is er voor de directeuren en de Privacy Officer een registratieformulier beschikbaar om de genomen stappen te bewaken en aantoonbaar te maken.

7. Functionaris voor Gegevensbescherming

Een Functionaris voor Gegevensbescherming (FG) is iemand die controleert of een school zich aan de regels van de Algemene Verordening Gegevensbescherming (AVG) houdt. Een schoolbestuur is verplicht een FG aan te wijzen. Scholen of vestigingen die onder een schoolbestuur vallen hoeven geen eigen FG aan te wijzen.

Naast een controlerende taak beoordeelt een FG beveiligingsincidenten en datalekken, adviseert het bestuur en maakt medewerkers bewust van het belang van informatiebeveiliging en privacy. De FG is dé vraagbaak als het gaat om verwerking van persoonsgegevens.

Daarnaast is de FG de contactpersoon voor de externe toezichthouder: de Autoriteit Persoonsgegevens. Binnen Willem van Oranje Scholengroep hebben wij een Functionaris voor Gegevensbescherming aangesteld in de persoon van:

mevrouw A. Groen-Vendrig
CED-Groep
Mail: a.groen@cedgroep.nl
Telefoon: 010-4071993

In basis lopen alle vragen via onze interne Privacy Officer die bereikbaar is via privacy@wvoranje.nl.

Het is ook mogelijk indien gewenst om rechtstreeks contact op te nemen met de Functionaris voor Gegevensbescherming. De regeling taken en verantwoordelijkheden Functionaris voor Gegevensbescherming zijn met instemming van de GMR en MR vastgesteld.

8. Verwerkersovereenkomsten en verwerkersregister

8.1 Wat is een verwerkersovereenkomst?

In de nieuwe privacywet is bepaald dat de school afspraken moet maken met alle leveranciers van de school die leerlinggegevens verwerken in zogenaamde Verwerkersovereenkomsten. Het gaat bijvoorbeeld om uitgevers van digitaal lesmateriaal, leveranciers van toetsen, onderwijsadviesdiensten, etc.
Het belangrijkste hierbij is dat scholen, als gegevensverantwoordelijke, de regie hebben en houden over wat er gebeurt met de persoonsgegevens. Dit mag niet overgelaten worden aan de leverancier (verwerker). De school beslist wat de leverancier wél en niet met de gegevens mag doen.

8.2 Uitwisseling van gegevens met samenwerkingsverband

Een uitzondering hierop is de uitwisseling van gegevens met het samenwerkingsverband in het kader van passend onderwijs. Het samenwerkingsverband is een zelfstandige organisatie die zelf verantwoordelijk is voor de gegevens van leerlingen. De wet regelt dat een school gegevens uitwisselt met het samenwerkingsverband. Hiervoor hoeft daarom geen verwerkersovereenkomst afgesloten te worden. Het blijft natuurlijk wel belangrijk om de gegevens op de juiste manier uit te wisselen (zie hoofdstuk 11).

8.3 Het afsluiten van een verwerkersovereenkomst

De verwerkersovereenkomsten worden bovenschools afgesloten. Hiervoor is een inventarisatie gedaan van de lopende contracten van de scholen binnen Willem van Oranje Scholengroep. Wanneer een school een contract afsluit met een nieuwe leverancier zal er een nieuwe verwerkersovereenkomst gesloten moeten worden. Voordat de school een nieuw contract afsluit neemt de school eerst contact op met de Privacy Officer. Deze kijkt of het bestuur al een contract met deze leverancier heeft en zorgt anders eerst voor de verwerkersovereenkomst alvorens de school kan starten met de software. De privacy bijsluiters (deze zijn toegevoegd als bijlage bij een verwerkersovereenkomst) moeten inzichtelijk zijn voor ouders indien zij hierom vragen. Dit kan opgevraagd worden via privacy@wvoranje.nl.
Voor het afsluiten van verwerkersovereenkomsten wordt gebruik gemaakt van het meest actuele model verwerkersovereenkomst, die te vinden is via https://privacyconvenant.nl.

8.4 Verwerkersregister

Iedere verwerkingsverantwoordelijke moet een register van de verwerkingsactiviteiten die onder de verantwoordelijkheid van de verwerkingsverantwoordelijke vallen, in een register bijhouden (art. 30 AVG).

Het bestuur houdt de volgende gegevens in het register bij:

- de naam en de contactgegevens van de verwerkingsverantwoordelijke(n) en de functionaris voor gegevensbescherming;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen (van wie worden persoonsgegevens verwerkt? Bijvoorbeeld leerlingen, ouders, medewerkers, oud-medewerkers,);
- een beschrijving van de categorieën van persoonsgegevens (wat voor persoonsgegevens worden er verwerkt? Bijvoorbeeld BSN, financiële gegevens etc.);
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- doorgiften van persoonsgegevens aan een derde land of internationale organisatie (indien van toepassing);
- indien mogelijk een algemene beschrijving van de technische en organisatorische maatregelen die genomen zijn om te beveiligen.

Wanneer er een nieuwe verwerking plaatsvindt, moet deze in het register komen te staan.
Het register en de verwerkersovereenkomsten zijn in te zien op verzoek. Een verzoek kan worden ingediend via het bestuur of via privacy@wvoranje.nl.

9. Procedure datalekken

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

Voorbeelden van datalekken zijn:

- een e-mail die aan een verkeerd persoon geadresseerd is
- verlies of diefstal van waardepapier, dossier, usb-stick, tablet of andere gegevensdragers, of inloggegevens die openbaar zijn geworden
- een gestolen telefoon
- een gehackte computer
- een phishing mail

Is er mogelijk sprake van een datalek, dan is een medewerker verplicht dit zo snel mogelijk te melden bij de Privacy Officer van Willem van Oranje Scholengroep en bij de direct leidinggevende (ook bij twijfel).
Hiervoor kan het volgende emailadres gebruikt worden: privacy@wvoranje.nl.
Als er persoonsgegevens verloren, beschadigd of onrechtmatig ingezien zijn, dan moet er mogelijk binnen 72 uur een melding gedaan worden bij de Autoriteit Persoonsgegevens. De FG doet de melding in overleg met de verwerkingsverantwoordelijke.

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

Willem van Oranje Scholengroep beschikt over een stappenplan van de procedure datalekken. Het volledige schema procedure melden datalekken is op te vragen bij de Privacy Officer.

10. Toegangsbeleid

Binnen de organisatie zijn veel persoonsgegevens aanwezig. Zowel van medewerkers als van leerlingen. Niet alle medewerkers hebben toegang nodig tot alle leerlinggegevens. Per rol is vastgesteld welke gegevens kunnen worden ingezien en gewijzigd, waarbij is gekeken wat iemand in die rol nodig heeft aan gegevens om zijn of haar werkzaamheden uit te kunnen voeren. Gegevens die daarbij niet noodzakelijk zijn, kunnen door die rol ook niet ingezien of gewijzigd worden.

De directeur van de school is verantwoordelijk voor het verstrekken van de juiste toegang (accounts met de juiste rollen en rechten). De directeur ziet er ook op toe dat de accounts worden ingetrokken na het beëindigen van een arbeids- of samenwerkingscontract of het wijzigen van functies. Daarnaast worden de accounts van systemen met persoonsgegevens periodiek gecontroleerd. Dit wordt bijgehouden door middel van een uitdienst formulier dat door PZ verstrekt wordt zodra de ontslagbrief binnen is. Daarna wordt dit bewaard in het personeelsdossier.

De toegang tot gegevens van de medewerkers is beperkt tot de direct leidinggevende en diens vervanger en de PZ-/HRM-afdeling van het bestuur.

11. Uitwisselen van gegevens

Om ervoor te zorgen dat binnen de school gegevens op de juiste wijze uitgewisseld worden, is een schema gemaakt wanneer er toestemming gevraagd moet worden en hoe de gegevens uitgewisseld worden. Wanneer het doel niet is opgenomen, dan dient daarover geïnformeerd te worden bij de Privacy Officer of de Functionaris voor Gegevensbescherming (FG).

Persoonsgegevens verstrekken aan:	Het doel is:	Is toestemming nodig?
Overstap van PO naar andere basis-, SO/SBO- of VO-school	Overdracht (OKR,) leerlingdossier (na aanmelding) **W**	**NEE** maar ouders hebben wel inzage en de mogelijkheid hun zienswijze toe te voegen.
Overstap van VO naar VSO of andere VO-school	Overdracht (OKR,) leerlingdossier (na aanmelding) **W**	**JA** ouders mogen bezwaar maken tegen deze uitwisseling. Ze moeten inzage gehad hebben en toestemming gegeven.
Dienst Uitvoering Onderwijs (DUO)	Bekostiging **W**	**NEE**
Inspectie van het Onderwijs	Toezicht **W**	**NEE**
Leerplicht gemeente	Controle verzuim **W**	**NEE**
Administratiekantoor	Salarisadministratie en HRM	**NEE,** wel verwerkersovereenkomst
Samenwerkingsverband (SWV)	Advies, arrangement, Toelaatbaarheids-verklaring (TLV) (gegevens uit OPP) **W**	**NEE,** wel ouders informeren, **géén** BSN uitwisselen
Samenwerkingsverband (SWV)	Aanvullende gegevens op de OPP, voor TLV of advies of arrangement. Bijv. onderzoeksverslagen of informatie thuissituatie voor inzet jeugdhulp.	**JA,** voor alle medische verslagen is toestemming van de ouders nodig!
Samenwerkingsverband (SWV)	Thuiszitters tegengaan **W**	**NEE**
Educatieve uitgeverijen, Basispoort, Entree Federatie	Gebruik digitale middelen	**NEE**, wel verwerkersovereenkomsten met uitgeverijen
Educatieve apps (niet in beheer van de leraar of ICT)	Ondersteuning Onderwijs	**JA,** dit geldt als nadat de leerling school verlaten heeft de app nog gebruikt kan worden.
Externe onderwijs specialisten	Zorgbegeleiding (onderzoeken)	**JA**
Stagiaires (gegevens)	Opleiding	**NEE,** wel stage overeenkomst
Stagiaires (foto's/video)	Opleiding	**NEE** indien het materiaal binnen de school blijft. **JA** indien het materiaal buiten de school gebruikt wordt.
TSO/BSO	Tussenschoolse opvang, Buitenschoolse opvang	**JA**
GGD/JGZ*	Er mag **niet uitgewisseld** worden door de school!	**n.v.t***

W = Wettelijk verplicht
W*= Wettelijk verplicht en uitbesteed bij gemeente
***** De GGD wisselt uit met DUO. Op dit moment werkt de uitwisseling via DUO nog niet overal goed. Indien de vraag toch komt, overleggen met FG.

Deze tabel is niet uitputtend. Staat het type persoonsgegevensverstrekking er niet bij, dan is dit na te vragen bij de Functionaris voor Gegevensbescherming (FG).

12. Richtlijnen veilig mailen

E-mail is niet een bijzonder veilig medium. Mail kan onderweg onderschept worden. Het mailaccount kan natuurlijk gehackt worden, maar dat is iets dat ook bij andere uitwisselmedia kan gebeuren. Zeker zo belangrijk is dat een e-mail per ongeluk bij de verkeerde persoon terecht kan komen. Om daar de nadelige gevolgen van te voorkomen, kunnen een aantal maatregelen getroffen worden.

1. **Check altijd of inderdaad het goede e-mailadres ingevuld is.**
   Let dus op wanneer een e-mailprogramma een adres automatisch aanvult.

2. **Vul het e-mailadres pas op het laatst in, nadat het bericht geschreven is.**
   Dan kan de mail niet per ongeluk verstuurd worden.

3. **Neem in het e-mailbericht niet meer informatie op dan noodzakelijk is.**
   Persoonsgegevens mogen namelijk niet bij de verkeerde persoon terecht komen. Om toe te lichten wat wel en wat beter niet in de mail is op te nemen, hieronder twee voorbeelden.

Voorbeeld 1

Leraar mailt aan andere leerkracht:

'Daan Verstraete gaat morgen niet mee zwemmen omdat hij oorontsteking heeft.'

Zowel de volledige naam als de vermelding van medische informatie zijn **persoonsgegevens** waarmee zorgvuldig omgegaan moet worden. Het is daarom beter dit bericht als volgt te formuleren:

'Daan gaat morgen niet mee zwemmen.'

In bijna alle gevallen weten de betrokkenen wel om welke Daan het gaat en de reden is minder belangrijk. Is de reden wel belangrijk of is het noodzakelijk om andere persoonsgegevens te vermelden, mail dan **beveiligd**.

Voorbeeld 2

Leraar mailt aan ouder:

'De afgesproken intelligentietest bij uw dochter Hilde Özgül zal afgenomen worden op woensdag 5 oktober om 13.30 uur.'

Ook hier bevat de mail persoonsgegevens die niet in verkeerde handen terecht mogen komen. Een betere mail is daarom:

'De afgesproken test bij uw kind zal afgenomen worden op woensdag 5 oktober om 13.30 uur.'

Binnen de Willem van Oranje Scholengroep werken we met Office 365, hiermee is het mogelijk versleuteld te mailen. Via de afdeling ICT is een handleiding hiervoor beschikbaar.

13. Bewaartermijnen

Archivering: voorlopige bewaartermijnen

Op dit moment wordt er door Kennisnet in samenspraak met het ministerie van OC&W gekeken naar bewaartermijnen van persoonsgegevens. Naar verwachting zal daar binnenkort meer duidelijk over worden. Zolang hier nog geen duidelijkheid over is houdt Willem van Oranje Scholengroep vast aan de bewaartermijnen voor leerlinggegevens zoals hieronder aangegeven, tenzij de wet anders voorschrijft.

Document / gegevens	**Wettelijke bewaartermijn**	**Ingangsdatum bewaartermijn**	**Afwijkende bewaartermijn**
Gegevens over in– en uitschrijving	5 jaar	datum van uitschrijving	
Gegevens over verzuim en afwezigheid	minimaal 5 jaar	datum van uitschrijving	
Gegevens die nodig zijn om de bekostiging te berekenen	minimaal 7 jaar	na afloop van het schooljaar waarop de bekostiging betrekking heeft	
Gegevens leerling na overstap naar speciaal onderwijs	3 jaar	datum van uitschrijving	5 jaar*
Camera en videobeelden	maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten	moment van opname	
Het onderwijskundig dossier	maximaal 2 jaar	datum van uitschrijving	5 jaar*
Gezondheidsgegevens die nodig zijn voor speciale begeleiding of voorzieningen	maximaal 2 jaar	datum van uitschrijving	5 jaar*
Adresgegevens	maximaal 2 jaar	datum van uitschrijving	5 jaar*

*I.v.m. de inspectie-uitdraaien wordt de afwijkende bewaartermijn van 5 jaar gehanteerd. Hiermee wordt het advies van Kennisnet en de PO/VO raad gevolgd.

Indien de leerling of ouder hierom verzoekt, kan er eerder verwijderd worden. Hiervoor is het verstandig de FG in te schakelen.

Bewaartermijnen personeel

Document / gegevens	Ingangsdatum bewaartermijn	Wettelijke bewaartermijn	Afwijkende bewaartermijn
Sollicitatiebrieven, -formulieren, correspondentie omtrent de sollicitatie, getuigschriften	na beëindiging sollicitatieprocedure	4 weken zonder toestemming, 1 jaar met toestemming van de sollicitant	
VOG	einde dienstverband	1 jaar	5 jaar i.v.m. de accountants-controle
Arbeidsovereenkomst en wijzigingen	einde dienstverband	2 jaar	
BSN	einde dienstverband	7 jaar	
Loonbelastingverklaringen en kopieën van identiteitsbewijzen	einde dienstverband	5 jaar	
Verslagen van functioneringsgesprekken	einde dienstverband	2 jaar	
Loonbeslagen	Tot opheffing	Tot opheffing	
Opleiding	einde dienstverband	5 jaar	
Personeelsdossier, Nationaliteit NAW, contactgegevens, geslacht, levensloop	einde dienstverband	7 jaar	
Correspondentie over benoemingen, promotie, demotie en ontslag	einde dienstverband	2 jaar	
Financiële gegevens salarisadministratie	einde dienstverband	7 jaar	

14. Jaarplan privacy

Bij het bestuur en op elke school is een jaarplan aanwezig met punten die elk jaar aan de orde komen qua privacy. Denk hierbij aan verwijderen van leerlingdossiers en personeelsdossiers, het nakijken van de rechten, het wijzigen van de wachtwoorden etc.
Dit overzicht is in te zien via de directeur of op te vragen bij het bestuur.

15. Geheimhouding

Voor alle medewerkers van Willem van Oranje Scholengroep geldt een geheimhouding.
Zowel de werkgever als de werknemer nemen met betrekking tot hetgeen in of uit hoofde van hun functie vertrouwelijk te hunner kennis is genomen de nodige zorgvuldigheid en geheimhouding in acht. Dit geldt ook na beëindiging van het dienstverband. Ook met alle verwerkers is door middel van de verwerkersovereenkomst een geheimhouding afgesproken. Vrijwilligers op de scholen hebben voor geheimhouding getekend. Deze is op te vragen via privacy@wvoranje.nl.

16. DPIA

Met een DPIA brengen we de privacyrisico's van een gegevensverwerking in kaart. Vervolgens kunnen we maatregelen treffen om deze risico's te verkleinen.
In de Nederlandse vertaling van de AVG wordt de term Data Protection Impact Assessment (DPIA) gegevensbeschermingseffectbeoordeling genoemd.

Wanneer een DPIA (Data Protection Impact Assessment)?
Een DPIA verplicht als een verwerking voldoet aan 2 of meer van de 9 criteria. De 9 criteria zijn:
1. beoordelen van mensen op basis van persoonskenmerken;
2. geautomatiseerde beslissingen;
3. stelselmatige en grootschalige monitoring;
4. gevoelige gegevens;
5. grootschalige gegevensverwerkingen;
6. gekoppelde databases;
7. gegevens over kwetsbare personen (bijvoorbeeld kinderen);
8. gebruik van nieuwe technologieën;
9. blokkering van een recht, dienst of contract.

Ook als er aan slechts één - of geen - van deze criteria wordt voldaan, moet er kunnen worden onderbouwd waarom er voor gekozen is om geen DPIA uit te voeren. Dit maakt onderdeel uit van de verantwoordingsplicht onder de AVG. Bij een nieuwe verwerking wordt dus altijd gekeken of er een DPIA moet worden uitgevoerd. Voor bestaande verwerkingen geldt dat er alleen een verplichting is om een DPIA uit te voeren als er iets verandert aan het risico van de gegevensverwerking. En de gegevensverwerking vervolgens (na de verandering) een hoog privacyrisico oplevert.

17. Cameratoezicht

Over het gebruik van cameratoezicht op de scholen is een apart protocol opgesteld. Dit is met instemming van de GMR en MR vastgesteld. Hierin te lezen valt waarom er in bepaalde gevallen gekozen kan worden voor cameratoezicht en welke afspraken daarover zijn.

Bijlage I – Persoonsgegevens