**Informatiebeveiligings- en privacy protocol**

**Stichting RKBS Vleuten- De Meern - Haarzuilens**



**Bron**

saMBO-ICT

Kennisnet

Wet&Recht.nl

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versie** | **Status** | **Datum** | **Auteur** | **Omschrijving** |
| 6 | Aanpassen | Maart 2019 | Just Hageman/  Diny de Rooij | De volgende aspecten zijn toegevoegd of gewijzigd:   * Bijlagen 3 tot en met 7 * Bewaartermijn leerlinggegevens aangepast (alles 5 jaar bewaren) |
| 7 | Aanpassen | Mei 2019 | Diny de Rooij | Kleine tekstuele wijzigingen  Geheimhoudverklaring aangepast |
| 8 | Aanpassing | Febr 2020 | Just Hageman/  Diny de Rooij | Aantal wijzigingen, zie document wijzigingsvoorstellen |

**Functionaris persoonsgegevens**

Per 1 januari heeft mevrouw S. van Rooijen de functie functionaris persoonsgegevens op zich genomen.

Voor problemen die u rondom de privacy ervaart kunt u, voor zover niet te regelen is met de school, met hem contact opnemen via [silvia.van.rooijen@rksvdmh.nl](mailto:silvia.van.rooijen@rksvdmh.nl)

**Vastgesteld door Stichting RK basisscholen Vleuten, De Meern, Haarzuilens**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Naam** | **Functie** |
| 8 |  | M. van den Haak | Voorzitter CVB |

Inhoudsopgave

[Inleiding 4](#_Toc33109305)

[Toelichting informatiebeveiliging 5](#_Toc33109307)

[Toelichting privacy 5](#_Toc33109308)

[Vervlechting informatiebeveiliging en privacy 5](#_Toc33109309)

[Doel en reikwijdte 6](#_Toc33109310)

[Doel 6](#_Toc33109311)

[Reikwijdte 6](#_Toc33109312)

[Uitgangspunten 7](#_Toc33109313)

[Algemene beleidsuitgangspunten 7](#_Toc33109314)

[Uitgangspunten privacy 8](#_Toc33109315)

[Wet- en regelgeving 9](#_Toc33109316)

[Wet en regelgeving 9](#_Toc33109317)

[Stichtings- dan wel schoolprotocollen 9](#_Toc33109318)

[Organisatie 10](#_Toc33109319)

[Rollen 10](#_Toc33109320)

[Controle, rapportage en evaluatie 12](#_Toc33109321)

[Voorlichting en bewustzijn 12](#_Toc33109322)

[Incidenten en datalekken 12](#_Toc33109323)

[Controle, naleving en sancties 12](#_Toc33109324)

[Bijlage 1: Tabel IBP rollen en taken 13](#_Toc33109325)

[Bijlage 2: Scholen - leerlinggegevens 15](#_Toc33109326)

[Basispoort 15](#_Toc33109327)

[Parnassys medewerkers voor school 15](#_Toc33109328)

[Bijlage 3: Scholen - personeelsgegevens 18](#_Toc33109329)

[Bijlage 3a: Bewaartermijnen personeelsgegevens via PDOL 19](#_Toc33109331)

[Bijlage 4: Goed werknemerschap 21](#_Toc33109332)

[Bijlage 5: Risico-analyse IBP 22](#_Toc33109333)

[Bijlage 6: checklist IBP medewerkers en school 24](#_Toc33109334)

[Bijlage 7: voorbeeld kwaliteitskaart privacy leerlingen 26](#_Toc33109335)

[Bijlage 8: Planning AVG Stichting rk scholen Vleuten, De Meern, Haarzuilens 29](#_Toc33109337)

# Inleiding

Privacy is de persoonlijke levenssfeer die onszelf en ons handelen, eigenschappen en informatie onderscheidt en afschermt van anderen.

Ter bescherming van de privacy bestaat er nationaal en internationaal privacywetgeving. In ons land is het recht op privacy vastgelegd in de Nederlandse Grondwet en de [Wet bescherming persoonsgegevens](https://www.marketingtermen.nl/begrip/wet-bescherming-persoonsgegevens). Toezichthouder op de privacy van alle Nederlanders is het College Bescherming Persoonsgegevens (CBP).

Het onderwijsveld is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. Ook neemt de hoeveelheid informatie over personen toe door ontwikkelingen als gepersonaliseerd leren met ICT. Deze afhankelijkheid van ICT en gegevens brengt nieuwe kwetsbaarheden en risico’s met zich mee. Het is van belang om adequate maatregelen te nemen op het gebied van informatiebeveiliging en privacy (IBP) 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.

In dit protocol staat beschreven hoe de stichting RK basisscholen Vleuten, De Meern, Haarzuilens (verder te noemen de stichting) de regelingen rond privacy vorm geeft.

De informatie en ict van de scholen worden blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Alle informatie die we bewaren en verwerken kan worden bedreigd door overmacht (bijv. overstroming of brand), een vergissing, een cyberaanval et cetera. Het niet beschikbaar zijn van ict, het voeren van incorrecte administraties en het lekken van gegevens kunnen leiden tot problemen rondom het geven van onderwijs en het vertrouwen in de scholen.

Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico’s die gepaard gaan met deze bedreigingen tot een aanvaardbaar niveau te reduceren. Om dit structureel op te pakken is het noodzakelijk dat we duidelijk maken waar het om gaat en de manier waarop we dit willen bereiken.

We hebben ons uiterste best gedaan om alle situaties te beschrijven waarbij privacyregels in het geding kunnen komen. We beseffen als geen ander dat er zich altijd situaties kunnen voordoen, die buiten de gemaakte afspraken vallen. In voorkomende gevallen zullen we dit document aanpassen.

In dit document is de privacy rondom leerlingen en ouders geregeld (instemming Ouder- en Personeel:10E, instemming personeel: 12P en ouderdeel MR WMS artikel 13I en 13K)

### Als werkgever is de stichting verplicht om van alle werknemers een personeelsdossier bij te houden. Het personeel moet erop kunnen vertrouwen dat er zorgvuldig met de gegevens wordt omgegaan en dat niet zomaar iedereen bij die gegevens kan.

Het personeelsdossier bevat vertrouwelijke informatie (de (mogelijke) inhoud van het Personeelsdossier Online is als bijlage 3a toegevoegd). Hier wordt op gepaste wijze mee omgegaan. Deze dossiers zijn niet voor iedereen toegankelijk. De toegang van deze dossiers is vastgelegd en verleend aan medewerkers die deze informatie nodig hebben om hun werk goed te kunnen doen, zoals leidinggevenden en daarvoor geautoriseerde medewerkers. Deze medewerkers zijn gebonden aan de geheimhoudingsplicht uit de AVG.

Iedere werknemer heeft recht op inzage in zijn eigen personeelsdossier. Als een werknemer daarom vraagt, wordt hieraan meegewerkt. Je moet dan binnen vier weken de gevraagde informatie beschikbaar stellen. Een werknemer mag je vragen om gegevens te wijzigen of te verwijderen. Dit hoef je alleen te doen als informatie aantoonbaar onjuist is of niet (meer) relevant voor de arbeidsrelatie. Iedere werknemer ontvangt een persoonlijke inlogcode van het PDOL zodra deze is ingericht. (instemming personeel MR WMS artikel 12M).

## Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening te garanderen.

Deze aspecten zijn:

* Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
* Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
* Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn (doelgebruik).

Onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico’s bij de uitvoering van onderwijs en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot persoonlijk leed, financiële schades en imagoverlies.

## Toelichting privacy

Privacy gaat over persoonsgegevens en integriteit. Persoonsgegevens dienen beschermd te worden conform de geldende wet – en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die herleidbaar zijn tot een bepaald individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. De wet noemt als voorbeelden van verwerking: *het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.*

Integriteit wordt beschreven in de kernwaarden van de gedragscode van de stichting.

## Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijk onderdeel is van privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar, en zijn van elkaar afhankelijk. Het onderwerp informatiebeveiliging en privacy wordt afgekort tot IBP. Dit beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen Stichting Rooms Katholieke Basisscholen Vleuten-De Meern-Haarzuilens (in dit document verder afgekort als de stichting). Onder deze stichting vallen de volgende scholen: de Drie Koningenschool, De Twaalfruiter, De Willibrordschool, Sint Bonifatiusschool (nevenvestiging Willibrordschool) en Het Veldhuis. Als we in dit document praten over scholen, dan bedoelen we de hierboven genoemde vestigingen.

.  
In dit document wordt beschreven hoe de bovenschoolse informatiebeveiliging en privacy geregeld is. De scholen hanteren een kwaliteitskaart informatiebeveiliging en privacybeleid

# Doel en reikwijdte

## Doel

*Dit beleid heeft als doelen:*

* *Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.*
* *Het garanderen van de privacy van leerlingen en (voor zover van toepassing: hun ouders) en medewerkers waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen.*

Dit protocol is een leidraad voor iedereen die betrokken is bij IBP binnen de stichting. Het is van toepassing op onze eigen medewerkers, tijdelijk personeel en andere personen die een rol spelen in de scholen (bijv. bestuur, ouders en leerlingen). Het is van toepassing op de hele organisatie van de stichting, waaronder de fysieke locaties, systemen op interne en externe locaties en gegevensverzamelingen [[1]](#footnote-2) die gebruikt worden.

## Reikwijdte

* Het informatiebeveiligings- en het privacy protocol binnen de stichting geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing), alsmede voor alle organisatieonderdelen.
* Onder dit protocol vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden en alle devices die gegevens dragen.
* De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van de stichting. Het beleid heeft betrekking op gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina’s van) websites en sociale media.
* Het protocol heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen De stichting waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op andere betrokkenen waarvan St. rk VDMH persoonsgegevens verwerkt.
* In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaats vindt onder de verantwoordelijkheid van de stichting, evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
* IBP-beleid binnen de stichting heeft raakvlakken met:
* Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
* Medezeggenschap van leerlingen, hun ouders/verzorgers en medewerkers
* Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
* IT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen
* Aannamebeleid, meldcode, klachtenregeling, meldcode datalekken etc.
* Gedragscode, Sociaal mediaplan

# Uitgangspunten

## Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij de stichting zijn:

* Informatiebeveiliging en privacy dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming (die 25 mei 2018 in werking treedt).

De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen. Waarbij een goede balans tussen het belang van De stichting om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is.

* Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich ‘fatsoenlijk’ gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag, onveilige situaties ontstaan die leiden tot (emotionele) schade en/of imagoverlies. De stichting heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
* Binnen de stichting is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van fysieke documenten.
* Het bestuur is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen moeten goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.
* De stichting is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt.
* De scholen onder de stichting sluiten met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) bewerkersovereenkomsten af, als zij persoonsgegevens ontvangen. Hierbij wordt gebruik gemaakt van de meest recente versie van het convenant ‘[Digitale leermiddelen privacy](https://www.privacyconvenant.nl/)’ en de bijbehorende model bewerkersovereenkomst. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt op wettelijke basis.
* De stichting maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy.
* Informatiebeveiliging en privacy is bij de stichting een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is. De evaluatie gebeurt op stichtings- en op schoolniveau.
* Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij de stichting vanaf de start rekening gehouden met informatiebeveiliging en privacy door afspraken met de betreffende partij(en) te maken. Er is een balans tussen risico’s van hetgeen we willen beschermen en de benodigde investeringen en maatregelen, er is een balans tussen privacy, functionaliteit/werkbaarheid en veiligheid.

## Uitgangspunten privacy

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij de stichting zijn:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie**: bij de verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan 5 jaar (bijlage 2) na uitschrijving voor leerlingen en de personele gegevens volgens de richtlijnen van deze stichting.
4. **Transparantie**: de scholen zorgen ervoor dat aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording afgelegd wordt over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben bovenstaande betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun Persoonsgegevens. Ook kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen, zoals genoemd in de wetten Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming.Bij alle registraties zal de stichting aan de betrokkene een eenduidige zogenaamde Opt-out procedure[[2]](#footnote-3) worden aangeboden.

# Wet- en regelgeving

## Wet en regelgeving

De stichting voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

* Wet op het primair onderwijs en/of Wet voortgezet onderwijs
* Wet goed onderwijs en goed bestuur PO/VO
* Wet bescherming persoonsgegevens
* Algemene Verordening Gegevensbescherming (AVG)
* Archiefwet
* Leerplichtwet
* Wetboek van Strafrecht

## Stichtings- dan wel schoolprotocollen

Daarnaast gelden op de volgende protocollen en de daarbij behorende kwaliteitskaarten:

* Meldplicht datalekken (stichting)
* Aannamebeleid (stichting)
* Meldcode (stichting)
* Klachtenregeling (stichting)
* Gedragscode (stichting)
* Klokkenluidersregeling (bestuur)
* Sociaal Mediaplan (school)
* Veiligheidsplan (school)

Hiernaast zijn de bepalingen van het convenant ‘Digitale onderwijsmiddelen en privacy 2.0’ leidend bij het maken van afspraken met leveranciers.

# Organisatie

De organisatie van IBPgaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol.

Dit hoofdstuk beschrijft hoe IBP in de stichting is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

* Richtinggevend (strategisch)
* Sturend (tactisch)
* Uitvoerend (operationeel)

Voor elk niveau wordt beschreven welke rollen, welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij de stichting een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen. Hieronder zijn de verschillende rollen beschreven. De namen van de betreffende functionarissen vindt u in bijlage 1 ‘Tabel IBP rollen te taken’

## Rollen

**Eindverantwoordelijke**

Het College van Bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.

De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd op initiatief van het bestuur.

De inhoudelijke verantwoordelijkheid voor IBP is op schoolniveau gemandateerd aan de directies. Binnen de scholen zijn verschillende functies aan medewerkers toebedeeld.

**Functionaris voor Gegevensbescherming**

De functionaris voor gegevensbescherming (FuG) houdt binnen de stichting toezicht op de toepassing en naleving van de AVG (Algemene Verordening Gegevensbescherming). De wettelijke taken en bevoegdheden van de FuG geven deze functionaris een onafhankelijke positie in de organisatie. De FuG zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. FuG heeft regelmatig overleg met het college van Bestuur. De FuG is ook de contactpersoon voor klachten en vragen van de scholen.

**Portefeuillehouder ICT / ICT beheer**

Adviseert samen met het College van Bestuur en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen de Stichting.

**Domeinverantwoordelijke**

Binnen de stichting zijn er verschillende domeinen/processen, zoals ICT, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken en onderwijs. Op elk van deze domeinen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies. Deze functionaris noemen we domeinverantwoordelijke. De domeinverantwoordelijke heeft de volgende taken:

* Samen met het College van Bestuur stellen zij het beleid voor toegang vast.
* Samen met functioneel beheer en ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
* Samen met functioneel beheer en ICT-beheer beoordelen zij regelmatig de toegangsrechten van gebruikers.

De domeinverantwoordelijke is tevens verantwoordelijk voor de risico’s die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico’s te verkleinen zijn er op de scholen proceseigenaren met specifieke taken. Informatie hierover vindt u in de bijlage.

Het bestuur heeft een voorbeeldrol tenopzichte van de scholen.

Directies hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers, zoals medewerkers dat weer hebben naar leerlingen en ouders.

**Medewerker**

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Zij nemen deze verantwoordelijkheid bijvoorbeeld door:

* veilige en verschillende wachtwoorden te hebben
* deze wachtwoorden niet te delen
* uit te loggen bij privacygevoelige websites als zij hun werkplek verlaten
* geen privacy gevoelige gegevens opslaan op gegevensdragers enz.

Daarnaast zijn deze verantwoordelijkheden beschreven in de bijlage 6.

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR).

**Leidinggevende**

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. De directie heeft op uitvoerend niveau de taak om:

* er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid;
* toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
* periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen, etc.;
* als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

# Controle, rapportage en evaluatie

Dit informatiebeveiligings- en privacybeleid wordt jaarlijk getoetst en bijgesteld door het CvB. Hierbij wordt rekening gehouden met:

* de status van de informatiebeveiliging als geheel (beleid, organisatie, risico’s, veranderende wetgeving)
* de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan (ervaring vanuit de praktijk)

Bijstelling geschiedt op:

* **strategisch niveau:** richtinggevend wordt gesproken over organisatie en compliance, alsmede over doelen, scope en ambitie op het gebied van IBP.
* **tactisch** **niveau:** wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering.
* **operationeel** **niveau**: worden de onderwerpen besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm wordt decentraal georganiseerd, en indien nodig in elke school.

## Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico’s op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij de stichting het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico’s wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de directies van de scholen met het College van Bestuur als eindverantwoordelijke.

## Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij [silvia.van.rooijen@rksvdmh.nl](mailto:silvia.van.rooijen@rksvdmh.nl). De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken.

## Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat leidinggevenden hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode en met periodieke bewustwordingscampagnes (goed werknemerschap).

Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de Functionaris voor Gegevensbescherming (FuG) een belangrijke rol. De FuG wordt aangesteld door het College van Bestuur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FuG werkt met een door het CvB vast te stellen reglement.

Mocht de naleving tekort schieten, dan kan de stichting de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Bij de stichting ics het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

([protocol meldplicht datalekken](https://rkscholenvdmh.nl/files/images/20161201_Protocol_meldplicht_datalekken_incl_stroomschema.pdf)).

# Bijlage 1: Tabel IBP rollen en taken

|  |  |  |  |
| --- | --- | --- | --- |
| **Niveau** | **Wie**  **Rollen** | **Hoe**  **Verantwoordelijkheid / taken** | **Wat**  **Realiseren / vastleggen** |
| **Richtinggevend**  **(strategisch)** | CvB | * Eindverantwoordelijk * IBP-beleidsvorming, -vastlegging en het uitdragen ervan * Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens * Evalueren toepassing en werking IBP-beleid op basis van rapportages * Organisatie IBP inrichten | * Informatiebeveiligings- en privacy beleid * Baseline / basismaatregelen * Reglement FG vaststellen * Privacyreglement vaststellen |
| **Sturend**  **(tactisch)** | CvB | * Inhoudelijk verantwoordelijk voor IBP * IBP-planning en controle * Adviseert directie over IBP * Voorbereiden uitvoeren IBP-beleid, * Hanteren IBP normen en wijze van toetsen * Evalueren IBP-beleid en maatregelen * Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze * Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen | Processen, richtlijnen en procedures IBP, waaronder:   * activiteitenkalender * Protocol beveiligingsincidenten en datalekken * Bewerkersovereenkomsten regelen * Brief toestemming gebruik foto’s en video * Opstellen informatie documentatie richting leerlingen, ouders / verzorgers * Security awareness activiteiten * Sociale media reglement * Gedragscode ICT en internetgebruik * Gedragscode medewerkers en leerlingen |
|  | Functionaris voor  Gegevensbescherming | * Toezicht op naleving privacy wetgeving * Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens * Afwikkeling klachten en incidenten | * Privacyreglement, * procedure IBP-incident afhandeling * Inrichten meldpunt datalekken |
|  | Domeinverantwoordelijke | * Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door *bestuur/CvB/directie* * *Samen met functioneel beheer en ICT beheer* er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. * *Samen met functioneel beheer en ICT* beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren. | * Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) * Classificatie- en risicoanalyse documenten.   Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder:   * Toegangsmatrix diverse informatiesystemen en netwerk |

|  |  |  |  |
| --- | --- | --- | --- |
| **Niveau** | **Wie**  **Rollen** | **Hoe**  **Verantwoordelijkheid / taken** | **Wat**  **Realiseren / vastleggen** |
| **Uitvoerend**  **(operationeel)** | Functioneel beheerder  Medewerker  Directies | * Uitvoeren taken conform gegeven richtlijnen en procedures. * Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. * Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. * Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. * Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. * Implementeren IBP-maatregelen. * periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; * Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur. | Communiceren, informeren en toezien op naleving van o.a.:   * IBP in het algemeen * Regels passend onderwijs * Hoe omgaan met leerling dossiers * Hoe omgaan met personeelsdossiers * Wie mogen wat zien * Gedragscode * Omgaan met sociale media * Mediawijs maken * Informatiebeveilings en privacyprotocol van de school |

# Bijlage 2: Scholen - leerlinggegevens

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Drie Koningenschool** | **Sint Bonifatiusschool** | **Twaalfruiter** | **Veldhuis** | **Willibrordschool** |
| Basispoort | **X** | **X** | **X** | **X** | **X** |
| Parnassys | **X** | **X** | **X** | **X** | **X** |
| * Groepsautorisatie | **X** | **X** | **X** | **X** | **X** |
| * Invallers |  |  |  |  |  |
|  |  |  |  |  |  |
| **Oudercommunicatie** |  |  |  |  |  |
| Ouderportaal Parnassys |  | **X** |  |  | **X** |
| Parro |  | **X** | **X** |  | **X** |
| Social School | **X** |  |  |  |  |
| Digiduif | **X** |  |  |  |  |

### Basispoort

Om leerlingen eenvoudig toegang te geven tot digitaal leermateriaal van de school, maakt de school gebruik van Basispoort. Basispoort is een initiatief van Alberts Onderwijs, Heutink, de Rolf Groep, Malmberg, Noordhoff Uitgevers, Reinders Oisterwijk, ThiemeMeulenhoff en Uitgeverij Zwijsen. Zij vormen de Stichting Basispoort en zijn de initiatiefnemers en investeerders in hét Single Sign On- platform[[3]](#footnote-4) voor het basisonderwijs.

Leraren en leerlingen loggen in op een beveiligde website om bij Basispoort te komen.

De school heeft met Basispoort een overeenkomst gesloten waarin afspraken zijn gemaakt over het gebruik van de leerlinggegevens. Via Basispoort worden geen leer- of toetsresultaten opgeslagen en/of uitgewisseld.

**ECK iD**

In maart 2019 heeft de stichting zich aangemeld om gebruik te maken van het ECK iD. Dit is een maatregel die de privacy van leerlingen nog beter beschermt.

Als de verwerkersovereenkomst met Kennisnet is gesloten, zal het ECK iD via de leerlingenadministratiesysteem worden opgehaald. Vanaf dan kunt u het ECK iD in gebruik nemen bij het uitwisselen van gegevens met andere digitale leermiddelen in de keten. De verwerkersovereenkomsten met de betrokken leveranciers zijn hierop aangepast zodat zij voldoen aan de AVG.

### Parnassys medewerkers voor school

Voor het registreren van leerlinggegevens maken wij gebruik van Parnassys, een leerlingadministratiesysteem. Leraren loggen in op een beveiligde website om bij Parnassys te komen. Wanneer een leraar een uur niet op de website actief is, wordt de leraar automatisch uitgelogd.

Parnassys voldoet aan de eisen die de wet rondom privacy stelt.

Parnasys biedt daarnaast nog een aantal extra functies om de leerlinggegevens te beschermen. Het betreft de functies:

- groepsautorisatie

- Inzage gegevens

*Groepsautorisatie*

Door de leraart te koppelen aan de eigen groep(en) en de groepsautorisatie aan te zetten, ziet de leraar alleen de groepen voor wie zij onderwijs verzorgt. De leraar voldoet hiermee aan doelbinding: administreren en gebruik maken van alleen gegevens van leerlingen van de eigen groep.

Een school is een dynamisch geheel. Leraren moeten soms invallen in een andere groep, bijvoorbeeld ter vervanging van een zieke collega of een collega die een bijscholing moet volgen. Het kan dus zijn dat een leraar tijdelijk bij de gegevens van een andere dan de eigen groep moet kunnen. Om deze reden kan de leraar voor zichzelf tijdelijk de groepsautorisatie opheffen.

Als leraren de groepsaurorisatie opheffen, kunnen ze dit alleen doen door een reden aan te geven. Ook om datateamonderzoek te kunnen doen is het soms nodig om bij alle gegevens te kunnen.

Ambulant personeel werkzaam in dienst van onze school[[4]](#footnote-5) kan bij alle leerlinggegevens.

In Parnassys wordt geregistreerd wie om welke reden de groepsautorisatie opheft.

*Invallers*

Voor invallers is er een invalleraccount om toegang te hebben tot de digitale omgeving van de school. Een kortdurende invaller heeft geen toegang tot de leerlinggegevens in Parnassys. Als een leraar langer (langer dan 5 dagen) voor een groep invalt, wordt er een eigen emailadres aangemaakt en krijgt de invaller toegang tot de gegevens van de groep via Parnassys.

*Inzage gegevens*

De situatie kan zich voordoen dat een school wil weten welke gebruiker welke gegevens heeft ingezien. Parnassys biedt hier de mogelijkheid voor. De applicatiebeheerder kan in de Parnassysomgeving bekijken wie bij welke leerlinggegevens toegang heeft gehad.

Naast de beveiligde website, is er ook een app van Parnassys voor de smartphone(s) van /voor leraren. Hier kunnen zij op inloggen en zo bij de leerlinggegevens komen. Ook kunnen zij via de app afgeschermd telefoneren met opvoeders[[5]](#footnote-6). Dit dan weer ter bescherming van de privacy van de leraren.

Daarnaast gebruiken wij de beveiligde Parnassys omgeving om via e-mail te communiceren met opvoeders.

**Oudercommunicatie**

Op scholen zijn keuzes gemaakt over de manier om met ouders te communiceren.

In het overzicht hierboven ziet u welke keus de school gemaakt heeft. Op de betreffende scholen is er informatie over de gebruikte systemen.

**Bewaartermijn leerlinggegevens**

De stichting houdt zich aan de door de overheid aangegeven bewaartermijnen van de leerlinggegevens.

In het leerlingdossier bewaart de school:

* gegevens over in- en uitschrijving (5 jaar na vertrek)
* gegevens over afwezigheid
* adresgegevens
* gegevens die nodig zijn om het leerlinggewicht vast te stellen
* gegevens over de gezondheid die nodig zijn voor eventuele speciale begeleiding of voorzieningen
* gegevens over de ondersteuningsbehoefte, al het kind dat nodig heeft.
* gegevens over verzuim
* Gegevens over de vorderingen en de resultaten van het kind.

Op onze scholen worden deze volgende gegevens vijf jaar bewaard nadat een leerling de school verlaten heeft (dus langer dan de wettelijke bepaalde twee jaar of 3 jaar (bij verwijzing naar (S)BO), omdat we op onze scholen onderzoek doen naar (onder andere) resultaten van toetsen. (High Performance Scholen- traject dat op alle scholen in 2016 gestart).

Na vijf jaar worden alle gegevens van kinderen uit het systeem verwijderd (vanaf maart 2020 wordt dit proces opgestart). Voor reüniedoeleinden worden voordat de leerlingen uit het systeem worden verwijderd, alleen de adresgegevens digitaal opgeslagen.

**Inzage en correctie leerlinggegevens**

Ouders hebben recht om de gegevens van hun kind(eren) in te zien (inzagerecht). De ouders dienen daarvoor een afspraak te maken met de betreffende school. Als de gegevens van het kind worden ingezien, blijft er iemand van de school aanwezig. Ouders kunnen de school vragen om verkeerde gegevens in het leerlingdossier van het kind te verbeteren of te verwijderen.

Als een ouder geen wettelijk gezag heeft, moet de school ook inzage geven in de gegevens van het kind. De betreffende ouder moet dan een afspraak maken met de directie van de school.

**Inzage leerlingegevens door anderen**

In sommige gevallen is de school verplicht om informatie aan bepaalde deskundigen te geven. Bijvoorbeeld:

* medewerkers van het voortgezet onderwijs of speciaal (basis)onderwijs wanneer het kind de school verlaat.
* hulpverleners (bijvoorbeeld bij noodsituaties of vermoeden van kindermishandeling)
* inspectie van onderwijs

In andere gevallen moet u als ouder eerst toestemming geven.

# Bijlage 3: Scholen - personeelsgegevens

### Als werkgever is de stichting verplicht om van alle werknemers een personeelsdossier bij te houden. Het personeel moet erop kunnen vertrouwen dat er zorgvuldig met de gegevens wordt omgegaan en dat niet zomaar iedereen bij die gegevens kan.

Het personeelsdossier bevat vertrouwelijke informatie (de inhoud van het Personeelsdossier Online is als bijlage 3a toegevoegd). Hier wordt op gepaste wijze mee omgegaan. De zijn niet voor iedereen toegankelijk zijn. De toegang van deze dossiers is vastgelegd en verleend aan medewerkers die deze informatie nodig hebben om hun werk goed te kunnen doen, zoals leidinggevenden en medewerkers van de administratie en van Personeelszaken. Deze medewerkers zijn gebonden aan de geheimhoudingsplicht uit de AVG.

Iedere werknemer heeft recht op inzage in zijn eigen personeelsdossier. Als een werknemer daarom vraagt, wordt hieraan mee gewerkt. Binnen vier weken wordt de gevraagde informatie beschikbaar gesteld. Een werknemer mag vragen om gegevens te wijzigen of te verwijderen. Dit wordt alleen gedaan als informatie aantoonbaar onjuist is of niet (meer) relevant voor de arbeidsrelatie.

Iedere werknemer ontvangt een inlogcode van het PDOL zodra deze is ingericht. (instemming personeel MR WMS artikel 12M).

In 2020 worden alle personeelsgegevens gedigitaliseerd en ondergebracht in het PDOL (Personeesldossier online van Raet).

Voor het bewaren van personeelsgegevens zijn richtlijnen (zie overzicht in bijlage 3a ). Deze richtlijnen geven aan hoe lang gegevens bewaard moeten blijven. Na die termijn worden de gegevens vernietigd.

# Bijlage 3a: Bewaartermijnen personeelsgegevens via PDOL





# Bijlage 4: Goed werknemerschap

Onderstaande informatie wordt opgenomen in de gedragscode:

3.1 Privacy en geheimhouding

Uitgebreide informatie over privacy en geheimhouding staat in ons IBP plan.

De volgende aspecten benoemen we daarnaast in deze gedragscode, waarbij we te maken hebben met goed werknemerschap en goed werkgeverschap:

* Ieder personeelslid wordt geacht te beseffen dat gegevens van de organisatie, collega’s, leerlingen, ouders van vertrouwelijke aard zijn.
* Bij telefonische of schriftelijke overdracht van informatie over kinderen aan derden worden de medewerkers geacht zich ervan te vergewissen dat er schriftelijke toestemming is van de ouders (of belanghebbenden) voor overdracht van deze informatie. Tevens dienen zij na te gaan of de ontvanger gerechtigd is deze informatie te ontvangen. Daarbij houden we uitdrukkelijk rekening met de privacy van leerlingen, ouders en personeelsleden, zoals in dit document is opgenomen.
* Personeelsleden dienen te voorkomen dat anderen gelegenheid wordt geboden om kennis te nemen van informatie die niet voor hen bedoeld is.
* Personeel dient vooraf (schriftelijk) toestemming te vragen voor publicaties (mondeling en/of schriftelijk) die het belang van de werkgever (school en/of stichting, dan wel een persoon werkzaam voor of namens de stichting) kan schaden.
* Bedrijfseigendommen (geautoriseerde bestanden, aantekeningen, correspondentie en gegevensdragers of apparaten) dienen aan het eind van de dienstbetrekking terug gegeven te worden aan de werkgever.

De gehele gedragscode treft u hier aan: gedragscode (Link invoegen als gedragscode gewijzigd/ goedgekeurd is)

# Bijlage 5: Risico-analyse IBP

|  |  |  |  |
| --- | --- | --- | --- |
| **Risico** | **Kans** | **Impact** | **Maatregelen** |
| Niet vergrendelen van de werkplek | Groot | Groot | * Automatisch vergrendelen van applicaties/netwerk na bepaalde tijd. * Gebruikers bewust maken van de risico’s. |
| Achterlaten/verlies/diefstal digitale media:   * USB-sticks * Externe harde schijven * Mobiele telefoons * Laptops * Tablets | Middel | Groot | * Verbieden van het gebruik van USB-sticks en externe harde schijven. * Goede vergrendeling van privé-apparaten ter bescherming van applicaties t.b.v. schoolwerk. * Privé-apparaten hebben een eigen inlog voor privacygevoelige of schoolinformatie, waardoor andere gebruikers (gezinsleden) niet bij deze gegevens kunnen. |
| Printopdrachten worden direct geprint | Groot | Groot | * Beveiligd printen, waarbij iedere gebruiker moet inloggen om printopdrachten uit te printen. * Consumentenprinters mogen niet meer in het netwerk, vanwege de onmogelijkheden van het beheer. |
| Diefstal hardware | Middel | Groot | * Goede inbraakbeveiliging * Hardware in beheeromgeving, zodat deze op afstand te wissen zijn. * BIOS-vergrendeling |
| Applicaties:   * Office 365/G-Suite/Apple/MDM * Lokale kopie/synchronisatie schijven * Basispoort/Software * Leeromgevingen gekoppeld aan netwerkbeheer | Middel | Groot | * Automatisch inloggen in applicaties mag alleen ingeschakeld worden als het apparaat vergrendeld wordt met een sterk persoonlijk wachtwoord. * Wachtwoorden zijn niet zichtbaar op papier bij de werkplek. * Wachtwoorden die bewaard worden op iedere papieren vorm worden vernietigd als deze niet meer gebruikt worden. Ze mogen niet bij het oud papier belanden. * Het is niet toegestaan om dezelfde wachtwoorden voor hoog privacygevoelige inlog te hebben zoals mail en leerlingadministratie- en volgsystemen. |
| Papieren dossiers / Adreslijsten   * Leerlinggegevens * Financiële zaken * Personeelsgegevens |  |  | * Het is niet toegestaan om zonder toestemming van ouders en medewerkers adreslijsten te verspreiden. * Papieren dossiers zijn opgeborgen in afgesloten kasten en/of ruimtes. * Papieren dossiers mogen nooit bij het oud papier, maar dienen vernietigd te worden. |
| Ongewenst delen van content sociale media:   * Ouderportalen * Facebookpagina school | Middel | Groot | * Scholen vragen ieder schooljaar opnieuw toestemming aan de ouders voor het gebruik van sociale media. * Scholen moeten hierbij specificeren voor welke onderdelen de media wordt gebruikt. Ouders moeten per medium aangeven of zij hiervoor toestemming geven. * Ouders hebben altijd het recht om hun toestemming in te trekken of een beeld als ongewenst te bepalen. * Bovenschools mogen alleen foto’s gebruikt worden waarvan de ouders toestemming hebben gegeven voor het gebruik van deze foto’s. * Ouders die geen respons geven, hebben geen akkoord gegeven. Dit betekent dat beeldmateriaal niet gebruikt mag worden. |
| Aanval:   * DDos * Hack * Virus | Middel | Groot | * De netwerkbeheerder zorgt voor een gedegen beveiliging van het netwerk. * Meerdere keren per jaar wordt er een mail verstuurd om personeel te waarschuwen voor deze aanvallen en hoe te handelen mocht dit toch gebeuren. * Scholen waarschuwen de netwerkbeheerder indien zij het gevoel hebben dat zij een virus hebben geopend op hun pc. |
| Storing van:   * Internetverbinding * Applicaties * Netwerkbeheer | Klein | Groot | * Internetproviders versturen een mailing om locaties op de hoogte te brengen van werkzaamheden. * Het moet duidelijk zijn wie de contactpersonen van de provider zijn mocht de internetverbinding uitvallen. |

Kans: kans van het optreden van het risico

Klein: kan minder dan jaarlijks voorkomen  
Middel: kan meerdere keren per jaar voorkomen  
Groot: kan dagelijks voorkomen

Impact: effect als het risico waarheid wordt, de nadelige gevolgen.

1. Klein: verstoring niet-primaire proces, alleen intern merkbaar
2. Middel: verstoring primair proces, extern merkbaar, snel opgelost
3. Groot: verstoring primair proces, reputatieschade, langdurig

# Bijlage 6: checklist IBP medewerkers en school

**Checklist IBP medewerkers en school**

In verband met de aangepast AVG is deze checklistlist gemaakt. Het is een handzame vertaling van het IBP beleid van onze stichting.

**Als medewerker ben je verantwoordelijk voor:**

|  |  |
| --- | --- |
| **Werkplek** | Zorg voor automatische vergrendeling van je computer als je je werkplek/ lokaal verlaat (Windows L **of** 1. Ga naar het Windowsteken/start  2. Configuratieschermen  3. Persoonlijke instellingen  4. Klik (1 keer) op schermbeveiliging  5. Kies bij schermbeveiliging foto's  6. Vink het vakje aanmeldingsscherm weergeven bij hervatten aan  7. Kies na hoe lang het scherm moet bevriezen  8. Druk op ok) |
| **Wachtwoorden** | * Zorg voor een sterk wachtwoord (gezichtsherkenning, patroon, cijfercombinatie, enz.) op eigen devices wanneer er werk gerelateerde gegevens op staan (Parro, foto’s van leerlingen, werkmail) * Zorg ervoor dat privé devices waar meerdere gezinsleden gebruik van maken, geen school informatie bevat of log na gebruik van de app automatisch uit. * Zorg ervoor dat wachtwoorden niet zichtbaar op papier bij de werkplek te vinden zijn. * Zorg ervoor dat wachtwoorden die bewaard worden op iedere papieren vorm worden vernietigd als deze niet meer gebruikt worden. Ze mogen niet bij het oud papier belanden. * Zorg ervoor dat je verschillende wachtwoorden voor hoog privacygevoelige inlog hebt zoals mail en leerlingadministratie- en volgsystemen. |
| **Leerlinggegevens** | * Gebruik geen USB-sticks en externe harde schijven voor opslag van werk gerelateerde gegevens. * Het is niet toegestaan om zonder toestemming van ouders en medewerkers adreslijsten te verspreiden. * Zorg ervoor dat papieren dossiers zijn opgeborgen in afgesloten kasten en/of ruimtes. * Zorg ervoor dat papieren dossiers vernietigd worden (nooit bij het oud papier) |
| **Datalek** | * Je weet wat een datalek is en hoe je moet handelen in geval van een datalek * Het betreft een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Ook is er sprake van een datalek wanneer persoonsgegevens verloren zijn geraakt en er geen back-up is. Een datalek is het gevolg van een beveiligingsprobleem. * Een beveiligingsprobleem: een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatieverwerkende systemen in gevaar is of kan komen. |

**School is verantwoordelijk voor**

|  |  |
| --- | --- |
| School/ printen | * Beveiligd printen, waarbij iedere gebruiker moet inloggen om printopdrachten uit te printen. * Consumentenprinters mogen niet meer in het netwerk, vanwege de onmogelijkheden van het beheer. |
| School/ beveiliging | * Goede inbraakbeveiliging * Hardware in beheeromgeving, zodat deze op afstand te wissen zijn. * BIOS-vergrendeling * Een netwerkbeheerder die zorgt voor een gedegen beveiliging van het netwerk. * Meerdere keren per jaar wordt er een mail verstuurd om personeel te waarschuwen voor deze aanvallen en hoe te handelen mocht dit toch gebeuren. * Het waarschuwen van de netwerkbeheerder indien zij het gevoel hebben dat zij een virus hebben geopend op hun pc. |
| School/ medewerkers | * De school is zorgt ervoor dat iedere medewerker een geheimhoudingsverklaring heeft getekend. |
| School/ ouders | * Scholen vragen ieder schooljaar opnieuw toestemming aan de ouders voor het gebruik van sociale media. * Scholen moeten hierbij specificeren voor welke onderdelen de media wordt gebruikt. Ouders moeten per medium aangeven of zij hiervoor toestemming geven. * Ouders hebben altijd het recht om hun toestemming in te trekken of een beeld als ongewenst te bepalen. * Bovenschools mogen alleen foto’s gebruikt worden waarvan de ouders toestemming hebben gegeven voor het gebruik van deze foto’s. * Ouders die geen respons geven, hebben geen akkoord gegeven. Dit betekent dat beeldmateriaal niet gebruikt mag worden. |

# Bijlage 7: voorbeeld kwaliteitskaart privacy leerlingen

Bij de punten waar **\*** is toegevoegd, kan dit per school iets anders zijn

# Kwaliteitskaart Privacy leerlingen

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Kaart [nummer]** | [Keuze uit: leerling/ouders/passend onderwijs, leiding en/of leraar] | | **Verantwoordelijke** | **directie** | | **Geëvalueerd** | **[datum]** | |
| **Doel:**  Onze school gaat zorgvuldig om de privacy van leerlingen.   * voor school is het duidelijk of er beeldmateriaal van leerlingen gebruikt mag worden voor de diverse communicatiekanalen.  Jaarlijks wordt hierover gecommuniceerd met ouders. * gegevens over kinderen in de groep worden bewaard in de groepsmap\*. De privacygevoelige documenten liggen niet op het bureau van de leraar als deze niet in het lokaal is * onze school vraagt ouders toestemming voor het delen van informatie met externe partijen (denk aan onderzoek, overdracht vervolgonderwijs, buurtteam) |
| **Privacy en beeldmateriaal**   * eenmalig wordt ouders tijdens de intake gevraagd een formulier met toestemming voor het gebruik van beeldmateriaal in te vullen en te ondertekenen. Zij ontvangen dan informatie met betrekking tot de gebruikte termen. **\*** * jaarlijks wordt privacy en het gebruik van beeldmateriaal aan de orde gesteld tijdens de informatieavond**\*** van de groep * twee keer per jaar (gedurende een periode) kunnen ouders via Parro**\*** hun wensen met betrekking tot het gebruik van beeldmateriaal wijzigen. Daarover wordt in de schoolbrief geïnformeerd. Aan hen wordt wel gevraagd aan te geven dat zij wijzigingen hebben aangebracht in hun voorkeur. * als ouders op een ander moment de voorkeur willen aanpassen, kunnen zij dit doorgeven aan de administratie van de school.   **Privacy en overdracht naar derden**   * school levert aan klasgenoten alleen een overzicht met namen aan (geen telefoonnummers en adressen). Als ouders (nadat het kind begonnen is op school) adresgegevens van klasgenoten willen zien, kunnen zij daarvoor inloggen in het ouderportaal van Parnassys. Als ouders hebben aangegeven dat de adresgegevens geheim zijn, staat er op de plaats van het adres een \* vermeld. * school levert alleen informatie aan aan derden als ouders daar schriftelijk toestemming voor hebben gegeven. school levert een OSO (overdrachtsdossier vervolgonderwijs) aan, nadat ouders daarvoor toestemming hebben gegeven.   **Privacy in de klas**   * alleen gegevens voor dagelijks gebruik (denk aan roosters, smoelenboek, plattegrond) liggen op het bureau van de leraren. Andere gegevens (adressen, handelingsplannen e.d.) liggen daar niet, maar zijn opgeborgen in een kast\*. * met leerlingen wordt besproken/ hen wordt geleerd om zich uit te loggen uit digitale systemen als zij hun werkplek verlaten.   **Privacy en het recht op vergetelheid**   * onze school verwijdert de gegevens van leerlingen vijf jaar nadat zij van school zijn gegaan. |
| **Informatie voor ouders/verzorgers**  **Privacy- info naar ouders**  Jaarlijks hebben we de verplichting om ouders te bevragen over de privacy met betrekking tot hun kind(eren).  Dit in verband met de aangescherpte regels rondom privacy. Vorig schooljaar hebben we alle ouders gevraagd om een formulier rondom privacy in te vullen. Alle documenten zijn verwerkt in ons administratiesysteem, zodat het voor de leraren duidelijk is welk beeldmateriaal er gebruikt mag/kan worden.  Dit bleek voor scholen een bijzonder arbeidsintensief proces.  Inmiddels biedt Parro de mogelijkheid voor ouders om via deze app de voorkeuren rondom privacy per kind aan te geven.  *Hoe werkt dat?*   * U opent Parro. * U gaat naar het vierde tabbladje 'Instellingen'. * Tik op Profiel en scroll naar het kopje 'Mijn kinderen'. * Hier kunt u per kind aangeven wat uw voorkeuren zijn.   Mocht u uw voorkeur via Parro wijzigen, dan helpt het de leraren als u dit specifiek aangeeft. Nu zit er een overzicht in de klassenmap van de op dit moment bekende gegevens.  https://lh6.googleusercontent.com/oU6qPPKDFpz38JgVsWeG1fuOqT7XolVonZTO2Mkpi74b5x_ADIxBWZFk8nh-3k5kkwA4lLgskoTQxwmGCn7b0gImFDvxTZKuJxoRZPc7JZVn14VE8yFrSL3iuzjrALc_BCMkmTdEDag\* wordt het overzicht aangepast. We gaan ervan uit dat u voor die tijd uw (eventuele) wijzigingen invoert.  Nog een korte uitleg van wat we bedoelen met de  Beeldmateriaal Parro: de app voor communicatie van de groep. Deze gaat alleen naar ouders van de groep.  Beeldmateriaal Schoolbrief: deze brief verschijnt om de woensdag en wordt (als pdf) gemaild naar alle ouders van de school. Verder wordt deze brief op onze site gezet, daar kunnen belangstellenden de schoolbrief lezen  Beeldmateriaal Website: plaatsen van foto’s op onze website  (www.willibrordschool-vleuten.nl)  Beeldmateriaal Schoolgids: jaarlijks verschijnt er een nieuwe schoolgids. Daarin een enkele foto. De schoolgids kan (als pdf) gedownload worden via onze site (zie hierboven)  Beeldmateriaal sociale media: op school maken we **geen** gebruik van Facebook. Lerarenen plaatsen geen foto’s van kinderen op facebook. Wel bestaat de mogelijkheid om bv. het optreden van kinderen tijdens het open podium te filmen en beveiligd op Youtube te plaatsen. De link van deze filmpjes kan gedeeld worden met ouders van de groep (via Parro). De filmpjes kunnen overigens alleen gemaakt worden als er toestemming is van alle ouders van de groep voor dit item. |
| **Wat registreren in leerlingvolgsysteem?**  **Privacyvoorkeuren:**   * Eénmalig wordt (bij de intake) een toestemmingsformulier aan ouders uitgereikt met het verzoek deze ondertekend terug te geven aan school\*. * dit formulier wordt ingescand en in het digitale dossier van de leerling gehangen * de aangegeven keuzes worden geregistreerd in Parnassys\* (leerling → personalia → privacyvoorkeuren) * lerarenen kunnen in Parro\* per kind inzien wat ouders hebben doorgegeven   **OSO:**   * een OSO kan alleen worden verstuurd als ouders daar toestemming voor hebben gegeven. * een pdf versie van de OSO wordt geprint en aan ouders meegegeven of opgestuurd (door de leraren) |
| **Overig** |

v

# Bijlage 8: Planning AVG Stichting rk scholen Vleuten, De Meern, Haarzuilens

|  |  |  |  |
| --- | --- | --- | --- |
| **Wat** | **wie** | **wanneer** |  |
| 1. Schrijven IBP plan | Esther, Just, Diny | April 18-maart 19 |  |
| 1. Aanstellen Fug | Bestuur RKVDMH | Augustus 2018 |  |
| 1. Checklist personeel | Diny | Februari 2020 |  |
| 1. Aangepaste Planning AVG | Just en Diny | Februari 2020 |  |
| 1. Laatste aanpassingen plan | Diny | Maart 2020 |  |
| 1. Voorleggen aan Penta, bestuur en GMR (instemming) | Diny | Maart 2020 |  |
| 1. Goedkeuring door bestuur | Bestuur RKVDMH | Mei 2020 |  |
| 1. Plan ondertekenen, PDF en op bestuurssite plaatsen | Silvia | Juni 2020 |  |
| 1. Communiceren met alle scholen, directies en administratief medewerkers | Silvia | Juni 2020 |  |
| 1. Alle scholen zetten het IBP plan op de eigen site (voorkeur voor linken aan de bestuurssite) | Directies of administratief medewerkers | Juni 2020 |  |
| 1. Risico inventarisatie AVG op alle scholen  * Wie is de persoon per school waarbij datalekken moeten worden gemeld. * Wie is per school het aanspreekpunt voor de FuG | Directies | Sept 2020 |  |
| 1. Opstellen verbeterplan per school | Directies | September 2020 |  |
| 1. Verbeterplannen (met tijdspad) delen met FuG | Directies | Oktober 2020 |  |
| 1. Analyse door FuG  * Een (bijgewerkte) planning\* * Terugkoppeling van gevoerd beleid * Overzicht van datalekken en ondernomen acties. * Vermelding van gewijzigd beleid * 3x per jaar in Marap | Just | November- december 2020 |  |
| 1. Evaluatie IBP, wijzigingsvoorstellen verwerken, plan opnieuw vaststellen | bestuur | Voorjaar 2021 |  |
| 1. Bewustwordingssessie Privacy voor alle medewerkers | Bestuur RKVDMH | Schooljaar 2020-2021 |  |
| 1. Eens per 3 jaar het IBP plan door een externe laten controleren |  | November 2019  November 2022 |  |

1. Server, interne en externe databewaarders (usb-stick), cloud, mail, bijlagen [↑](#footnote-ref-2)
2. Een opt-outregeling houdt in dat betrokkenen niets hoeven te doen om mee te doen met de regeling, maar de mogelijkheid hebben ervan af te zien [↑](#footnote-ref-3)
3. Single sign-on-software (afgekort SSO) stelt eindgebruikers in staat om eenmalig [in te loggen](https://nl.wikipedia.org/wiki/Inloggen) waarna automatisch toegang wordt verschaft tot meerdere applicaties en resources in het netwerk. [↑](#footnote-ref-4)
4. intern begeleiders, directie, remedial teacher, ICT-er, administratie [↑](#footnote-ref-5)
5. Met opvoeders worden ouder(s) en of verzorger(s) bedoeld [↑](#footnote-ref-6)