Juli 2018

Informatiebeveiligings- en privacy protocol

RKBS Vleuten- De Meern - Haarzuilens

Stichting
RK Basisscholen
Vleuten - De Meern - Haarzuilens

Bron
saMBO-ICT
Kennisnet

Bewerkt door:
Esther Merkx en Diny de Rooij (Willibrordschool)

Versie	Status	Datum	Auteur	Omschrijving
1	Eerste opzet	2-11-2017	Esther Merkx en Diny de Rooij	Start schrijven beleid bestuur, nadat er een voorstel ligt voor een beleidsplan op schoolniveau (Willibrord en Boni)
2	Aanpassen	23-11-2017	Esther Merkx en Diny de Rooij	Aanpassingen naar aanleiding van opmerkingen
3	Aanpassen	Maart 2018	Diny de Rooij	Aanpassingen naar 1 document ipv school en bestuursdocument
4	Aanpassen	April 2018	Diny de Rooij	Aanvullingen vanuit de scholen en opname overzicht bewaren personeelsgegevens
5	Aanpassen	Juli	Just Hageman	Aanstelling functionaris persoonsgegevens

Functionaris persoonsgegevens

Per 1 augustus heeft de heer J,Hageman 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 just.hageman@rksvdmh.nl

Vastgesteld door Stichting RK basisscholen Vleuten, De Meern, Haarzuilens

Versie	Datum	Naam	Functie
		M. van der Haak	Voorzitter CVB

Inhoud

1 INLEIDING 5

1.1 TOELICHTING INFORMATIEBEVEILIGING 5
1.2 TOELICHTING PRIVACY 6
1.3 VERVLECHTING INFORMATIEBEVEILIGING EN PRIVACY 6

2 DOEL EN REIKWIJDTE 6

2.1 DOEL 6
2.2 REIKWIJDTE 6

3 UITGANGSPUNTEN 7

3.1 ALGEMENE BELEIDSUITGANGSPUNTEN 7
3.2 UITGANGSPUNTEN PRIVACY 8

4 WET- EN REGELGEVING 9

4.1 WET EN REGELGEVING 9
4.2 STICHTINGS- DAN WEL SCHOOLPROTOCOLLEN 9

5 ORGANISATIE 10

5.1 RICHTINGGEVEND 10
5.2 UITVOEREND 11

6 CONTROLE, RAPPORTAGE EN EVALUATIE 12

6.1 VOORLICHTING EN BEWUSTZIJN 12
6.2 INCIDENTEN EN DATALEKKEN 12
6.3 CONTROLE, NALEVING EN SANCTIES 12

BIJLAGE 1: TABEL IBP ROLLEN EN TAKEN 13
BIJLAGE 2:SCHOLEN - LEERLINGGEGEVENS 15

Basispoort 15
Parnassys medewerkers voor school 15

BIJLAGE 3:SCHOLEN - PERSONEELSGEGEVENS 18

1 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. 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 St. rk VDMH) 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 uitlekken 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 ouderdeel MR WMS artikel 13I)
Privacy rondom personeel moet nog beschreven worden (instemming personeel MR WMS artikel 12M). Een groot aantal zaken zijn in de praktijk al ingeregeld maar moeten nog beschreven worden.

1.1 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.

1.2 Toelichting privacy

Privacy gaat over persoonsgegevens. 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.*

1.3 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 RK VDMH). Onder deze stichting vallen de volgende scholen: Drie Koningenschool, De Twaalfruiter, De Willibrordschool, Sint Bonifatiusschool (nevenvestiging Willibrordschool) en Het Veldhuis. Deze scholen hebben allen een eigen informatiebeveiligings- en privacybeleid dat is toegespitst op de situatie op de betreffende scholen en is afgeleid van dit protocol.
In dit document wordt beschreven hoe de bovenschoolse informatiebeveiliging en privacy geregeld is. Als we in dit document praten over scholen, dan bedoelen we de hierboven genoemde vestigingen.

2 Doel en reikwijdte

2.1 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 St. rk VDMH. 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] die gebruikt worden.

2.2 Reikwijdte

- Het informatiebeveiligings- en het privacy protocol binnen St. rk VDMH 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.

[1] Server, interne en externe databewaarders (usb-stick), cloud, mail, bijlagen

- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van St. rk VDMH. 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 Stichting RK VDMH 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 Stichting RK VDMH, 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 St rk VDMH 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, Sociaal mediaplan, gedragscode, meldcode datalekken etc.

3 Uitgangspunten

3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij St. rk VDMH 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 Stichting RK VDMH 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.

- Binnen St. rk VDMH 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 scholen onder St. rk VDMH 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' 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.

- 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. Stichting RK VDMH heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

- De stichting is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt.

- De stichting maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy.

- Informatiebeveiliging en privacy is bij St. rk VDMH 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 St. rk VDMH 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.

3.2 Uitgangspunten privacy

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij Stichting RK VDMH 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 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 Stichting RK VDMH aan de betrokkene een eenduidige zogenaamde Opt-out procedure[2] worden aangeboden.

4 Wet- en regelgeving

4.1 Wet en regelgeving

De Stichting RK VDMH 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

4.2 Stichtings- dan wel schoolprotocollen

Daarnaast gelden op de volgende protocollen:

- Meldplicht datalekken (stichting)
- Aannamebeleid (stichting)
- Meldcode (stichting)
- Klachtenregeling (stichting)
- Gedragscode (stichting)
- 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.

[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

5 Organisatie

De organisatie van IBP gaat 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 Stichting RK VDMH 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 Stichting RK VDMH 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 de bijlage.

5.1 Richtinggevend

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 Stichting RK VDMH 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 RK VDMH 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.

5.2 Uitvoerend

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.

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.

6 Controle, rapportage en evaluatie

Dit informatiebeveiligings- en privacybeleid wordt minimaal elk jaar 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

Voor alle overlegmomenten geldt dat deze zoveel mogelijk ingepast worden in bestaande overlegvormen met hetzelfde karakter waarbij 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.

6.1 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 Stichting RK VDMH 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.

6.2 Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij s.vanrenswoude@rkscholenvdmh.nl. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken.

6.3 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. Bij Stichting RK VDMH wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode en met periodieke bewustwordingscampagnes.
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 Stichting RK VDMH de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.
Bij St. rk VDMH is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol. (link naar protocol).

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*	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) • Classificatie- en risicoanalyse documenten.

		• *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.	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**
• Invallers					
• Inzage gegevens					
Oudercommunicatie					
Ouderportaal Parnassys		**X**			**X**
Parro		**X**			**X**
Social School	**X**				
Digiduif	**X**		**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] voor het basisonderwijs.
Leerkrachten 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.

Parnassys medewerkers voor school

Voor het registreren van leerlinggegevens maken wij gebruik van Parnassys, een leerlingadministratiesysteem. Leerkrachten loggen in op een beveiligde website om bij Parnassys te komen. Wanneer een leerkracht een uur niet op de website actief is, wordt de leerkracht 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 leerkracht te koppelen aan de eigen groep(en) en de groepsautorisatie aan te zetten, ziet de leerkracht alleen de groepen voor wie zij onderwijs verzorgt. De leerkracht voldoet hiermee aan doelbinding: administreren en gebruik maken van alleen gegevens van leerlingen van de eigen groep.
Een school is een dynamisch geheel. Leerkrachten moeten soms invallen in een andere groep, bijvoorbeeld ter vervanging van een zieke collega of een collega die een bijscholing moet volgen.

3 Single sign-on-software (afgekort SSO) stelt eindgebruikers in staat om eenmalig in te loggen waarna automatisch toegang wordt verschaft tot meerdere applicaties en resources in het netwerk.

Het kan dus zijn dat een leerkracht tijdelijk bij de gegevens van een andere dan de eigen groep moet kunnen. Om deze reden kan de leerkracht voor zichzelf tijdelijk de groepsautorisatie opheffen.
Als leerkrachten 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] kan bij alle leerlinggegevens.

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 leerkracht 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. De invallers tekenen hiervoor een geheimhoudingsverklaring. **Geheimhoudverklaring moet nog gemaakt?!**

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 leerkrachten. Hier kunnen zij op inloggen en zo bij de leerlinggegevens komen. Ook kunnen zij via de app afgeschermd telefoneren met opvoeders[5]. Dit dan weer ter bescherming van de privacy van de leerkracht.
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.

[4] intern begeleiders, directie, remedial teacher, ICT-er, administratie
5 Met opvoeders worden ouder(s) en of verzorger(s) bedoeld

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
- Gegevens over afwezigheid
- Adresgegevens
- Gegevens die nodig zijn om het leerlinggewicht vast te stellen

Ook de volgende gegevens mag de school bewaren:

- Gegevens over de vorderingen en de resultaten van het kind
- Gegevens over de gezondheid die nodig zijn voor eventuele speciale begeleiding of voorzieningen
- Gegevens over de ondersteuningsbehoefte, al het kind dat nodig heeft.

De basisschool mak de meeste gegevens nog twee jaar bewaren, nadat het kind van school is gegaan. De volgende gegevens moet de school langer bewaren:

- Gegevens over verzuim en in- en uitschrijving (5 jaar na vertrek)
- Gegevens over een leerling die naar een school voor speciaal onderwijs is doorverwezen (3 jaar)
- Adresgegevens van (oud)leerlingen mag de school bewaren voor het organiseren van reunies.

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

Met personeelsgegevens wordt zorgvuldig omgegaan.
Momenteel is er nog een papieren dossier van personeelsleden. Het streven is om in schooljaar 2018-2019 over te stappen naar een digitaal personeelsdossier.
Voor het bewaren van personeelsgegevens zijn richtlijnen (bewaartermijn personeelsdossier- aangeleverd door Groenendijk). Deze richtlijnen geven aan hoe lang gegevens bewaard moeten blijven. Na die termijn worden de gegevens vernietigd.

De directie van de school heeft inzage in de personeelsgegevens. Zij besteden deels de administratie rondom personeel uit. Dat betekent op onze schoolen dat de administratief medewerker toegang heeft tot de personeelsdossiers (zowel papier als digitaal).
In het onderstaande schema de bewaartermijnen:

Bewaartermijn personeelsdossier				
Sollicitatiegegevens				
Document / gegevens	**Verplichte bewaartermijn**	**Ingangsdatum bewaar-termijn**	**Fiscus aspect**	**Vastgelegd in**
Sollicitatiebrief, -formulier, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek	4 weken zonder toestemming, 1 jaar met toestemming van de sollicitant	na beëindiging sollicitatieprocedure of einde dienstverband	-	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
Arbeidsvoorwaarden				
Document / gegevens	**Verplichte bewaartermijn**	**Ingangsdatum bewaar-termijn**	**Fiscus aspect**	**Vastgelegd in**
Akte van aanstelling / arbeidsovereenkomst	tot 2 jaar	einde dienstverband	-	Art. 52 Wet Rijksbelastingen
Wijzigingen arbeidsovereenkomst	tot 2 jaar	einde dienstverband	-	Art. 52 Wet Rijksbelastingen
Aanvullende arbeids- en salarisafspraken	minimaal 7 jaar	einde dienstverband	Ja	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
Loonbelastingverklaringen en kopie identiteitsbewijs	minimaal 5 jaar	einde dienstverband	-	Art.23a Uitvoeringsregeling loonbe-lasting
Correspondentie inzake benoemingen, pro-motie, demotie	tot 2 jaar	einde dienstverband	-	Art. 52 Wet Rijksbelastingen
Correspondentie inzake ontslag	tot 2 jaar	einde dienstverband	Ja	Art. 52 Wet Rijksbelastingen
VUT-regeling	tot 2 jaar	einde dienstverband	-	Art. 52 Wet Rijksbelastingen
Afspraken inzake werk OR	tot 2 jaar	einde lidmaatschap	-	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
Burgerlijke staat werknemer	minimaal 7 jaar	einde dienstverband	Ja	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
Kopie getuigschrift	tot 2 jaar	einde dienstverband	-	-
Loopbaan / personeelsontwikkeling				
Document / gegevens	**Verplichte bewaartermijn**	**Ingangsdatum bewaar-termijn**	**Fiscus aspect**	**Vastgelegd in**
Afspraken inzake opleidingen	periode dat werknemer evt nog kosten moet vergoeden	einde dienstverband	-	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
Aanvraag opleiding door werknemer	tot afronding / afbreking opleiding	-	-	-

Afspraken omtrent loopbaan	tot realisatie	-	-	-
Verslagen functionerings- en beoordelings-gesprekken	tot 2 jaar	einde dienstverband	-	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
Verzuim				
Document / gegevens	**Verplichte bewaartermijn**	**Ingangsdatum bewaar-termijn**	**Fiscus aspect**	**Vastgelegd in**
Ziektekosten	duur verzekering tot einde dienst-verband	-	-	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
Correspondentie UWV en bedrijfsarts	tot 2 jaar	einde dienstverband	-	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
Verslaglegging inzake Wet Verbetering Poortwachter	tot 2 jaar	einde dienstverband	-	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
Overige zaken				
Document / gegevens	**Verplichte bewaartermijn**	**Ingangsdatum bewaar-termijn**	**Fiscus aspect**	**Vastgelegd in**
Afstandsverklaring woon-werkverkeer	duur afspraak + 7 jaar	-	Ja	Art. 52 Wet Rijksbelastingen
Verslaglegging van probleemsituaties	tot 2 jaar	einde dienstverband	-	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
Verslaglegging van financiële problemen	2 jaar	-	-	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
Loonbeslagen	tot opheffing	-	-	Vrijstellingsbesluit Wet Bescherming Persoonsgegevens (WBP)
Brieven inzake jubilea	tot einde dienstverband	-	-	-
Correspondentie directie / PZ / direct leidinggevende	Afhankelijk van ontslagsituatie bij einde dienstverband of tot 2 jaar daarna	-	-	-
Gegevens inzake etniciteit en herkomst	minimaal 5 jaar	einde dienstverband	-	Wet Stimulering Arbeidsdeelname Minderheden - Wet Samen
Identiteitspapieren van van derden inge-leende vreemdelingen waarvoor een tewerkstellingsvergunning is verleend	minimaal 5 jaar	einde dienstverband	-	Wet Arbeid Vreemdelingen