| Werkveld | Datum | Vastgesteld CvB | |
|---|---|---|---|
| ICT | 9 september 2016 | | |

# Privacy

## Richtlijnen, gedragsregels en afspraken

Inhoudsopgave

# 1. Voorwoord

Er is de afgelopen jaren veel veranderd in het onderwijsveld. Er wordt steeds verder gedigitaliseerd. Zo werd Parnassys geïntroduceerd binnen KPOA, waarmee het gebruik van een gedegen wachtwoord enorm belangrijk is geworden. Met de komst van Office365, mobiele devices, MOO, de Z-schijf, digitale dossiers en “Single Sign On”, is beveiliging van persoonsgegevens steeds belangrijker geworden. De beveiliging van persoonsgegevens gaat niet alleen om de digitale versies, maar ook zeker over de papieren versies.
In dit document wordt beschreven hoe de wet en KPOA omgaan met deze “bijzondere gegevens” en hoe medewerkers om moeten gaan met de ICT omgeving.
Voor het schrijven van dit document is gebruik gemaakt van de huidige wetgeving en van de publicatie van Kennisnet; Privacy in 10 stappen.

## 2. Privacy en de wet

Privacy is een grondrecht. Een duidelijke uitleg is terug te lezen in Hoofdstuk 2 van https://www.kennisnet.nl/fileadmin/kennisnet/publicatie/Privacy_in_10_stappen.pdf van Kennisnet, zie bijlage 1. Hierin wordt het volgende uitgelegd over privacy (schuin gearceerd en soms ingekort);

*Privacy is niet zomaar iets: het is een grondrecht. Net als het recht op vrijheid van godsdienst of het recht op vrijheid van meningsuiting. In de Universele Verklaring van de Rechten van de Mens is privacy geborgd als mensenrecht. In Europa is privacy vastgelegd in artikel 8 van het Europees Verdrag voor de Rechten van de Mens. Sinds 1983 is privacybescherming opgenomen in artikel 10 van de Nederlandse Grondwet.*

### 2.1 De Wet bescherming persoonsgegevens

*In Nederland is privacy onder andere uitgewerkt in de Wet bescherming persoonsgegevens (Wbp). Deze wet beschermt de privacy door regels te stellen voor de omgang met persoonsgegevens in Nederland. Het uitgangspunt van de wet is dat privacy wordt gerespecteerd. De Wbp is mede gebaseerd op de belangrijke Europese richtlijn 'bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (95/46/EG)'. Deze richtlijn geeft de Europese overheden opdracht om privacy op een uniforme manier te regelen. De komende jaren zal deze richtlijn vervangen worden door de 'Algemene Verordening Gegevensbescherming' (AVG), waardoor privacy binnen Europa beter wordt beschermd.*

### 2.2 Bijzondere persoonsgegevens

*Leerlinggegevens zijn ook persoonsgegevens. De Wbp is hierop dus van toepassing. Vaak bevatten leerlinggegevens gevoelige informatie. Denk aan informatie over gezondheid, gedragsproblemen, godsdienst, seksuele voorkeur of een problematische thuissituatie. Deze gevoelige persoonsgegevens worden ook wel bijzondere persoonsgegevens genoemd. Deze mogen alleen worden vastgelegd als dat noodzakelijk is, bijvoorbeeld voor speciale begeleiding van leerlingen of om bijzondere voorzieningen te kunnen treffen. Denk aan registratie van allergieën, zodat hiermee rekening gehouden kan worden bij traktaties of lunches. Een ander voorbeeld is registratie van diabetes, zodat in geval van nood de juiste procedure kan worden gevolgd. Alles wat er met persoonsgegevens wordt gedaan, wordt in de wet verwerken genoemd. Verwerken is dus onder meer: online en offline persoonsgegevens verzamelen, kopiëren, opslaan, verspreiden, publiceren, delen én uitwisselen.*

### *2.3 Rollen*

*De Wet bescherming persoonsgegevens kent 3 belangrijke rollen. Te weten:*

- *De verantwoordelijke.*
  *De verantwoordelijke stelt vast welke persoonsgegevens er verwerkt worden én wat het doel is van die verwerking. Het gaat hier om de persoon of instantie die formeel en juridisch het initiatief neemt tot het verzamelen van persoonsgegevens en daarvoor ook verantwoordelijk is. In het basisonderwijs is dit vaak de directie of het bestuur van de rechtspersoon waar de school onder valt: het bevoegd gezag.*
- *De bewerker.*
  *De bewerker verwerkt de persoonsgegevens namens de verantwoordelijke. Dit is bijvoorbeeld een aanbieder van leermiddelen. De bewerker handelt in opdracht van de verantwoordelijke en mag alleen verwerkingen doen waarvoor hij uitdrukkelijk opdracht krijgt.*
- *De betrokkene.*
  *De betrokkene is de persoon over wie de persoonsgegevens gaan: in het basisonderwijs is dit de leerling. Als de betrokkene jonger dan 16 jaar is, dan mogen volgens de Wbp alleen de wettelijke vertegenwoordigers (ouders) beslissen over de gegevens van de betrokkene.*

### *2.4 Uitgangspunt van de wet*

*Uitgangspunt van de Wbp is dat het bevoegd gezag eindverantwoordelijk is voor de privacy van leerlingen. De verantwoordelijke is verplicht om volgens de wet te handelen en daarbij behoorlijk en zorgvuldig te werk gaan. De wet biedt scholen gelukkig genoeg ruimte om persoonsgegevens te gebruiken: binnen de kaders van de wet is voldoende mogelijk.*

### *2.5 Scholen zijn verantwoordelijk*

*Scholen hebben de regie op wat er gebeurt met de persoonsgegevens. Dit mag niet worden overgelaten aan een bewerker (leverancier). Die verantwoordelijkheid houdt ook in dat scholen ouders en leerlingen volledig moeten informeren over het gebruik van persoonsgegevens én hoe ouders gebruik kunnen maken van hun rechten. Dit kan bijvoorbeeld op basis van gegevens van leveranciers.*

Hier wordt o.a. mee bedoeld het gebruik van online software middels Basispoort, online dataopslag (Heutink MOO en Z-schijf) en de integratie met Parnassys.

### *2.6 Werken met persoonsgegevens:*

*Om persoonsgegevens te mogen verwerken kent de Wbp een aantal uitganspunten. Deze uitgangspunten gelden voor elke school en zijn samengevat in 5 vuistregels.*

1. *Doel,*
   *Persoonsgegevens worden altijd verzameld met een vooraf vastgesteld en concreet doel.*
2. *Doelbinding,*
   *Persoonsgegevens mogen alleen worden verwerkt om het vooraf vastgestelde doel te bereiken. Gegevens die daarmee niet in verband staan, mogen dus niet worden verzameld. Ook de juiste beveiligingsmaatregelen dragen eraan bij dat de gegevens niet voor een verkeerd doel kunnen worden gebruikt.*
3. *Grondslag,*
   *Persoonsgegevens mogen alleen verwerkt worden als de Wbp hier een grond voor noemt.*
4. *Dataminimalisatie,*
   *De hoeveelheid persoonsgegevens die de school verwerkt, moet redelijkerwijs nodig zijn om het doel te bereiken. De gegevens moeten in verhouding staan tot het doel ('proportioneel') en het doel kan niet met minder dan deze verzamelde gegevens worden bereikt ('subsidiair'). Het gaat er dus om dat scholen uitsluitend gegevens verzamelen die écht nodig zijn om het gestelde doel te bereiken.*
5. *Transparantie en rechten van de betrokkene,*
   *De betrokkene (dus: de leerling en/of zijn ouders) is vooraf in begrijpelijke taal geïnformeerd over wat er precies aan informatie wordt verwerkt en wat het doel daarvan is.*

### *2.7 Meldplicht Datalekken*

*Op 1 januari 2016 is de meldplicht datalekken ingegaan. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek ontdekken. En in sommige gevallen moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).*

*Organisaties die een datalek willen melden bij de Autoriteit Persoonsgegevens kunnen dat doen via het meldloket datalekken.*

*Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.*

*We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.*
*Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.*

*De Autoriteit Persoonsgegevens heeft beleidsregels opgesteld over de meldplicht datalekken. Deze beleidsregels zijn bedoeld om organisaties te helpen bij het bepalen of sprake is van een datalek dat zij moeten melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.*

*Bron: https://autoriteitpersoonsgegevens.nl/nl*

### 2.8 Wat betekent dit voor KPOA?

Dit betekent dat we transparant moeten zijn in wat er gebeurt met de gegevens van de leerlingen en we moeten ons bewust zijn van het feit dat we te maken hebben met gevoelige informatie en daar dan ook naar handelen. Dit houdt in:

- Inzicht hebben in de status van onze security
- Aanpassen van communicatie
- Bewustwording
- Aanpassen van gedrag

Begin 2016 hebben we een extern bedrijf een security test laten afnemen om inzicht te krijgen in de security van onze organisaties. De uitkomsten van deze test hebben wij geprioriteerd en in overleg met de betrokkene leveranciers besproken en opgelost.
Een gedeelte van de uitkomsten van deze testen zijn aandachtspunten voor de gebruikers.
De medewerkers van KPOA gaan niet goed om met de gegevens die vallen van de Wbp. Denk hierbij aan wachtwoord beleid, privé gebruik van het WiFi, gebruik e-mail, USB-sticks, lokaal opslaan van bestanden etc.

Dit alles betekent dat zowel de omgevingen technisch op orde moeten zijn, als wel de professionaliteit van onze medewerkers.

## 3. Communicatie

Privacy moet een vast onderdeel zijn van deKPOA scholen, schoolgidstekst en de website waarmee je ouders op de hoogte stelt dat er informatie wordt uitgewisseld met uitgevers om het onderwijsleerproces te bevorderen.

Een voorbeeld van zo'n tekst is:

*Wet Bescherming Persoonsgegevens*
*Binnen de school worden slechts de volgende persoonlijke gegevens verwerkt:*

- *Persoonsgegevens in relatie tot de wettelijke verplichtingen bij inschrijving van de leerling*
- *Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling*
- *Gegevens over de aard en verloop van het onderwijs, over de behaalde studieresultaten*
- *Gegevens met het oog op de organisatie van het onderwijs*
- *Gegevens ten behoeve van de begeleiding van de leerling*

*Bij de uitwisseling van (persoonlijke) gegevens met derden is uitgangspunt dat:*

- *Zoveel mogelijk gekozen wordt voor de uitwisseling van anonieme gegevens*
- *Persoonlijke gegevens slechts worden uitgewisseld met toestemming van de ouders/verzorgers*
- *Bij het ontbreken van toestemming van de ouders/verzorgers gebeurt dit op basis van het verenigbaarheid criterium uit de WBP. Daarbij gaat het om de belangen van de leerling in het kader van begeleiding, gezondheid en welzijn, waarbij slechts die gegevens mogen worden uitgewisseld die een relatie hebben met het doel van de oorspronkelijke registratie.*

Bovenstaand voorbeeld verwijst naar de communicatie tussen Parnassys, Basispoort en de uitgeverijen zoals Zwijsen.

# 4. Wachtwoord beleid

## 4.1 Het belang van correcte omgang met wachtwoorden

Wachtwoorden vormen een belangrijk aspect van de beveiliging van persoonlijke informatie over leerlingen, ouders en medewerkers van KPOA (vallen onder Wbp en worden vanaf nu "bijzondere gegevens" genoemd).
Wachtwoorden zorgen ervoor dat onbevoegden geen toegang kunnen krijgen tot de bijzondere gegevens van leerlingen, ouders en medewerkers.
Alle medewerkers van KPOA dienen een goed wachtwoord te kiezen en zijn verantwoordelijk voor de geheimhouding van hun wachtwoorden en inloggegevens.

## 4.2 Wachtwoorden

Wachtwoorden hebben een bepaalde sterkte nodig om het moeilijker te maken dat ze worden geraden. De sterkte van een wachtwoord wordt bepaald door de lengte, de complexiteit en de onvoorspelbaarheid. Zwakke wachtwoorden zijn vaak te kort, zijn te eenvoudig van samenstelling of zijn een eenvoudige toets combinatie. Hierdoor zijn ze makkelijk te raden. Medewerkers van KPOA dienen een sterk wachtwoord te gebruiken bij de verschillende programma's.

KPOA hanteert de volgende definitie van een sterk wachtwoord:
Een sterk wachtwoord is een wachtwoord dat minimaal bestaat uit 8 tekens, waaronder minimaal 1 hoofdletter, 1 cijfer en 1 symbool (bijvoorbeeld: !,@,#,$,%)

### 4.3 Programma's

Bij de volgende programma's zijn wachtwoorden van belang voor een beveiligde uitwisseling van gegevens.

| Programma | Directie | Leerkracht | ICT | Medewerker bestuursbureau | Bijzonderheden informatie |
|---|---|---|---|---|---|
| Parnassys | x | x | x | x | Bijzondere gegevens, NAW gegevens & onderwijskundige resultaten |
| Netwerk omgeving (Heutink) | x | x | x | x | Bijzondere gegevens van directie |
| Office365 | x | x | x | x | Bijzondere gegevens |
| AFAS | x | x | X | x | |
| MOO | | x | | | NAW gegevens |
| Basispoort | | x | x | | Naam en groep |
| Website | x | | x | x | Portretrecht |
| | | | | | |

4. Wachtwoord processen

Het verstrekken van een wachtwoord dient door de ICT-coördinator of directeur geregeld te worden of bij de beleidsmedewerker ICT of stafmedewerker aangevraagd te worden.

Bijvoorbeeld: Er komt een nieuwe medewerker in dienst. De ICT-coördinator of directeur vraagt een gebruikersaccount aan. Administratie maakt een nieuw account aan met een standaard tijdelijk wachtwoord, welke verstrekt wordt aan de nieuwe gebruiker. Dit tijdelijk wachtwoord moet de eerste keer dat het gebruikt wordt direct worden gewijzigd.

Gebruiker is leerkracht:

| | |
|---|---|
| Office365 | Beleidsmedewerker ICT |
| Parnassys | Administratie van de school |
| Netwerk & MOO | ICT-coördinator school |
| AFAS | Medewerker bestuursbureau |

Gebruiker is directeur:

| | |
|---|---|
| Office365 | Beleidsmedewerker ICT |
| Parnassys | Administratie van de school |
| Netwerk & MOO | ICT-coördinator school |
| AFAS | Medewerker bestuursbureau |

Bij veranderingen van functie, uittreding of bij mobiliteit moeten deze wijzigingen aan de bovengenoemde personen worden doorgegeven, zodat aanpassingen gedaan kunnen worden. De directie van de school is hiervoor verantwoordelijk

Bij uitdiensttreding zal het gebruikersaccount van Office 365 nog maximaal 1 maand actief blijven, waarna het account zal worden verwijderd.

Periodiek dient de school (via een vastgesteld format) een overzicht aan te leveren van de wijzigingen. In ieder geval bij de start van het schooljaar.

## 5. Digitale personeelsdossiers

KPOA heeft besloten om met ingang van 1 augustus 2016 gebruik te maken van de omgeving van AFAS. Het papieren personeelsdossier zoals dat soms nog aanwezig is op de school zal vanaf die datum niet meer worden aangevuld, maar kan wel worden geraadpleegd.

Al enige tijd is het bestuurskantoor van KPOA bezig met het digitaliseren van personeelsdossiers binnen het personeelsadministratiesysteem van AFAS. Vanuit het Stafbureau worden de documenten die nodig zijn voor een correcte salarisverwerking en voor een juiste opbouw van het personeelsdossier in het digitale systeem Personeelsdossier van AFAS gezet.

*Dit hoofdstuk zal in samenspraak met de beleidsmedewerker personeel nog verder worden aangevuld.*

## 6. Basispoort

In het huidige onderwijs wordt veelvuldig gebruik gemaakt van online methodesoftware van verschillende uitgeverijen. Om dit goed te laten werken is Stichting Basispoort ontstaan. Basispoort is een samenwerkingsverband tussen vier grote educatieve uitgeverijen en vier schoolleveranciers. Het doel is om “single sign on” te bieden voor de software van de aangesloten partners. Aangezien Heutink ICT het netwerk van KPOA beheert en tevens partner is van Basispoort, maken de scholen van KPOA gebruik van Basispoort. In bijlage 2 een verwijzing naar de website http://info.basispoort.nl/privacy ,waarin uitgelegd wordt hoe de privacy door Basispoort is geregeld.

### 6.1 Overdracht van informatie

De volgende informatie wordt door Basispoort uitgewisseld (bron: producten diensten overeenkomst basispoort):

*C. Categorieën en soorten persoonsgegevens*
*Omschrijving en opsomming categorieën Persoonsgegevens die gebruikt worden:*

- *van leerlingen: Basispoort ID (aangemaakt door Basispoort), voornaam, achternaam, tussenvoegsel, geboortedatum, leerlingkey, groepskey, groepsnaam, jaargroep, geslacht en BRIN;*
- *van Afgevaardigden en leerkrachten: Basispoort ID (aangemaakt door Basispoort), voornaam, achternaam, tussenvoegsel, geboortedatum, leerkrachtkey, groepskey, groepsnaam, jaargroep, geslacht, BRIN, e-mailadres.*
- *Van Scholen: Basispoort ID (aangemaakt door Basispoort), ASSU_nummer_RP, BRIN, schoolnaam en bezoekadres.*

## 7. Overstapservice Onderwijs (OSO)

KPOA maakt gebruik van Parnassys als leerling administratie systeem. In Parnassys zit privacy gevoelige informatie. Om de overstap van PO naar PO en PO naar VO soepel en vooral veilig te laten verlopen is de Overstapservice Onderwijs (OSO) ontwikkeld.
KPOA is voor het gebruik gecertificeerd. De digitale overdracht van gegevens gebeurt dus via OSO. Om dit mogelijk te maken zal er toestemming verleend moeten worden van de ouders van de betreffende leerling. Zij moeten inzage gehad hebben in het overstapdossier. Hiervoor dient door de ouder/verzorger altijd getekend te worden. Bij de overstap van PO naar VO zal dit gebeuren op het aanmeldformulier. Als een leerlingen wisselt van PO naar PO, dan zal de ouder/verzorger tekenen op een toestemmingsformulier waarmee ze toestemming geven voor de digitale overdracht van het overstapdossier (Bijlage 3).

## 8. Mobiele devices

Doordat KPOA mobiele devices beschikbaar stelt aan hun medewerkers is het belangrijk om afspraken te maken met betrekking tot het gebruik in verband met toegang tot “bijzondere gegevens”. Hiervoor is een gebruikersovereenkomst opgesteld, welke door de gebruiker ondertekend dient te worden. Zie hiervoor; “Notebook of Device”, bijlage 4.

*KPOA geeft in vol vertrouwen de medewerker de beschikking over een Mobiel device (laptop/device). Hierbij is KPOA niet verantwoordelijk voor oneigenlijk gebruik van de accounteigenaar.*

*Account eigenaar is verantwoordelijk voor veilig gebruik, dit houdt in:*

- *Er wordt gebruik gemaakt van een sterk wachtwoord of pincode als beveiliging bij het openen of opstarten van het device.*
- *Bij verlies of diefstal meldt de account eigenaar dit bij de directeur, welke melding zal maken bij de beleidsmedewerker ICT, zodat accounts geblokkeerd kunnen worden.*
- *Zorgen dat derden niet bij “Bijzondere gegevens” kunnen. (de inloggegevens worden vaak door de computer bewaard zodat snel inloggen zonder wachtwoord mogelijk is)*
- *Er geen porno / geweld etc. aanwezig is op het device.*
- *Geen illegale films, muziek of software aanwezig is op het device.*
- *Er geen lokale bestanden of bestanden die vallen onder de Wbp aanwezig zijn op het device.*
- *Verdere aanvullingen zijn opgenomen in de gebruikersovereenkomst “mobiele devices” zie bijlage.*

*De directeur is verantwoordelijk voor:*

- *Bij vermoeden van oneigenlijk gebruik, wordt de account eigenaar aangesproken door de directeur/CVB. De directeur / CVB heeft het recht om hierbij inzage te hebben in de gebruiks history.*
- *Verlies of diefstal wordt door de directeur aan de beleidsmedewerker ICT gemeld.*
- *De directeur is verantwoordelijk voor de politieaangifte bij verlies of diefstal.*

*De beleidsmedewerker ICT is verantwoordelijk voor:*

- *Het laten ondertekenen van een gebruikersovereenkomst door de accounteigenaar.*
- *De gebruikersovereenkomsten archiveren in insite.*
- *Verlies of diefstal van het device. De beleidsmedewerker ICT maakt melding van het datalek (in overleg met het CvB) indien van toepassing.*
- *Er zal gekeken worden of het device te vinden is via “Mijn apparaat zoeken” (link).*
- *Inname van het device na het verlopen van de afschrijvingstermijn of uitdiensttreding.*

## 9. Sociale Media

Onder sociale media verstaan we;

“Sociale media is een verzamelbegrip voor online platforms waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen”.
(Bron: https://nl.wikipedia.org/wiki/Sociale_media)

In de praktijk betekent dit dat ouders toestemming aan de school moeten geven voor het gebruik van foto’s en filmpjes op de sociale mediakanalen van de school. Dit kan zijn;

- Website
- Youtube
- Twitter
- Facebook
- Etc…

De school zal dit bij de aanmelding van een leerling vragen via het aanmeldformulier. Door te tekenen geven ouders toestemming voor het gebruik van foto’s en filmpjes van hun kind op de boven genoemde sociale media. Tevens verplicht de school zich hiermee tot het jaarlijks benoemen van de overeenkomst mocht de ouder dit willen wijzigen. Dit kan bijvoorbeeld via de nieuwsbrief of de schoolgids.

Op het moment dat een ouder geen toestemming geeft, zal de school ervoor zorgdragen dat de betreffende leerling of leerlingen niet herkenbaar in beeld zullen zijn.

### 9.1 Protocol sociale media

Hiervoor verwijzen we naar het Protocol sociale media / internet / e-mail

Sociale media is de verzamelnaam voor alle toepassingen op internet waarmee het mogelijk is met elkaar te communiceren en informatie te delen. Bij sociale media wordt de content, de informatie die beschikbaar is, bepaald door de gebruikers. Belangrijk kenmerk van sociale media is dat informatie snel verspreid kan worden. Sociale media worden ingezet voor kennisontwikkeling, kennisdeling door gebruik te maken van de kennis van een grote groep, voor discussie en nieuwsverspreiding.

KPOA gaat ervan uit dat bij het gebruik van digitale communicatiemiddelen de algemeen geldende en gebruikelijke gedragsregels worden gehanteerd. Om het gebruik van internet, e-mail en sociale media op een gewenste manier in te zetten binnen het onderwijs en de organisatie zijn er richtlijnen opgesteld met als doel om een handreiking te bieden en om duidelijkheid te geven over het gebruik van digitale communicatiemiddelen en publicatie in media.

Uitgangspunt:

- Het digitale gedrag op sociale media wijkt niet af van de gebruikelijke gedragsregels binnen de stichting / school.
- Professionals weten hoe zij verstandig om moeten gaan met sociale media.
- Er zijn verschillen in kennis en ervaringen met het gebruik van sociale media bij medewerkers.

Richtlijnen gebruik sociale media:

- Het gedrag van medewerkers op e-mail, Facebook, Youtube, Twitter etc. wijkt niet af van wat in de klas, op school of binnen de stichting gebruikelijk is.
- Medewerkers delen kennis en andere waardevolle informatie op het gebied van onderwijs en onderwijs gerelateerde onderwerpen.
- Bij onderwijs of onderwijs gerelateerde onderwerpen maken medewerkers duidelijk of zij op persoonlijke titel of namens de school / de organisatie publiceren.
- Medewerkers hanteren bij publiceren van informatie op sociale media altijd de wet op de privacy.
- Medewerkers gebruiken sociale media als communicatiemiddel en niet als discussiemiddel met leerlingen / ouders / collegae / leidinggevenden.
- Medewerkers zijn persoonlijk verantwoordelijk voor hetgeen zij publiceren.
- Medewerkers maken hun bronnen kenbaar.
- Medewerkers weten dat publicaties op sociale media altijd vindbaar zijn.
- Medewerkers gebruiken in werktijd geen privé gerelateerde social media (Whats-App, facebook e.d.) en gebruiken/belasten hiervoor ook niet het netwerk van de school (WiFi).
  Bij twijfel over een publicatie of over de raakvlakken met KPOA of een onderdeel van KPOA zoeken medewerkers vooraf contact met hun leidinggevende.
- KPOA, de school zorgt voor een veilig gebruik van digitale middelen (veilige digitale leeromgeving) en communiceert met leerlingen, ouders , studenten / stagiaires, medewerkers en derden hoe zij dit doet.
- Gebruik alleen logo's, beeldmateriaal of muziek als schriftelijke toestemming is verleend door de eigenaar.
- Gebruik alleen foto's als schriftelijke toestemming is verleend door degene die erop staat of verantwoordelijk is voor diegene. (zoals de ouders van een leerling.)

KPOA heeft een verantwoordelijkheid als het gaat om de veiligheid van leerlingen, ouders, studenten / stagiaires en medewerkers. Dat begint met duidelijke en gecommuniceerde normen en waarden en de handhaving daarvan. Dit protocol geldt voor alle gebruikers van de internetfaciliteiten die door KPOA worden geboden. Naast gebruikers van de netwerken in schoollocaties zijn deze regels ook van toepassing op gebruikers die thuis of elders gebruik maken van een e-mailadres van de school of een inlog op het schoolnetwerk.

Medewerkers mogen internet en e-mail incidenteel en kortstondig voor privédoeleinden gebruiken. zowel intern als extern, voor zover hieraan geen bijzondere kosten verbonden zijn, als dit niet storend is voor de dagelijkse werkzaamheden.

De infrastructuur voor elektronische communicatie kent een eigen vorm van kwetsbaarheid en een eigen vorm van beveiliging. Deze vraagt om speciale aandacht op tenminste de volgende punten:

- User-identificatie (inlognaam) en wachtwoord zijn persoonsgebonden en mogen niet aan anderen worden doorgegeven. Het downloaden van software en applicaties is niet toegestaan, tenzij vooraf toestemming is verleend door de leidinggevende. Deze toestemming wordt alleen verleend als wordt voldaan aan de geldende rechten en (eventuele) licenties worden betaald, mits deze ook op de lijst van KPOA staat.
- Vertrouwelijke gegevens mogen niet zonder toestemming naar derden worden verstuurd.
- Onbedoelde inbreuk op beveiliging, van binnenuit of van buitenaf, wordt aan de Beleidsmedewerker ICT gemeld.

E-mail

Om het gebruik van e-mail in goede banen te leiden, het gezicht van KPOA en de scholen naar buiten te beschermen gelden de volgende regels:

- Een bericht verstuurd vanaf het school e-mailadres wordt door de ontvanger gezien als een e-mail van KPOA. Houd berichten kort en zakelijk en gebruik correct Nederlands, zoals dat ook in schriftelijke communicatie gebruikelijk is.
- Het versturen van een privé bericht aan grote groepen mensen is toegestaan als deze hiervoor toestemming hebben gegeven.
- Het versturen van een bericht naar alle medewerkers van KPOA mag worden uitgevoerd, als er duidelijk een algemeen onderwijsbelang is gediend en na overleg met leidinggevende / het stafbureau.
- Het doorsturen van email van KPOA naar privé accounts is niet toegestaan.
- Het is niet toegestaan om werk gerelateerde emails te versturen vanuit een mailbox anders dan die door de KPOA is gefaciliteerd.

Controle
Om veiligheidsredenen wordt al het inkomende en uitgaande verkeer van KPOA netwerk vastgelegd op een online back-up zodat wanneer er iets misgaat, informatie weer terug geplaatst kan worden.

- Binnenkomend internet- en e-mailverkeer wordt zo goed mogelijk gecontroleerd op virussen.
- KPOA kan het recht tot gebruik van (een deel van) internet toestaan, maar ook weer intrekken.
- Het College van Bestuur kan de systeembeheerder opdracht geven de back-up en bestanden van de server te bekijken.
- Controleren, alsmede openen van e-mail, ten behoeve van het opsporen van onrechtmatig gedrag van de werknemer, is in opdracht van het College van Bestuur toegestaan als er sprake is van een vermoeden of een redelijke verdenking van ongeoorloofd handelen.

Gebruik mobiel
Medewerkers van KPOA mogen op hun mobiele apparaat gebruik maken van school gerelateerde informatie als mail, parro app. enz. De medewerker wordt hierdoor verplicht om een pincode op het apparaat (telefoon / tablet / laptop) in te stellen. Daarnaast mag de gebruiker dit apparaat niet meer uitlenen aan derde.

Streaming video /muziek
Spotify en netflix zijn voorbeelden van programma's waar muziek en films worden gedeeld. Medewerkers die hier een account hebben mogen dit account niet gebruiken op de school. Het is de medewerker dus niet toegestaan films en muziek te delen binnen de school.

# 10. Externen

KPOA verleent geen toegang tot zijn administratiesysteem (Parnassys) aan “derden”, welke niet voor onbepaalde tijd bij KPOA verbonden zijn. Indien een medewerker voor een bepaalde periode voor zijn werk toegang heeft is het aan de directeur om te beoordelen of deze medewerker toegang krijgt en te zorgen dat de toegang ook gedeactiveerd wordt bij het einde van deze bepaalde periode.

## 10.1 Foto’s en video door derden

Als school heb je regelmatig te maken met ouders in de school. Veel van de ouders maken tegenwoordig gebruik van een smartphone om actuele activiteiten van hun eigen kinderen (en daarmee vaak ook dat van anderen) te verslaan. Ze maken foto’s en of video’s, welke met regelmaat op de sociale media terecht komen. Wie is hier nu verantwoordelijk voor? José van Snek, juridisch adviseur van Voss Abb vertelt hierover het volgende;

*“Wie op een foto afgebeeld staat, kan zich soms beroepen op het zogenaamde 'portretrecht'. Dat houdt in dat in sommige gevallen de foto niet mag worden verwerkt/gepubliceerd zonder de toestemming van degene die op de foto staat. Van een 'portret' is sprake als iemand herkenbaar is afgebeeld. Als een portret in opdracht is gemaakt, dan is voor publicatie zonder meer toestemming van de afgebeelde persoon (in dit geval de ouders) nodig. De maker van het portret heeft wel het auteursrecht, maar ook hij mag het portret niet publiceren zonder toestemming van de geportretteerde. Als een portret niet in opdracht is gemaakt, mag het in beginsel vrij gepubliceerd worden. Dit ligt anders als de afgebeelde persoon een 'redelijk belang' heeft om zich tegen publicatie van zijn portret te verzetten. Vaak gaat het dan om een privacybelang. Het is meestal wel toegestaan foto's te maken in de openbare ruimte en die te publiceren, zonder dat aan personen die toevallig in beeld komen toestemming hoeft te worden gevraagd. De fotograaf moet zich wel rekenschap geven van de belangen die deze toevallig gefotografeerde mensen zouden kunnen hebben. Een school of schoolplein is echter geen openbare ruimte.*

*Kortom: als ouders foto’s maken van de leerlingen tijdens een evenement op school of tijdens schooltijd, dan mogen deze ouders de foto’s niet verwerken (bijvoorbeeld plaatsen op een facebookpagina) zonder dat de ouders van de leerlingen die op de foto staan hiervoor hun toestemming hebben gegeven. Het is verstandig om de ouders hier bij aanvang van de activiteit op te wijzen. De school kan eventueel voorstellen dat zij foto’s van de activiteiten maakt en verspreid onder de ouders waarbij de school leerlingen onzichtbaar kan maken indien de betreffende ouders hebben aangegeven dat zij niet wensen dat hun kind door de school wordt gefotografeerd.*

*Het is verstandig om hier beleid op te maken, zodat alle ouders, werknemers en eventueel leerlingen op voorhand op de hoogte zijn van de wijze waarop hier binnen de school mee om wordt gegaan."*

Gezien het feit dat je dus als schoolorganisatie verantwoordelijk bent voor de foto's en filmpjes die gemaakt en verspreid worden door ouders is het aan te raden de verantwoordelijkheid duidelijk in de schoolgids op te nemen.

Op te nemen in de schoolgids:
Het is ouders/verzorgers niet toegestaan om foto's en filmpjes van kinderen, anders dan hun eigen kind op sociale media te verspreiden. De school zal tijdens evenementen zelf foto's en video's maken en deze verspreiden via de eigen sociale media (website, facebook, twitter), waarbij er rekening gehouden wordt met de privacy rechten van het kind.

## 11. Netwerkbeheer

Stichting KPOA heeft in 2015 in gezamenlijkheid met Stichting Meerkring de ICT infrastructuur Europees aanbesteed. In de selectiecriteria van de aanbesteding is veel aandacht geweest voor een veilige omgeving. Begin 2016 hebben daarom security testen plaats gevonden om te testen of de geleverde omgeving van Heutink-ICT voldoet aan de door ons gestelde eisen. Enkele aanpassingen worden nog gemaakt maar de basis veiligheid van de netwerkomgevingen op school is op orde.

Voor directie, beheer, leerkrachten, ib, leerlingen en eventueel gasten is er een persoonlijke omgeving, welke beschermd is met een sterk wachtwoord.

Indien een medeweker op meerdere locaties werkt en gebruik maakt van een laptop, dan is het mogelijk om wel altijd bij je bestanden te kunnen.

Leerlingen hebben een eigen afgesloten omgeving op het netwerk. Zij loggen in met standaard gebruikersnamen en wachtwoorden passend bij de groepen. Het is voor leerlingen niet toegestaan om (zonder toezicht van de leerkracht) van een andere omgeving dan “leerling” gebruik te maken.

Gasten kunnen ook een plek krijgen binnen het netwerk. Deze omgeving is volledig afgeschermd. Het is niet mogelijk om via deze omgeving bij de documenten van de school te komen.

## 12. Draadloos netwerk

Het draadloos netwerk van Meerkring en KPOA is opgebouwd uit de volgende SSID's met elk hun eigen doel dit om de privacy en veiligheid van het gehele netwerk te kunnen borgen.

| SSID | Gebruiker | Bijzonderheden |
|---|---|---|
| Naamschool-GAST | Ouders, logopedist, GGD | Open tussen 7.00 en 22.00 uur, verloop van wachtwoord. |
| Eduroam | Medewerkers & leerlingen | Inlog gekoppeld aan indiensttreding |
| 3000-Brin | Beheerde werkplekken | Niet toegankelijk voor gebruik anders dan voor Heutink ICT |

Er is bewust gekozen voor deze indeling, omdat op deze manier het wachtwoordwijzigingen simpel zijn door te voeren bij vermoeden van misbruik. Bij vermoeden van misbruik heeft KPOA het recht om vanuit de online WiFi omgeving een rapportage op te vragen van de locatie waar er een vermoeden is van misbruik.

Aangezien Eduroam een persoonlijk WiFi account is is het niet toegestaan om het wachtwoord aan externen te overhandigen/delen.

Het gebruik van WiFi is voor onderwijsdoeleinde bedoelt en niet voor privé gebruik (Whatsapp, internet op mobiel) ed moeten dus mede vanwege security /virussen tot een minimum worden beperkt.

Aandachtspunten:

- De WiFi code voor gasten is niet zichtbaar aanwezig in de school.
- Delen van WiFi codes is niet toegestaan.

## Bijlage 1

**Kennisnet publicatie Privacy_in_10_stappen**

Zie hiervoor:

https://www.kennisnet.nl/artikel/privacy-op-school-in-10-stappen/

## Bijlage 2

### Privacyverklaring Basispoort

*In deze privacyverklaring vindt u de belangrijkste informatie over het gebruik van persoonsgegevens door de Stichting Basispoort.*

*Waarom deze gebruikersovereenkomst?*
*De Stichting Basispoort maakt het gebruik van digitale leermiddelen in het primair onderwijs eenvoudiger door één eenvoudige en uniforme inlogprocedure. Ten behoeve van deze inlogprocedure worden persoonsgegevens verwerkt. Wij vinden het belangrijk om uiterst zorgvuldig met persoonsgegevens om te gaan en u duidelijk te informeren over de wijze waarop wij persoonsgegevens gebruiken.*

*Wat is Basispoort?*
*De kern van de dienstverlening van Basispoort is dat in opdracht van de school aan leerkrachten en leerlingen toegang wordt verleend tot online educatief materiaal door middel van één uniforme inlogprocedure. In de Product- en Dienstenovereenkomst wordt deze dienst de Basispoortdienst genoemd. Dankzij deze Basispoortdienst hoeven leerlingen of leerkrachten niet voor iedere aanbieder van online educatief materiaal apart in te loggen met verschillende inloggegevens en –procedures.*
*De Basispoortdienst wordt door Basispoort geleverd aan de hand van de gegevens die door een school (vaak via een leerlingadministratiesysteem) aan Basispoort worden verstrekt. Wanneer een leerling of leerkracht op basis van deze gegevens inlogt via Basispoort, kan een aanbieder van leermiddelen vaststellen wie gebruik maakt van zijn online educatief materiaal. Daardoor kan een leermiddel bijvoorbeeld voor een leerkracht de leerresultaten van zijn leerlingen inzichtelijk maken. Het is voor leerlingen en leerkrachten uitsluitend mogelijk om via de Basispoortdienst in te loggen op online educatief materiaal waarvoor licenties zijn geactiveerd. Een overzicht van geactiveerde licenties kan per groep worden geraadpleegd via het beheerscherm. Er worden vanuit Basispoort dus geen gegevens doorgegeven aan uitgevers waarmee een school geen klantrelatie heeft, omdat geen licenties zijn geactiveerd. De rol van Basispoort is bovendien beperkt tot het faciliteren van de inlogprocedure: er worden door Basispoort bijvoorbeeld geen leer- of toetsresultaten opgeslagen of uitgewisseld.*

*Educatieve uitgeverijen die thans participeren binnen Basispoort zijn lid van de brancheorganisatie GEU en conformeren zich aan het privacyreglement van de GEU.*

*Verantwoordelijkheid van de school*
*Basispoort heeft het 'Convenant Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen' onderschreven. In dit convenant is tussen aanbieders en de onderwijssectorraden vastgelegd dat een school in juridische zin de 'verantwoordelijke' is voor de verwerking van persoonsgegevens. Daardoor hebben en houden scholen zeggenschap over de gegevens die binnen leermiddelen worden verwerkt. Basispoort is een 'bewerker', die uitvoering geeft aan de opdracht van een school. Daarbij zal Basispoort altijd zorg dragen voor een passende beveiliging van persoonsgegevens. Het feit dat de school verantwoordelijk is voor de gegevensverwerking, brengt voor haar belangrijke verplichtingen met zich mee. Meer informatie hierover treft u op de websites van de PO-Raad en Kennisnet.*

*Bewerkersovereenkomst en beveiliging*
*In de Bewerkersovereenkomst van Basispoort wordt tussen scholen en Basispoort vastgelegd welke opdracht wordt gegeven tot verzameling en verwerking van persoonsgegevens bij het gebruik van de Basispoortdienst. Graag wijzen wij u op het volgende:*

- *Basispoort gebruikt de 'Model Bewerkersovereenkomst', die onderdeel uitmaakt van het 'Convenant Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen'.*
- *De Bewerkersovereenkomst vormt onderdeel van de Product- en Dienstenovereenkomst die op het gebruik van de Basispoortdienst van toepassing is.*
- *In onze Privacy Bijsluiter leest u voor welke doeleinden welke persoonsgegevens in opdracht van de school worden verwerkt.*
- *Basispoort treft technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. Deze maatregelen garanderen een passend beveiligingsniveau. Het gebruik van de inlogfunctionaliteit van de Basispoortdienst verloopt bijvoorbeeld via een beveiligde https-verbinding, waarbij gegevens worden versleuteld. In de bijlage met technische en organisatorische beveiligingsmaatregelen treft u als school een overzicht welke beveiligingsmaatregelen Basispoort heeft getroffen.*

*Download de Product- en Dienstenovereenkomst, Bewerkersovereenkomst en Privacy Bijsluiter.*

*Kennisgeving, verbetering en verwijdering van persoonsgegevens*
*Op grond van de wettelijke rolverdeling en het 'Convenant Digitale Onderwijsmiddelen en Privacy - Leermiddelen en Toetsen' moeten scholen (ouders van) leerlingen informeren over het gebruik van digitale leermiddelen en Basispoort. Betrokkenen kunnen via de school gebruikmaken van hun wettelijke rechten. Voor de uitoefening van deze rechten dienen betrokkenen zich te wenden tot de school.*

*Verwerking van gegevens van ICT-coördinatoren van scholen*
*Voor de Basispoortdienst treedt Basispoort in opdracht van een school op als bewerker. Basispoort verwerkt daarnaast persoonsgegevens van afgevaardigden (ICT-coördinatoren) van scholen voor relatiebeheer. Daardoor kan Basispoort deze afgevaardigden zelfstandig informeren over de ontwikkelingen van Basispoort, wijzigingen in dienstverlening, wijzigingen in dienstverleningsvoorwaarden en wijzigingen op de website van Basispoort. Deze verwerkingen zijn aangemeld bij de Autoriteit Persoonsgegevens onder meldingsnummer M1538319.*

*Gebruik van cookies*
*In het kader van de dienst waarvoor Basispoort wordt ingeschakeld, plaatst Basispoort uitsluitend zogenaamde 'functionele cookies' op de computer van de gebruiker.*
*Hiervoor is op grond van de Telecommunicatiewet geen aanvullende toestemming vereist.*
*Alleen op de website http://info.basispoort.nl plaatst Basispoort cookies voor het gebruik van Google Analytics. Binnen de Basispoortdienst wordt hiervan geen gebruik gemaakt.*

*Vragen*
*Heeft u verdere vragen of opmerkingen over de bescherming van persoonsgegevens? Neem dan gerust contact op met info@basispoort.nl. Wij zullen uw vragen zo spoedig mogelijk beantwoorden.*

*Kan deze privacyverklaring worden gewijzigd?*
*Het kan voorkomen dat deze Privacyverklaring, Privacy Bijsluiters of de bewerkersovereenkomst in de toekomst wordt uitgebreid of gewijzigd. Alle wijzigingen worden op deze website gepubliceerd. Deze privacyverklaring is voor het laatst gewijzigd op 1 december 2015.*

## Bijlage 3

**Toestemmingsformulier OSO**

Ouder(s) / verzorger(s) hebben inzage gekregen in het overstapdossier van:

……(naam kind)

En gaan akkoord met de digitale verzending naar

……(naam school)

Datum:

……

Naam & handtekening ouder(s) / verzorger(s)

……

……

Naam & handtekening vanuit de school

……

……

## Bijlage 4

Gebruikersovereenkomst Mobiele Telefonie en/of Device (versie 2016-06-24)

De werkgever: Stichting voor Katholiek Primair Onderwijs Amersfoort e.o.

En de werknemer:_____

Geboortedatum: _____

Adres: _____

Verklaren dat zij een gebruikersovereenkomst mobiele telefonie en/of device voor onbepaalde duur zijn aangegaan, in aanmerking nemende dat:

- Werkgever aan werknemer een mobiele telefoon en/of device (hierna: de apparatuur) heeft verstrekt ten behoeve van de uitoefening van de werkzaamheden van de dienstbetrekking;
- De apparatuur eigendom is van werkgever en in bruikleen wordt gegeven aan werknemer;
- Het telefoonnummer is eigendom van de werkgever. Werknemer mag in overleg het telefoonnummer met het contract overnemen. Abonnementskosten zijn daarna voor rekening van werknemer.
- Deze overeenkomst de nadere gebruiksvoorwaarden bepaalt waaronder werknemer de apparatuur kan gebruiken;
- Door acceptatie aanvaardt werknemer alle voorwaarden van deze overeenkomst.

### 1. Aard en uitvoering telefonie

Het type apparatuur kan door de medewerker zelf worden uitgekozen. Contracten kunnen alleen worden afgenomen via Reitsma Telecom. Abonnementen worden afgesloten binnen de raamovereenkomst die KPOA bij Reitsma heeft vastgelegd. Deze telefoon zal vanaf aanschaf minimaal 3 jaar gebruikt worden.

Gekozen toestelmerk: _____
Type: _____
Telefoonnr: _____

## 2. Aard en uitvoering device

Werkgever en werknemer verklaren tevens dat zij een gebruikersovereenkomst voor onbepaalde duur zijn aangegaan voor een Device. Dit device zal vanaf aanschaf minimaal 3 jaar gebruikt worden.

Gekozen apparaat: _ Ipad / Netbook / Laptop *___
Serienummer: _S/N_____
Aanschafjaar: _____

### a. Inleveren device

De gebruiker zal ervoor zorg dragen dat persoonlijke wachtwoorden en persoonlijke bestanden van zakelijk / onderwijs belang (zoals e-mail en agenda's) tijdig aan KPOA worden overgedragen, en dat verplichtingen (abonnementen op nieuwsgroepen, externe login accounts e.d.) worden opgezegd of overgedragen.

## 3. Rechten en plichten van werknemer

- Werknemer verklaart de apparatuur in goede staat te hebben ontvangen en zal deze niet aan derden ter beschikking stellen, verpanden noch op enige andere wijze vervreemden.
- Werknemer zal binnen twee werkdagen na aflevering van de in bruikleen gegeven goederen controleren of deze correct functioneren. Bij niet of onjuist functioneren van de in bruikleen gegeven goederen is werknemer gehouden dit onmiddellijk bij de interne contactpersoon van het bestuursbureau te melden.
- Werknemer is verantwoordelijk voor het in goede en representatieve staat houden van de apparatuur.
- Val en stoot schade is voor rekening van de werknemer.
- Het is werknemer verboden de apparatuur te gebruiken voor activiteiten die in strijd zijn met de doelstellingen of het imago van werkgever kunnen schaden.

## 4. Termijn van gebruik, beëindiging dienstverband en functieverandering

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

Bij einde van het abonnement, of bij verlengen van het abonnement wordt het oude toestel ingeleverd of tegen restwaarde overgenomen.
De werkgever is bevoegd de bruikleenovereenkomst tussentijds en zonder enige opzegtermijn op te zeggen en van werknemer de onmiddellijke teruggave van de in bruikleen gegeven goederen te verlangen indien werknemer de in bruikleen gegeven goederen verwaarloost, misbruikt, voor een ander doel gebruikt dan waarvoor deze bestemd is of als de werknemer op enigerlei andere wijze in strijd handelt met de bepalingen van deze overeenkomst, voor zover hiervan niet uitdrukkelijk in de onderhavige overeenkomst is afgeweken.

**5. Diefstal en beschadiging**

- Werknemer dient alle zorgvuldigheid in acht te nemen ter voorkoming van beschadiging, diefstal of verlies van de apparatuur.
- In geval van schade of diefstal van de apparatuur is werknemer verplicht dit zo spoedig mogelijk bij werkgever te melden. Werknemer dient verder het gebruik onmiddellijk te laten blokkeren via de interne contactpersoon van het bestuursbureau. Indien dit gebeurt in het weekend dient de werknemer zelf contact op te nemen met de provider voor het blokkeren van de simkaart. Vervolgens dient de werknemer de eerstvolgende werkdag contact op te nemen met de interne contactpersoon van het bestuursbureau. Als contractant draagt werkgever het risico voor misbruik na diefstal, mits aan het hiervoor gestelde is voldaan.
- Werknemer kan aansprakelijk worden gesteld voor schade aan de apparatuur ontstaan door verwijtbare nalatigheid of onachtzaamheid.

**6. Telefoongedrag**

- Van de werknemer wordt verantwoordelijk, professioneel en integer handelen verwacht.
- Privé kosten buiten de bundel worden in rekening gebracht en verrekend met het salaris.

**7. Bewustheid**

- Door ondertekening van deze overeenkomst verklaart werknemer dat hij gevolgen van deze overeenkomst heeft begrepen en zich daarmee akkoord verklaart.

Aldus overeengekomen en getekend te Amersfoort,

| | |
|---|---|
| Stichting voor Katholiek Primair Onderwijs Amersfoort e.o. | Naam werknemer: |
| | _____ |
| Handtekening werkgever: | Handtekening werknemer: |
| _____ | _____ |

N.B. Door ondertekening van deze gebruikersovereenkomst komen (evt.) voorgaande exemplaren te vervallen.

**Bijlage 5**

Flyer voor de school

**Bijlage 6**

Flyer voor leerkrachten

## Bijlage 7

Geaccordeerde software lijst (niet in de lijst dan eerst check)
www.Privacyconvenant.nl lijst met leveranciers

**A**

Ars Scribendi Uitgeverij B.V. *

**B**
Basisacademie B.V.
Bazalt Educatieve Uitgaven
BeatsNbits *
Blink *
BOLAS
Boom uitgevers / Uitgeverij Edu'Actief *
Boom uitgevers Amsterdam *
Bordfolio
Briter
Bureau ICE *

**C**
Cito ^
Codename Future *

**D**
De Rolf groep °
Diataal B.V.
DigiDUIF ^
Digiloket B.V. ^
Dotcomschool ^
Driestar Educatief ^
Digikeuzebord
Drillster B.V.

**E**
Eisma Edumedia *
EXOVA

**F**

**G**
Gynzy

**H**
Heutink ICT °
Heutink Primair Onderwijs BV °

**I**
Iddink Voortgezet Onderwijs bv °
Instruct
Intertaal *

**J**
Jongbloed Educatief *

**K**
Kennisnet
Koninklijke Van Gorcum *

**L**
LearningStone

**M**
Magnaview ^
MaxClass
Mijnschoolinfo ^
MIEGROEP Automatisering

**N**
Noordhoff Uitgevers *

**O**
Onlineklas
OpenEdu

**P**
ParnasSys *
Pearson *
Peppels B.V.

**Q**

**R**
RealOpen IT
Reinders Oisterwijk BV °
Rovict B.V. ^
RTTI-online B.V. ^

**S**
Safe School
Schoolmaster BV ^
Schoolplanner
SchouderCom
Skool
SLB Diensten B.V.
Slim
SnapIT ^
SOMtoday b.v. ^
Stichting Basispoort
Studio Krok B.V.
SWIS Suite, Praktikon

**T**
Thiememeulenhoff *
Tumult *

**U**
Uitgever Essener *
Uitgever Zwijsen *
Uitgeverij Betelgeuze *
Uitgeverij Deviant b.v. *
Uitgeverij Malmberg BV *
Unilogic BV ^

**V**

Van Dijk Educatie bv °
Van Dijk Educatie, Digitaal Leren ^
Van Tricht uitgeverij *
Visiria Uitgeversmaatschappij *
VO-digitaal

**W**

**X**

**Y**

**Z**