Privacy-protocol

Stichting OPONOA
Borculo
April 2017

Status: vastgesteld door CvB

Inhoud

Samenvatting

Met de invoering van de Europese wet op de privacy moeten we voor wat betreft dit onderwerp even de puntjes op de i zetten. Niet-naleving van de wet kan forse straffen opleveren.

Op onze scholen wordt gewerkt met persoonlijke gegevens (leerlinggegevens). Om die op te mogen slaan, moet het doel daarvan voldoende duidelijk gemaakt worden aan de betrokkenen (voor kinderen jonger dan 16 zijn dat de ouders). De reden voor de opslag moet voldoen aan een of meer van de volgende regels:

- **Doel**: Er is een vooraf gesteld concreet doel en de betrokkenen kunnen dit verifiëren.
- **Doelbinding**: Gegevens mogen alleen gebruikt worden voor het doel waarvoor ze zijn verzameld
- **Grondslag**: Voor het onderwijs gelden wettelijke grondslagen om persoonsgegevens op te mogen opslaan. Alleen vanwege deze grondslagen mogen gegevens worden geregistreerd.
- **Dataminimalisatie**: Er mogen niet meer gegevens worden vastgelegd dan nodig is om het doel te bereiken.
- **Transparantie**: Betrokkene heeft recht op inzage en eventuele correctie.

Wanneer leerlinggegevens worden doorgespeeld aan derden (uitgeverijen), dient hiervoor een bewerkersovereenkomst te worden afgesloten waarin wordt bepaald dat de bewerker de gegevens niet voor zichzelf mag gebruiken.

Ouders hebben recht om te weten waarvoor de geregistreerde gegevens worden gebruikt, zij hebben inzage, kunnen correctie verlangen of verwijdering van gegevens die niet langer nodig zijn.

De (G)MR heeft een adviserende rol, gevraagd of ongevraagd bij het vaststellen van dit protocol.

Zonder toestemming van ouders mag een school geen beeld- of geluidsopnames van leerlingen openbaar maken. Jaarlijks moet van ouders aandacht voor en recht op herroeping van deze toestemming worden gegeven.

Voor gebruik van sociale media beschikt OPONOA over een apart protocol: “Modelprotocol Sociale Media”, waarvoor de GMR in november 2013 haar instemming heeft gegeven.

Bij overstap naar een andere school worden door de school de wettelijk verplichte gegevens aangeleverd plus gegevens betreffende het leren van het kind. Dit gebeurt via een door de overheid in het leven geroepen, beveiligd platform: OSO.

Omdat scholen persoonlijke gegevens opslaan, moet er alles aan gedaan worden om te voorkomen dat deze gegevens openbaar worden: beveiliging. Het is belangrijk dat medewerkers niet meer te zien krijgen dan wat zij werkelijk nodig hebben. Speciale aandacht is er voor de zeer gevoelige informatie.

Gegevens uit de leerlingenadministratie dienen verwijderd te worden nadat de leerling 5 jaar van school is, leerlingendossiers worden 2 jaar bewaard. Uitzondering: bij doorverwijzing naar SBO is de bewaartermijn 3 jaar.

Om de gegevens voldoende te kunnen beveiligen, is het noodzakelijk dat gebruikers goed omgaan met de beveiligingsregels t.a.v. inloggen, wachtwoorden, afsluiten/”locken” van de computer etc.

Oude apparatuur mag alleen worden afgevoerd als privacygevoelige data daar vakkundig van is verwijderd.

Voor vertrekkende leerkrachten moet de toegang tot vertrouwelijke gegevens worden geblokkeerd.

Bij een datalek moet worden beoordeeld of er nadelige gevolgen zijn te verwachten voor de betrokkene(n). Zo ja, dan moet het lek binnen twee dagen worden gemeld bij de Autoriteit Persoonsgegevens. Een datalek kan erg vervelende gevolgen hebben, niet alleen voor de betrokkenen, maar ook voor de school en de stichting vanwege de negatieve publiciteit en de eventuele boete die zal worden uitgedeeld.

Er wordt aanbevolen om een functionaris voor de gegevensbescherming aan te stellen, die toezicht houdt op naleving van de protocollen, klachten behandelt en indien nodig contact onderhoudt met de Autoriteit Persoonsgegevens.

Het bevoegd gezag van de school is verantwoordelijk, maar de medewerkers dienen de regels na te leven.

Het is verstandig om regelmatig, bijvoorbeeld eenmaal per jaar, de “Checklist privacy” te doorlopen.

1. Aanleiding

Privacy is de laatste tijd een erg “hot” onderwerp. En niet zonder reden. Steeds meer gegevens worden digitaal opgeslagen en soms is volstrekt niet duidelijk waarvoor. Dat is op scholen niet anders, in het verleden had privacy minder prioriteit, maar de digitale mogelijkheden maken het nodig om regels op te stellen.

Binnen de Europese Unie had ieder land zo zijn eigen privacyregels. Vanaf 25 mei 2018 wordt dat anders, vanaf dat moment is er nog maar één privacywet voor de hele EU, de Algemene Verordening Gegevensbescherming (AVG)

Wanneer gebruikers (ook scholen) deze wet overtreden, dan dreigen er forse straffen. Reden genoeg dus om de privacyregels op onze scholen eens onder de loep te nemen.

Door Kennisnet werd de brochure “Privacy in 10 stappen” gepubliceerd. Deze ligt ten grondslag aan dit stuk.

2. Waarover gaat privacy?

Privacy is een grondrecht dat is vastgelegd in de Universele Verklaring van de Rechten van de Mens en binnen Europa in artikel 8 van het Europees Verdrag voor de Rechten van de Mens, binnen Nederland in artikel 10 van de Nederlandse Grondwet.

Leerlinggegevens zijn persoonsgegevens en deze bevatten vaak gevoelige informatie, bijvoorbeeld over gezondheid, gedragsproblemen, godsdienst, seksuele voorkeur of een problematische thuissituatie. Deze gegevens mogen alleen worden vastgelegd als dat noodzakelijk is, bijvoorbeeld voor speciale begeleiding van leerlingen om bijzondere voorzieningen te kunnen treffen. Denk ook aan de registratie van allergieën, zodat hiermee rekening kan worden gehouden bij traktaties of lunches, of om de noodzakelijke procedure te kunnen volgen bij bijvoorbeeld wespenallergie of diabetes.

Alles wat met die gegevens wordt gedaan wordt in de wet verwerken genoemd. Onder meer dus: online en offline persoonsgegevens verzamelen, kopiëren, opslaan, verspreiden, publiceren, delen en uitwisselen.

Nu er een Europese wet ingevoerd wordt, waarin ook de straffen zijn vermeld voor het niet-naleven, is het erg belangrijk dat alle betrokkenen de belangrijkste begrippen en uitgangspunten kennen, maar vooral dat ze de wet naleven. In het onderwijs zijn we daar met zijn allen, College van Bestuur, directeuren, teamleiders, leerkrachten en werknemers op het Stafbureau voor verantwoordelijk. Uiteraard dienen alle medewerkers hierover te worden geïnformeerd en waar kinderen omgaan met privacygevoelige gegevens, ook de leerlingen.

2.1 De AVG: 3 rollen waar het om bescherming van privacy gaat

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

Dit 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 AVG alleen de wettelijke vertegenwoordigers (ouders) beslissen over de gegevens van de betrokkene.

Voorbeeld

Ouders melden hun kind aan op een basisschool. De basisschool valt onder een stichting waar meerdere basisscholen onder vallen. De schooldirecteur verwerkt de inschrijving in de leerlingenadministratie 'XYZ'.

In dit voorbeeld is de leerling de betrokkene. De ouders beslissen over diens persoonsgegevens. De school valt onder de stichting: het bevoegd gezag. Dat stichtingsbestuur is daarmee ook de verantwoordelijke voor de AVG. XYZ is de aanbieder waarmee afspraken zijn gemaakt over de leerlingadministratie: XYZ is de bewerker voor de school.

De school maakt afspraken met de leverancier over wat er met de persoonsgegevens gedaan mag worden, de leverancier moet zich hieraan houden. De leverancier mag bijvoorbeeld niet op eigen initiatief aanbiedingen aan een ouder doen op basis van de resultaten van de leerling.

2.2 Uitgangspunt van de wet

Uitgangspunt van de AVG 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 mag er best veel.

3. Regels voor leerlinggegevens:

Al bij de opgave van de leerling op school moet voor de ouders duidelijk zijn welke gegevens van de leerling zullen worden opgeslagen en wat het doel daarvan is. Dit kan bijvoorbeeld via de Schoolgids of via de schoolwebsite. Hierbij gaat het om de gegevens in:

- Administratieprogramma Parnassys
- Cijferlijsten en toetsregistraties
- Leerlingnotities, ook notities die gemaakt worden door de IB-er
- Eventuele verslagen van medische, logopedische en andere onderzoeken
- Registraties voor gebruik van software etc.
- Overdracht naar een andere school

Bij de registratie wordt steeds rekening gehouden met de volgende vijf vuistregels:

Om volgens de Wet Algemene Verordening Gegevensbescherming (AVG) persoonlijke informatie te mogen verwerken, moet aan een aantal voorwaarden worden voldaan. Deze wettelijke eisen zijn terug te brengen tot de volgende vijf vuistregels:

1. **Doel**
   Persoonsgegevens worden altijd verzameld met een vooraf vastgesteld en concreet doel. Eenmaal verzamelde gegevens mogen dus niet zomaar voor een heel nieuw doel gebruikt worden. In het onderwijs gaat het in het algemeen om een of meerdere van de volgende doelen:
   a. Onderwijs geven en organiseren
   Om onderwijs te geven moet de docent weten welke leerlingen er in de klas zitten.
   b. Leerlingen begeleiden
   Leraren moeten de voortgang van leerlingen kunnen registreren.
   c. Leermiddelen verstrekken
   Om in te kunnen loggen bij een leverancier, mogen de gegevens van leerlingen wel worden gedeeld met de leverancier. Alleen dan kunnen leerlingen worden herkend als zij een digitaal leermiddel gebruiken.
   d. Informatie geven over de hierboven genoemde organisatie en leermiddelen
   De school moet met ouders en leerlingen kunnen communiceren, bijvoorbeeld via het rapport of een uitnodiging voor een ouderavond.

e. Informatie over leerlingen bekendmaken via de eigen communicatiekanalen (website)
De school mag in de nieuwsbrief of op de website opnemen dat een van de leerlingen kampioen is geworden tijdens het damkampioenschap van groep 6, 7 en 8.

f. Activiteiten van de instelling of het instituut bekendmaken op de eigen website
De school mag op de website informatie geven over een schoolvoetbaltoernooi én daarbij het e-mailadres vermelden van de leraar of leerlingen die dit organiseren.

g. Berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden, bijdragen en vergoedingen
De school mag persoonsgegevens gebruiken om bijvoorbeeld te registreren wie het geld voor de schoolreis al heeft betaald.

h. Geschillen behandelen
Als er een procedure plaatsvindt bij de geschillencommissie, dan mag de school ook voor dat doel gegevens vastleggen (bijvoorbeeld in een dossier).

i. Accountantscontrole uitoefenen

j. Uitvoering of toepassing van een wet
De school is verplicht om elk jaar voor 1 oktober een bestand met leerlinggegevens op te sturen naar DUO. Verzending van deze gegevens is geregeld in een aparte wet. Op basis hiervan ontvangt de school onder andere inkomsten van de overheid. Als een school gegevens verzamelt met een ander doel dan hierboven genoemd, dan eist de AVG van een school dat deze gegevensverzameling apart wordt aangemeld bij het College bescherming persoonsgegevens (CBP). In de praktijk zal dit niet vaak voorkomen.

2. **Doelbinding**
Persoonsgegevens mogen alleen worden verwerkt voor zover dat nodig is om het vastgestelde doel te bereiken. Gegevens die daarmee niet in verband staan, mogen dus ook niet worden verwerkt.
De ouders geven hun telefoonnummer voor onder meer noodgevallen. De school mag deze telefoonnummers niet (laten) gebruiken om de ouders uit te nodigen voor een inloopavond van de gemeente over een opknapbeurt voor de wijk waarin de school ligt.

3. **Grondslag**
Persoonsgegevens mogen alleen verwerkt worden als de Wet bescherming persoonsgegevens hier toestemming (grondslag) voor geeft. Voor het onderwijs gelden deze grondslagen:

a. Toestemming: als de betrokkene toestemming geeft (bijvoorbeeld het vinkje aanklikken bij een inschrijfformulier voor school of de knop Akkoord indrukken).
Bijvoorbeeld toestemming van ouders voor gebruik van beeld- of geluidsopnames van het kind.

b. Overeenkomst: gegevens mogen verzameld worden als dat nodig is voor de uitvoering van de overeenkomst met betrokkene (bijvoorbeeld de onderwijsovereenkomst).

c. Wet: als de wet eist dat persoonsgegevens verwerkt worden (bijvoorbeeld voor het doorgeven van leerlinginformatie aan het ministerie van OCW).

d. Publiekrechtelijke taak: op onze scholen is op basis van de haar opgedragen publieke taak (het geven van onderwijs) gegevensverwerking nodig

e. Vitaal belang (bescherming van de betrokkene) Verwerking van persoonsgegevens is noodzakelijk om een ernstige bedreiging van de gezondheid van de betrokkene te beperken/voorkomen.
Een leerling valt onder schooltijd en de ouders zijn onbereikbaar. Voor medische informatie over de leerling belt de school met de huisarts. Er is geen toestemming gevraagd voor dit overleg, maar het gesprek is wél in het belang van de leerling.

f. Gerechtvaardigd belang: het verzamelen van de persoonsgegevens is belangrijker dan het privacybelang van de betrokkene. Dit vereist een belangenafweging. De betrokkene mag zich verzetten tegen verwerking van zijn persoonsgegevens met deze grondslag.

4. **Dataminimalisatie**
   De persoonsgegevens die de school verwerkt, moeten redelijkerwijs nodig zijn om het doel te bereiken. De gegevens moeten in verhouding staan tot het doel ('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 doel te bereiken.
   Bij de inschrijving van een kind mag de school niet vragen naar de schoenmaat. De school heeft die informatie nergens voor nodig. Dit is anders als de school alle (nieuwe) leerlingen gymschoenen aanbiedt, of schoenen inkoopt voor het volleybalteam van de school. Dan is de vraag over de schoenmaat wel relevant.
5. **Transparantie en rechten 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. De ouders zijn op de hoogte van hun rechten als het gaat om de verwerking van persoonsgegevens door de school. Daarbij kan de school gebruikmaken van de informatie die uitgevers over hun producten verstrekken aan scholen: in de zogenoemde 'privacybijsluiter' wordt door de uitgever uitgelegd welke persoonsgegevens nodig zijn om het product te gebruiken. De onderwijsinstelling is verplicht deze bijsluiter (of zelf opgestelde informatie) delen met de ouders. Dit kan bijvoorbeeld in de schoolgids of via de website.

Bovengenoemde vuistregels zijn een hulpmiddel om te voldoen aan de wet, maar in twijfelgevallen is de Wet bescherming persoonsgegevens leidend.

4. Digitaal leermateriaal

Naast een leerling administratiesysteem en leerlingvolgsysteem, maken scholen meestal ook gebruik van digitaal leermateriaal. Daarvoor is het vaak nodig dat elke leerling wordt 'herkend', zodra hij of zij inlogt. Leraren willen bijvoorbeeld ook de vorderingen van leerlingen volgen: de aanbieder moet daarvoor gegevens leveren aan de school.

Bewerkersovereenkomst

Om te voorkomen dat de leverancier van software met privacygevoelige gegevens aan de haal gaat, is het wettelijk verplicht dat schriftelijke afspraken worden gemaakt in een zgn. bewerkersovereenkomst.

Het belangrijkste uitgangspunt in deze bewerkersovereenkomst is dat de bewerker (leverancier) alleen verwerkingen uitvoert in opdracht van de school. De leverancier mag de ontvangen gegevens niet voor iets anders gebruiken, de data doorverkopen of zelf contact opnemen met de ouders om bijvoorbeeld reclame te maken voor extra lesmateriaal.

Meestal neemt de leverancier zelf contact op om een bewerkersovereenkomst op te stellen, maar de school blijft zelf verantwoordelijk voor de aanwezigheid van zo'n overeenkomst.

In alle gevallen dient een bewerkersovereenkomst te worden ondertekend door een lid van het College van Bestuur als zijnde de wettelijk tekenbevoegde voor stichting OPONOA. De school dient de overeenkomst dus aan te bieden aan het CvB voor ondertekening.

De PO-raad heeft een model van zo'n bewerkersovereenkomst ontworpen. Bijna alle softwareleveranciers hanteren dit model. Het is bijgesloten in bijlage 7c.

Privacybijsluiter

Bij de Modelbewerkersovereenkomst hoort een bijlage, de 'privacybijsluiter'. Hierin leggen de partijen vast met welk doel de gegevensverwerking plaatsvindt, wat de dienstverlening van de leverancier omvat en wat de producteigenschappen zijn. Daarnaast staat er beschreven welke categorieën persoonsgegevens de leverancier verwerkt. De leverancier vult de bijsluiter in. De school gaat vanzelfsprekend na of alles klopt en besluit uiteindelijk om wel of niet akkoord te gaan met de voorgestelde afspraken. De uiteindelijke ondertekening moet namens de

school worden gedaan door een lid van het College van Bestuur, de school dient het formulier daarvoor aan het CvB aan te bieden.

5. Rechten van ouders

- Tot de leeftijd van 16 jaar (dus voor alle basisschoolleerlingen) beslissen de ouders daar waar het om persoonsgegevens van de leerlingen gaat. Daarom moet aan de ouders in alle gevallen vooraf in begrijpelijke taal informatie over het gebruik van persoonsgegevens worden gegeven. Dat kan op de schoolwebsite, in de schoolkrant of in een ander geschrift.
- Ouders hebben recht op inzage van alle verwerkte persoonsgegevens van hun kind, ook waar het gaat om aan derden (leveranciers) verstrekte gegevens. De school dient hierbij een omschrijving van het doel te geven waarvoor de gegevens worden geregistreerd.
- Ouders hebben recht op correctie van foutieve gegevens, bijvoorbeeld in geval van verhuizing of verandering van telefoonnummer.
- Ouders kunnen verzoeken om verwijderen van persoonsgegevens die niet (langer) nodig zijn. Zo kunnen zij bijvoorbeeld verzoeken om de gegevens van de opvang voor hun kind te verwijderen zodra die gegevens niet meer nodig zijn.
- Ouders kunnen verzet aantekenen tegen de verwerking van persoonsgegevens. De school heeft na het verzoek maximaal 4 weken tijd om hierop actie te ondernemen.

6. De (G)MR

De (G)MR dient betrokken te worden bij het verwerken van persoonsgegevens. Zonder instemming van de (G)MR kan dit privacyprotocol niet in werking treden. Na de instemming van de (G)MR moet dit protocol ter inzage liggen op de school.

Verder heeft de (G)MR een adviserende rol, gevraagd of ongevraagd.

7. Foto’s en video’s op school

Een foto waarop een leerling herkenbaar in beeld is, zegt iets over de leerling. De foto is een persoonsgegeven. Daarom is de AVG van toepassing op gebruik van (pas) foto’s waarop een of meerdere leerlingen herkenbaar in beeld zijn. Als de school die foto bijvoorbeeld op de website wil zetten, dan is daar geen andere grondslag voor mogelijk dan toestemming. Die toestemming wordt op onze scholen gevraagd op het aanmeldingsformulier. Daarbij wordt specifiek omschreven waarvoor het beeldmateriaal zal worden gebruikt, bijv. de website, nieuwsbrieven, schoolgids, folder, sociale media, … . Een gegeven toestemming voor de schoolwebsite betekent niet dat daarmee de foto’s bijvoorbeeld ook op Facebook mogen worden gebruikt.

Foto’s waarop leerlingen herkenbaar in beeld worden gebracht, moeten worden afgeschermd voor derden met een wachtwoord of code.

Zolang ouders geen toestemming hebben gegeven, is het de school wettelijk verboden om foto’s van de leerlingen te gebruiken.

Aan de ouders moet wel jaarlijks duidelijk worden gemaakt dat die toestemming op elk moment kan worden ingetrokken, bijvoorbeeld in de schoolgids of op de website.

8. Internet en sociale media

Internet en sociale media worden steeds vaker door leerlingen en docenten gebruikt. De informatie die online wordt gedeeld, bevat vaak persoonsgegevens: een foto, naam, gedrag, uitnodiging of gesprek. Is het niet in de les, dan is het wel op het schoolplein. Internet en sociale media maken daarmee onderdeel uit van het schoolklimaat.

Wanneer dit in het onderwijsprogramma past, kan op OPONOA-scholen gebruik gemaakt worden van websites en zoekmachines. De leerkracht dient daarbij te voorkomen dat leerlingen hun persoonlijke gegevens prijsgeven via internet.

Daarnaast wordt online software gebruikt. Hiervoor dient steeds een bewerkersovereenkomst op school aanwezig te zijn. Dit werd hiervoor al beschreven in hoofdstuk 4.

Voor het gebruik van sociale media beschikt OPONOA over een protocol voor alle medewerkers en leerlingen. Zie daarvoor de bijlage "Modelprotocol Sociale Media".

9. Overstap naar een andere school

Als een leerling overstapt naar een andere school, moeten bij de aanmelding wettelijk verplichte gegevens worden aangeleverd.

Daarnaast is het zinvol om bepaalde leerresultaten door te geven aan de vervolgschool, zodat daar het onderwijs afgestemd kan worden op de behoeften van het kind.

Voor de overstap wordt gebruik gemaakt van de Overstapservice voor het Onderwijs (OSO). OSO werkt via wettelijke richtlijnen en er wordt voor gezorgd dat een overstapdossier alleen via een beveiligde verbinding tussen de juiste scholen wordt overgedragen.

In de praktijk is de administratieve overdracht als volgt:

- In de schooladministatie wordt een dossier verzameld. Dit dossier bevat administratieve gegevens, zorggegevens, begeleidingsgegevens in informatie over de leerresultaten.
- Het dossier wordt vervolgens afgedrukt en ter kennisneming en ondertekening aangeboden aan de ouders. Het is niet noodzakelijk dat ouders akkoord gaan met het dossier, maar eventuele bezwaren en opmerkingen moeten wel opgenomen worden in het dossier en worden meegestuurd.
- Nadat de ouders hebben getekend voor de inzage wordt het dossier geplaatst op het OSO-platform, waar de school van bestemming het weer af kan halen.

10. Gegevens beveiligen

Zorgvuldig omgaan met persoonsgegevens vraagt om een goede beveiliging. Scholen zijn verplicht om persoonsgegevens te beveiligen tegen risico's zoals verlies, onbevoegde toegang, vernietiging, gebruik, wijziging of openbaarmaking van gegevens. Voor deze beveiliging zijn een aantal richtlijnen:

10.1 Dataminimalisatie.

Niet meer mensen dan nodig moeten bij de gegevens kunnen. Een conciërge moet bijvoorbeeld ouders kunnen bellen in geval van ziekte, maar heeft geen toegang nodig tot de cijfers of het leerlingvolgsysteem. In dit verband is het belangrijk dat de medewerkers de goede rol in het administratiepakket en het leerlingenvolgsysteem krijgen toebedeeld. En in het schoolnetwerk wordt onderscheid gemaakt tussen documenten voor directie (locatieleiders), IB-ers, leerkrachten en leerlingen. Verder is het de bedoeling dat iedereen met zijn eigen gebruikersnaam/wachtwoord inlogt, om te voorkomen dat leerlingen en medewerkers informatie te zien krijgen die niet voor hen bedoeld is.

10.2 Type persoonsgegevens.

We onderscheiden 3 categorieën persoonsgegevens:

- Publieke informatie. Informatie die met iedereen gedeeld kan worden.
- Gevoelige informatie. Informatie die bestemd is voor een beperkt publiek. Deze informatie moet worden afgeschermd zodat derden geen inzage hebben en niets kunnen wijzigen.

- Zeer gevoelige informatie. Informatie die bedoeld is voor een zeer beperkt publiek en die absoluut niet bedoeld is voor derden. Denk aan accountgegevens, medische informatie, geheime telefoonnummers.

Afhankelijk van het type persoonsgegeven moet worden bepaald welke beveiligingsmaatregelen moeten worden getrokken. Zo hoort een leerkracht standaard geen inzage te hebben in alle medische informatie, maar een zorgcoördinator of IB-er weer wel.

10.3 Bewaartermijnen.

Gegevens mogen niet langer bewaard worden dan nodig is.

In de Wet worden de volgende bewaartermijnen voorgeschreven:

- Leerlingenadministratie:
  Voor de leerlingenadministratie geld een termijn van minimaal 5 jaar vanaf de datum van uitschrijving.
- Leerlingendossiers:
  Voor leerlingendossiers geldt een bewaartermijn van minimaal 2 jaar na uitschrijving van de school.
- Overstapdossiers:
  Voor het dossier bij overstap naar een school voor speciaal onderwijs geldt een bewaartermijn van 3 jaar.

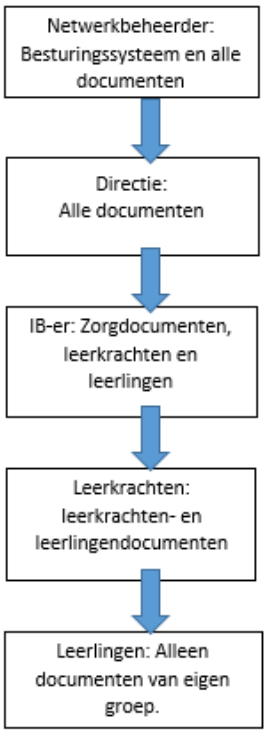
11. Naar een optimaal beveiligingsniveau

Nu er steeds meer persoonsgegevens worden opgeslagen en verwerkt, is het zaak om de beveiliging goed voor elkaar te hebben.

11.1 Leveranciers

Voor leveranciers wordt een set van beveiligingsafspraken gehanteerd ("Certificeringsschema ROSA"). Hiermee moeten leveranciers aantonen dat ze aantoonbare beveiligingsmaatregelen genomen hebben. Hiermee wordt gewaarborgd dat er een betrouwbare keten voor uitwisseling van gegevens ontstaat.

11.2 Op school



We kunnen onze privacy m.b.t. leveranciers zo goed beveiligen als we willen, maar als op schoolniveau zaken niet goed geregeld zijn, staat alles nog open. In verband hiermee hanteren we binnen de scholen de volgende afspraken:

- Zorg dat er geen schriftelijk, privacygevoelig materiaal ligt waar onbevoegden zo maar in kunnen kijken. Dus geen cijferlijsten laten slingeren, klassenmappen opruimen etc.
- Laat geen computer onbeheerd en ingelogd staan. Ben je maar even weg, dan kun je de computer "locken" door op de Windows-toets+L te drukken. Via CTRL+ALT+DEL kun je hem weer "unlocken". Ga je langer weg, log dan uit of sluit de pc af.
- Laat iedereen werken onder zijn eigen inlog. Dus geen leerlingen achter een pc die ingelogd is als andere groep, leerkracht, IB-er, locatieleider of directie. De inrichting van het schoolnetwerk is volgens een bepaalde hiërarchie: de directeur kan alles zien en de leerlingen zien alleen documenten van de eigen groep. Zie bijgaand schema. De gebruikers hoger in het schema zie ook de documenten van alles wat eronder staat.
- Gebruik wachtwoorden die voldoende gecompliceerd zijn en wissel minimaal 1x per halfjaar van wachtwoord voor de mail en de netwerk-accounts van leerkrachten, IB-er, locatieleider en directie.
- Sla nooit privacygevoelige bestanden lokaal op de pc op. Wanneer de pc aan het eind van zijn leven is, zou iemand de harde schijf eruit kunnen halen en de bestanden weer leesbaar maken (zelfs als de bestanden zijn verwijderd!!). Om deze reden is lokale opslag voor de meeste gebruikers onmogelijk gemaakt.

- Hang nooit briefjes met wachtwoorden op het prikbord, aan de monitor of op een andere zichtbare plaats.
- Wachtwoorden voor websites opslaan op je pc? Alleen als de pc zelf met een voldoende gecompliceerd wachtwoord beveiligd is.
- Wanneer je een smartphone gebruikt om je werkmail te lezen, zorg dan ook dat deze niet vrij toegankelijk is, stel op zijn minst een pincode of een tekenpatroon in. Ook voor dit apparaat geldt dan dat het teruggezet moet worden in de fabrieksinstellingen voordat het wordt afgedankt.

11.3 Wie mag inloggen en wanneer?

Inloggen op het netwerk is vanzelfsprekend toegestaan voor de op het netwerk aangemaakte gebruikers. Maar uitsluitend voor hen. Het kan dus niet zo zijn dat bijv. het zoontje van een leerkracht dat hier geen leerling is, zo lang een spelletje doet via een inlog van vader of moeder op het netwerk.

Vrijwel alle digibord-pc's werken via de inlog als Leerkracht. Bij afwezigheid van de leerkracht dienen deze "gelockt" te worden. Moet het beeld van de beamer op het bord blijven staan, dan kan deze in de stand "freeze" worden gezet. Het laatste beeld blijft dan op het digibord staan.

Inloggen op een school-pc buiten schooltijd is voor leerlingen alleen toegestaan na uitdrukkelijke toestemming van de leerkracht. Deze dient hierbij toezicht te houden. Immers via de groepsinlog zijn ook documenten beschikbaar van de andere leerlingen in de groep.

11.3 Thuis, werkgerelateerd

Het bovenstaande geldt niet alleen voor de schoolcomputers. Wanneer je de computer thuis ook gebruikt voor je werk, ligt het voor de hand dat je daar werk gerelateerde bestanden opslaat. Ook in dat geval gelden bovenstaande regels en onderstaande regels m.b.t. afvoer van materialen. Het mag niet gebeuren dat een buurjongen op de oude, cadeau gekregen pc nog vertrouwelijk materiaal van school vindt. Overigens is het bovenstaande ook belangrijk i.v.m. je eigen privacy. Over het leegmaken van een harde schijf vind je meer informatie op deze link.

11.4 Afvoer van oude apparatuur

Elke pc is een keer aan zijn eind. Als voldaan is aan de afspraak dat op pc's geen privacygevoelige bestanden worden opgeslagen, kan een pc na gebruik voor recycling naar de Kringloop.

Gaat het om een server, dan moeten de harde schijven worden gedemonteerd en ontdaan worden van data. Dat kan op twee manieren:

- Demontage van de onderdelen van de schijf of fysieke vernieling (bankschroef, hamer).
- Met een speciaal programma (bijv. Killdisk) wordt alle data van de schijf verwijderd, zodat ze niet terug te halen is.

Oude servers mogen dus nooit worden afgevoerd als niet helemaal zeker is of er nog vertrouwelijke informatie op staat. Dat is pas zeker als de harde schijf eruit gehaald is of vakkundig is leeggemaakt ("geshred").

12. Vertrekkende leerkrachten

Wanneer leerkrachten vertrekken, moet i.v.m. de beveiliging aan het volgende gedacht worden:

- De leerkracht moet in Parnassys op "niet-actief" worden gezet. Na de nachtelijke synchronisatie is ook de inlog in Basispoort verdwenen. Taak: locatieleider.
- Het Office365-account moet op "niet-actief" worden gezet of worden verwijderd. Zo zijn er geen rechten meer in Sharepoint, OneDrive en de mailbox. Er kunnen afspraken worden gemaakt of de leerkracht nog gelegenheid krijgt om waardevolle berichten in veiligheid te brengen. Taak: melding door locatieleider, uitvoering Stafbureau.

- De mogelijkheid om in systemen van het ministerie in te loggen namens school (bijv. het Schooldossier van de Inspectie, Mijn Vensters, …) moet worden stopgezet. Taak: melding door locatieleider, uitvoering Stafbureau.

13. Wanneer het mis gaat: een datalek

13.1 Wat is een datalek precies?

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 Algemene Verordening). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Hierbij moeten we niet alleen denken aan onrechtmatige toegang tot een server (hacken), maar bijvoorbeeld ook in de volgende gevallen:

- Een verloren of weggegooide USB-stick met nog aanwezige gegevens (let op: formatteren is niet voldoende om de gegevens te wissen en ook defecte sticks zijn soms nog weer leesbaar te maken!!) of een gestolen laptop;
- Een afgedankte pc of server die wordt afgevoerd met harde schijf aan boord waarop nog data staat (ook in dit geval is wissen en/of formatteren niet voldoende);
- Een bestand met persoonlijke gegevens dat per ongeluk wordt gemaild naar onbevoegden;
- Economische of financiële gegevens van personen (salarisopgaven, schuldenregelingen etc.) vallen in onbevoegde handen;
- Gegevens die kunnen worden gebruikt voor (identiteits-)fraude (identiteitsgegevens, BSN etc.) komen in onbevoegde handen.

13.2 Waarom is een datalek (voor de school en schoolbestuur) vervelend?

Het bevoegd gezag van een school is verantwoordelijk voor de bescherming van persoonsgegevens van leerlingen en personeel. Een medewerker hoort een usb-stick met leerlingzorgdossiers niet in de trein te laten liggen, maar is het ook een dramatisch datalek?

Ja, dat is het. Het is vervelend voor de leerlingen (en hun ouders) wiens persoonsgegevens op straat komen te liggen. Maar ook de school kan er last van krijgen. Datalekken kunnen op flinke media-aandacht, en bijbehorende imagoschade, rekenen.

Daarnaast is sinds 1 januari 2016 de Wet meldplicht datalekken van kracht. Die wet geeft de privacytoezichthouder College Bescherming Persoonsgegevens (CBP) een verzwaarde boetebevoegdheid. Het niet (tijdig) melden van een datalek kan bestraft worden met een boete van maximaal 810.000 euro of zelfs een boete van 10 procent van de omzet van de organisatie.

13.3 Welke datalekken moeten gemeld worden?

Volgens de Wet Bescherming Persoonsgegevens hoeven niet alle datalekken te worden gemeld. De meldplicht is van toepassing op datalekken die plaatsvinden in gegevensbestanden waarvoor je als school verantwoordelijk bent: bijvoorbeeld een Excel-sheet met NAW-gegevens van klas 3a of de database met personeelsgegevens.

Daarnaast moet er sprake zijn van een inbreuk op de beveiliging van persoonsgegevens die leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van de persoonsgegevens. Dat is bijvoorbeeld het geval als een hele database met leerlinggegevens is gehackt, of bij het lekken van bijzondere persoonsgegevens zoals medische gegevens. Dan dient het lek binnen twee werkdagen gemeld te worden bij het CBP.

In sommige gevallen moet je een datalek niet alleen bij het CBP maar ook bij de benadeelde melden. Was de verloren usb-stick niet beveiligd of waren de gehackte gegevens niet versleuteld? En zal het datalek waarschijnlijk ongunstige gevolgen hebben voor de persoonlijke levenssfeer van de betrokkene? Als er geen zwaarwegende redenen zijn tegen het melden van het lek aan de betrokkenen, ben je ook verplicht het datalek aan hen te melden.

14. Functionaris voor de gegevensbescherming

Binnen overheidsinstanties en publieke instanties is het volgens de Algemene Verordening Gegevensbescherming (AVG) verplicht om een "functionaris voor de gegevensbescherming" (FG) aan te stellen. Dit geldt ook voor onderwijsinstellingen.

De belangrijkste taken voor een FG kunnen zijn:

- Toezicht houden;
- Inventarisaties van gegevensverwerkingen maken;
- Meldingen van gegevensverwerkingen bijhouden;
- Vragen en klachten van mensen binnen en buiten de organisatie behandelen;
- Interne regelingen ontwikkelen;
- Adviseren over technologie en beveiliging;
- Input leveren bij het opstellen of aanpassen van een gedragscode

Nadere informatie over de functionaris voor de gegevensbescherming is te hier vinden. Hier staan ook eisen, taken en bevoegdheden van een FG beschreven en er wordt bericht over zijn ontslagbescherming.

Het aanstellen van een FG kan op verschillende manieren:

- Bedrijfsmatige inhuur van een FG die zijn diensten aan de stichting verleent;
- Aanstelling van een FG binnen de stichting die zijn werk op de scholen en in het Stafbureau doet;
- Aanstelling van een FG per school.

Een FG kan binnen de organisatie niet dezelfde persoon zijn als degene die het doel van en de middelen voor de gegevensverwerking vaststelt.

Zodra een FG benoemd is, dient deze te worden aangemeld bij de Autoriteit Persoonsgegevens (en worden afgemeld bij het stoppen van deze taak). Ieder personeelslid van onze stichting dient geïnformeerd te worden over de FG.

15. Verantwoordelijken

In principe is het bevoegd gezag van de school verantwoordelijk voor het opstellen en handhaven van een privacyprotocol, dus ons College van Bestuur. Echter voor de uitvoering daarvan zijn de medewerkers verantwoordelijk. Een protocol waaraan de medewerkers zich niet houden heeft geen enkele waarde.

In dit verband is het belangrijk dat bijvoorbeeld eenmaal per jaar de bijgevoegde "Checklist privacy" door alle personeelsleden wordt doorlopen en dat geconstateerde tekortkomingen worden aangepakt.

Wij allemaal willen niet dat ónze persoonlijke gegevens op straat komen te liggen. Daarom dienen wij allen mee te werken aan de bescherming van de privacy van de hele schoolbevolking.

16. Bijlagen:

a. Protocol sociale media

b. Voorbeeld bewerkersovereenkomst PO-raad, inclusief Privacy-bijsluiter

c. Checklist privacy

a. Protocol sociale media

Samen actief voor een rijk onderwijsaanbod

Modelprotocol Sociale Media

Inleiding

Sociale media zoals Twitter, Facebook, YouTube en LinkedIn bieden de mogelijkheid om te laten zien dat je trots bent op je school en kunnen een bijdrage leveren aan een positief imago van [naam onderwijsinstelling]. Van belang is te beseffen dat je met berichten op sociale media (onbewust) de goede naam van de school en betrokkenen ook kunt schaden. Om deze reden vragen wij om bewust met de sociale media om te gaan.

Essentieel is dat, net als in communicatie in de “normale” wereld, de onderwijsinstellingen en de gebruikers van sociale media de reguliere fatsoensnormen in acht blijven nemen en de nieuwe mogelijkheden met een positieve instelling benaderen.

[naam onderwijsinstelling] vertrouwt erop dat zijn medewerkers, leerlingen, ouders/verzorgers en andere betrokkenen verantwoord om zullen gaan met sociale media en heeft dit protocol opgezet om een ieder die bij de [naam school] betrokken is of zich daarbij betrokken voelt daarvoor richtlijnen te geven.

Uitgangspunten

1. [naam onderwijsinstelling] onderkent het belang van sociale media.
2. Dit protocol draagt bij aan een goed en veilig school- en onderwijsklimaat;
3. Dit protocol bevordert dat de instelling, medewerkers, leerlingen en ouders op de sociale media communiceren in het verlengde van de missie en visie van de onderwijsinstelling en de reguliere fatsoensnormen. In de regel betekent dit dat we respect voor de school en elkaar hebben en iedereen in zijn waarde laten;
4. De gebruikers van sociale media dienen rekening te houden met de goede naam van de school en van een ieder die betrokken is bij de school;
5. Het protocol dient de onderwijsinstelling, haar medewerkers, leerlingen en ouders tegen zichzelf en anderen te beschermen tegen de mogelijke negatieve gevolgen van de sociale media;

Doelgroep en reikwijdte

1. Deze richtlijnen zijn bedoeld voor alle betrokkenen die deel uitmaken van de schoolgemeenschap, dat wil zeggen medewerkers, leerlingen, ouders/verzorgers en mensen die op een andere manier verbonden zijn aan [naam school].
2. De richtlijnen in dit protocol hebben enkel betrekking op schoolgerelateerde berichten of wanneer er een overlap is tussen school, werk en privé.

Sociale media in de school

A. Voor alle gebruikers (medewerkers, leerlingen en ouders/verzorgers)

1. Het is medewerkers en leerlingen niet toegestaan om tijdens de lessen actief te zijn op sociale media tenzij door de schoolleiding respectievelijk leraren hiervoor toestemming is gegeven.
2. Het is betrokkenen toegestaan om kennis en informatie te delen, mits het geen vertrouwelijke of persoonlijke informatie betreft en andere betrokkenen niet schaadt.
3. De betrokkene is persoonlijk verantwoordelijk voor de inhoud welke hij of zij publiceert op de sociale media.
4. Elke betrokkene dient zich ervan bewust te zijn dat de gepubliceerde teksten en uitlatingen voor onbepaalde tijd openbaar zullen zijn, ook na verwijdering van het bericht.
5. Het is voor betrokkenen niet toegestaan om foto-, film- en geluidsopnamen van schoolgerelateerde situaties op de sociale media te zetten tenzij betrokkenen hier uitdrukkelijk toestemming voor plaatsing hebben gegeven;
6. Het is medewerkers niet toegestaan om ‘vrienden’ te worden met leerlingen op sociale media.
7. Alle betrokkenen nemen de fatsoensnormen in acht. Als fatsoensnormen worden overschreden (bijvoorbeeld: mensen pesten, kwetsen, stalken, bedreigen, zwartmaken of anderszins beschadigen) dan neemt de onderwijsinstelling passende maatregelen. Zie ook : *Sancties en gevolgen voor medewerkers en leerlingen*

B. Voor medewerkers tijdens werksituaties

1. Medewerkers hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media: privémeningen van medewerkers kunnen eenvoudig verward worden met de officiële standpunten van de onderwijsinstelling.
2. Indien een medewerker deelneemt aan een discussie die (op enigerlei wijze) te maken heeft met [naam onderwijsinsteling] dient de medewerker te vermelden dat hij/zij medewerker is van [naam school].
3. Als online communicatie dreigt te ontsporen dient de medewerker direct contact op te nemen met zijn/haar leidinggevende om de te volgen strategie te bespreken.
4. Bij twijfel of een publicatie in strijd is met deze richtlijnen neemt de medewerker contact op met zijn/haar leidinggevende.

C. Voor medewerkers buiten werksituaties

1. Het is de medewerker toegestaan om schoolgerelateerde onderwerpen te publiceren mits het geen vertrouwelijke of persoonsgebonden informatie over de school, zijn medewerkers, leerlingen, ouders/verzorgers en andere betrokkenen betreft. Tevens mag de publicatie de naam van de school niet schaden.
2. Het is voor medewerkers niet toegestaan standpunten en/of overtuigingen uit te dragen welke in strijd zijn met de missie en visie van [naam onderwijsinstelling] en de uitgangspunten van dit protocol.
3. Indien de medewerker deelneemt aan een discussie die (op enigerlei wijze) te maken heeft met de onderwijsinstelling dient medewerker te vermelden dat hij/zij medewerker is van [naam school].
4. Indien de medewerker over [naam onderwijsinstelling] publiceert dient hij/zij het bericht te voorzien van het bericht dat de standpunten en meningen in dit bericht de eigen persoonlijke mening zijn en los staan van eventuele officiële standpunten van [naam onderwijsinstelling. Verder meldt de medewerker dat hij of zij niet verantwoordelijk is voor de inhoud en uitlatingen van derden.

Sancties en gevolgen voor medewerkers en leerlingen

1. Medewerkers die in strijd handelen met dit protocol maken zich mogelijk schuldig aan plichtsverzuim. Alle correspondentie omtrent dit onderwerp wordt opgenomen in het personeelsdossier.
2. Indien [naam bevoegd gezag] de wijze van communiceren door een medewerker(s) als 'grensoverschrijdend' kwalificeert, dan wordt dit telefonisch gemeld bij de Landelijke Vertrouwensinspecteur (0900 – 1113111).
3. Afhankelijk van de ernst van de uitlatingen, gedragingen en gevolgen worden naar medewerkers toe rechtspositionele maatregelen genomen welke variëren van waarschuwing, schorsing, berisping, ontslag en ontslag op staande voet;
4. Leerlingen en/of ouders/verzorgers die in strijd met dit protocol handelen maken zich mogelijk schuldig aan verwijtbaar gedrag. Alle correspondentie omtrent dit onderwerp wordt opgenomen in het leerlingendossier.
5. Afhankelijk van de ernst van de uitlatingen, gedragingen en gevolgen worden naar leerlingen en / of ouders/verzorgers toe maatregelen genomen welke variëren van waarschuwing, schorsing en verwijdering van school
6. Indien de uitlating van leerlingen, en/of ouders/verzorgers en medewerkers mogelijk een strafrechtelijke overtreding inhoudt zal door [naam onderwijsinstelling] aangifte bij de politie worden gedaan.

Dit protocol is met instemming van de (G)MR op [datum] tot stand gekomen.

Borculo, versie 04 november 2013

b. Voorbeeld bewerkersovereenkomst PO-raad, inclusief Privacy-bijsluiter

Model Bewerkersovereenkomst Versie 2.0

Deze Model Bewerkersovereenkomst is een bijlage bij het *Convenant Digitale Onderwijsmiddelen en Privacy* (hierna: het Convenant) afgesloten tussen de PO-Raad, VO-raad en de brancheorganisaties van educatieve uitgeverij (GEU), distributeurs van leermiddelen (leden van sectie educatief van de Koninklijke Boekverkopersbond) en digitale dienstverleners in het onderwijs-ICT (VDOD).

De uitgangspunten van deze Model Bewerkersovereenkomst sluiten aan bij de bepalingen in het Convenant, de Algemene Verordening Gegevensbescherming (hierna: AVG), en de uitgangspunten zoals in jurisprudentie en de toezichthouder de Autoriteit Persoonsgegevens deze in richtsnoeren en uitspraken heeft aangegeven.

De model bewerkersovereenkomst versie 2016 is de opvolger van de model bewerkersovereenkomst die in 2015 in het kader van het Convenant *Digitale Onderwijsmiddelen en Privacy, leermiddelen en toetsen* is opgesteld. De versie 2.0 ziet naast het gebruik van leermiddelen en toetsen ook op School- en Leerlinginformatiemiddelen. Daarnaast is de overeenkomst op onderdelen bijgesteld naar aanleiding van recente ontwikkelingen in wet- en regelgeving, waaronder de wijziging van de AVG in verband met de meldplicht datalekken.

De nieuwe Model Bewerkersovereenkomst 2.0 komt in de plaats van de Model Bewerkersovereenkomst uit 2015. Reeds afgesloten bewerkersovereenkomsten op basis van het oude model uit 2015 blijven in beginsel hun gelding houden totdat deze bewerkersovereenkomsten door partijen worden beëindigd en aansluitend worden opgevolgd door een nieuwe bewerkersovereenkomst op basis van de nieuwe Model Bewerkersovereenkomst 2.0.

In het Convenant is afgesproken dat Onderwijsinstellingen en Ketenpartijen dit model gebruiken bij het maken van afspraken. Indien geen gebruik kan worden gemaakt van (onderdelen van) de Model Bewerkersovereenkomst, dan kan daar alleen gemotiveerd en schriftelijk van worden afgeweken. Gezien het aantal bepalingen dat ofwel wettelijk is voorgeschreven, of waarvan de Autoriteit Persoonsgegevens aangeeft dat deze in de bewerkersovereenkomst moeten worden opgenomen, is de ruimte voor afwijking van de bepalingen in het model beperkt.

Deze Model Bewerkersovereenkomst bevat twee bijlagen:

1. In de Privacy Bijsluiter (Bijlage 1) wordt een beschrijving gegeven van de dienstverlening, producteigenschappen en welke categorieën Persoonsgegevens worden verwerkt en onder welke doeleinden deze verwerkingen vallen.
2. In de Technische en Organisatorische Maatregelen (Bijlage 2) wordt omschreven welke beveiligingsmaatregelen er worden getroffen. De beveiliging dient een continu punt van aandacht en zorg te blijven

Informatie over het Convenant en de model bewerkersovereenkomst is te vinden op de website http://ww.privacyconvenant.nl. Meer informatie en antwoorden op vragen over privacy en de wettelijke rechten en verplichtingen voor Onderwijsinstellingen zijn te vinden op de websites van de sectorraden PO-Raad en VO-raad en bij Kennisnet.

Juni 2016

Partijen:

1. Het bevoegd gezag van <naam + rechtsvorm onderwijsinstelling>, geregistreerd onder BRIN-nummer <brin> bij de Dienst Uitvoering Onderwijs van het Ministerie van Onderwijs, gevestigd en kantoorhoudende aan <adres>, te (<postcode>) <plaats>, te dezen rechtsgeldig vertegenwoordigd door <functie + naam>, hierna te noemen: "**Onderwijsinstelling**".

en

2. De besloten vennootschap <Naam> B.V., gevestigd en kantoorhoudende aan <adres>, te (<postcode>) <plaats>, te dezen rechtsgeldig vertegenwoordigd door <functie + naam>, hierna te noemen: "**Bewerker**"

hierna gezamenlijk te noemen: "**Partijen**", of afzonderlijk: "**Partij**"

Overwegen het volgende:

a. Onderwijsinstelling en Bewerker zijn een overeenkomst aangegaan waarbij <**concrete omschrijving van de door Bewerker in opdracht van Onderwijsinstelling te leveren producten/diensten**>, ('de Product- en Dienstenovereenkomst'). Deze Product- en Dienstenovereenkomst leidt ertoe dat Bewerker in opdracht van Onderwijsinstelling Persoonsgegevens verwerkt.
b. Partijen wensen, mede gelet op het bepaalde in artikel 14 Wet bescherming persoonsgegevens, in deze Bewerkersovereenkomst hun wederzijdse rechten en verplichtingen voor de Verwerking van Persoonsgegevens vast te leggen.

Komen het volgende overeen:

Artikel 1: Definities

In deze Bewerkersovereenkomst wordt verstaan onder:

a. Betrokkene, Bewerker, Derde, Persoonsgegevens, Verwerking van Persoonsgegevens, en Verantwoordelijke: de begrippen zoals gedefinieerd in artikel 1 van de AVG;
b. Bewerkersovereenkomst: deze Bewerkersovereenkomst, inclusief Bijlagen;
c. Bijlage: een bijlage bij deze Bewerkersovereenkomst, welke daarvan een onlosmakelijk deel uitmaakt;
d. Convenant: het *Convenant Digitale Onderwijsmiddelen en Privacy;*
e. Datalek: een inbreuk op de beveiliging, zoals bedoeld in artikel 13 AVG, die leidt tot de aanzienlijke kans op ernstig nadelige gevolgen, dan wel ernstig nadelige gevolgen heeft voor de bescherming van persoonsgegevens, zoals bedoeld in artikel 34a, lid 1, AVG;
f. Digitaal Onderwijsmiddel: Leermiddelen en Toetsen, en School- en Leerlinginformatiemiddelen;
g. Leermiddelen en Toetsen: digitaal product en/of digitale dienst bestaande uit leerstof en/of toetsen en de daarmee samenhangende digitale diensten, gericht op onderwijsleersituaties, ten behoeve van het geven van onderwijs door of namens Onderwijsinstellingen;
h. School- en Leerlinginformatiemiddelen: een digitaal product en/of digitale dienst ten behoeve van het onderwijs(proces), zoals een leerling administratiesysteem, roostersysteem, ouderportaal, leerling- en oudercommunicatiesysteem, een elektronische leeromgeving en een leerling volgsysteem;
i. Privacy Bijsluiter: de privacy bijsluiter zoals opgenomen in Bijlage 1;
j. Product- en Dienstenovereenkomst: de overeenkomst tussen Onderwijsinstelling en Bewerker, zoals omschreven in overweging a;
k. Model Bewerkersovereenkomst: het model voor een bewerkersovereenkomst die als bijlage is bijgevoegd bij het Convenant;

l. Subbewerker: de partij die door Bewerker wordt ingeschakeld als Bewerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van deze Bewerkersovereenkomst en de Product- en Dienstenovereenkomst;
m. Wbp: Wet bescherming persoonsgegevens.

Artikel 2: Onderwerp en opdracht Bewerkersovereenkomst

1. Deze Bewerkersovereenkomst is van toepassing op de Verwerking van Persoonsgegevens in het kader van de uitvoering van de Product- en Dienstenovereenkomst.
2. De Onderwijsinstelling verstrekt aan de Bewerker de opdracht tot Verwerking van Persoonsgegevens ten behoeve van de uitvoering van de Product- en Dienstenovereenkomst.

Artikel 3: Rolverdeling

1. Onderwijsinstelling is ten aanzien van de in diens opdracht uit te voeren Verwerkingen van Persoonsgegevens de Verantwoordelijke. Bewerker is bewerker in de zin van de AVG. De Onderwijsinstelling heeft en houdt zelfstandige zeggenschap over het doel en de middelen van de Verwerking van de Persoonsgegevens.
2. Bewerker draagt er zorg voor dat de Onderwijsinstelling voorafgaande aan het sluiten van deze Bewerkersovereenkomst toereikend wordt geïnformeerd over de dienst(en) die de Bewerker verleent, en de uit te voeren Verwerkingen. De gegeven informatie moet de Onderwijsinstelling in staat stellen een keuze te maken met betrekking tot de aangeboden diensten als zodanig, en daarnaast een afzonderlijke keuze te maken voor eventueel aangeboden optionele diensten.
3. De in lid 2 bedoelde diensten, waaronder eventuele optionele diensten, moeten in de Privacy Bijsluiter bij deze Bewerkersovereenkomst in begrijpelijke taal zijn beschreven, waarna de Onderwijsinstelling geïnformeerd akkoord kan gaan met de afname van deze dienst(en).
4. De Onderwijsinstelling kan verplicht zijn de Verwerking van de Persoonsgegevens te melden bij de Autoriteit Persoonsgegevens. De Onderwijsinstelling onderzoekt of zij hiervan is vrijgesteld en doet melding bij de Autoriteit Persoonsgegevens indien zij hiertoe verplicht is.
5. Onderwijsinstelling en Bewerker verstrekken elkaar over en weer alle benodigde informatie teneinde een goede naleving van de relevante privacywet- en regelgeving mogelijk te maken.

Artikel 4: Privacy convenant

1. Partijen onderschrijven de bepalingen in het Convenant Digitale Onderwijsmiddelen en Privacy.

Artikel 5: Gebruik Persoonsgegevens

1. Bewerker verplicht zich om de van Onderwijsinstelling verkregen Persoonsgegevens niet voor andere doeleinden of op andere wijze te gebruiken dan voor het doel, en de wijze waarvoor, de gegevens zijn verstrekt of aan hem bekend zijn geworden. Het is Bewerker derhalve niet toegestaan andere gegevensverwerkingen uit te voeren dan door de Onderwijsinstelling (mondeling, schriftelijk dan wel elektronisch) aan Bewerker zijn opgedragen. Deze verplichting geldt zowel gedurende de looptijd van deze overeenkomst als na afloop daarvan.
2. Een overzicht van de categorieën Persoonsgegevens en gebruik waarvoor de Persoonsgegevens worden verwerkt, is uiteengezet in de Privacy Bijsluiter bij deze Bewerkersovereenkomst.
3. De Bewerker dient in de Privacy Bijsluiter aan te geven of de Privacy Bijsluiter ziet op een Leermiddel en Toets en/of School- en Leerlinginformatiemiddel. Bewerker specificeert in de Privacy Bijsluiter voor welke (in het Convenant opgenomen) doeleinden persoonsgegevens worden verwerkt bij het gebruik zijn product en/of dienst, en welke categorieën Persoonsgegevens daarbij worden verwerkt. Indien

aangegeven in de toelichting in de Privacy Bijsluiter, dient de Bewerker tevens aan te geven onder welke van de in het Convenant omschreven doeleinden bij het gebruik van het product en/of de dienst de Verwerking van Persoonsgegevens plaatsvindt.

4. Bewerker onthoudt zich van verstrekking van Persoonsgegeven aan een Derde, tenzij deze uitwisseling plaatsvindt in opdracht van de Onderwijsinstelling of wanneer dit noodzakelijk is om te voldoen aan een op de Bewerker rustende wettelijke verplichting. In geval van een wettelijke verplichting, verifieert Bewerker voorafgaande de verstrekking de grondslag van het verzoek en de identiteit van de verzoeker. Daarnaast informeert Bewerker de Onderwijsinstelling – indien wettelijk toegestaan - onmiddellijk, zo mogelijk voorafgaand aan de verstrekking.
5. *SPECIFIEKE BEPALING IN GEVAL VAN UITWISSELING VAN HET ONDERWIJSKUNDIG RAPPORT: In aanvulling op het bepaalde in lid 4, geldt dat indien Bewerker wordt verzocht Persoonsgegevens te verstrekken aan een door Onderwijsinstelling aangewezen en geselecteerde Derde, zijnde een andere onderwijsinstelling, de Bewerker slechts tot die verstrekking zal overgaan nadat deze onderwijsinstelling zijn administratieve onderwijsidentiteit (bijvoorbeeld BRIN of OiN), voor zover hij daarover beschikt, kenbaar heeft gemaakt.*
6. *[SPECIFIEKE BEPALING IN GEVAL VAN DISTRIBUTIE VAN LEERMIDDELEN: Partijen zullen jaarlijks bij het opstellen van de leermiddelenlijsten voor het eerstvolgende schooljaar, welke leermiddelenlijsten ten behoeve van de uitvoering van de Product- en Dienstenovereenkomst worden opgesteld, de Privacy Bijsluiter aanvullen en/of wijzigen door het opnemen van de categorieën Persoonsgegevens en het gebruik dat van deze Persoonsgegevens wordt gemaakt, met betrekking tot de (digitale) leermiddelen die op de desbetreffende leermiddelenlijsten worden opgenomen.]*

Artikel 6: Geheimhouding

1. Bewerker zorgt er voor dat een ieder, waaronder haar werknemers, vertegenwoordigers en/of Subbewerkers, die betrokken zijn bij de Verwerking van de Persoonsgegevens deze gegevens als vertrouwelijk behandelt. Bewerker bewerkstelligt dat voor een ieder die betrokken is bij de Verwerking van de Persoonsgegevens een geheimhoudingsovereenkomst of –beding is gesloten.
2. De in dit artikel bedoelde geheimhoudingsplicht geldt niet voor zover Onderwijsinstelling uitdrukkelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te verstrekken, indien het verstrekken van de Persoonsgegevens aan een Derde noodzakelijk is gezien de aard van de door Bewerker aan Onderwijsinstelling te verlenen diensten, of indien er een wettelijke verplichting bestaat om de Persoonsgegevens aan een Derde te verstrekken.

Artikel 7: Beveiliging en controle

1. Bewerker zal, gelijk de Onderwijsinstelling, zorg dragen voor passende technische en organisatorische maatregelen om Persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige Verwerking. Deze maatregelen zullen, met inachtneming van de stand van de techniek en de kosten gemoeid met de implementatie en de uitvoering van de maatregelen, een passend beschermingsniveau verzekeren, zulks met inachtneming van de risico's die het verwerken van Persoonsgegevens, en de aard daarvan, meebrengen.
2. De maatregelen zoals genoemd in artikel 7.1 omvatten in ieder geval:

a. maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Persoonsgegevens die in het kader van de Bewerkersovereenkomst worden verwerkt;

b. maatregelen om de Persoonsgegevens te beschermen tegen met name onopzettelijke of onrechtmatige vernietiging, verlies, onopzettelijke wijziging, onbevoegde of onrechtmatige opslag, toegang of openbaarmaking;

c. maatregelen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Onderwijsinstelling;

d. een passend informatiebeveiligingsbeleid voor de Verwerking van de Persoonsgegevens.

3. Bewerker zal de door haar getroffen informatiebeveiligingsmaatregelen evalueren en verscherpen, aanvullen of verbeteren voor zover de eisen of (technologische) ontwikkelingen daartoe aanleiding geven.

4. In Bijlage 2 worden de afspraken tussen Partijen vastgelegd over de technische en organisatorische beveiligingsmaatregelen, alsmede over de inhoud en de frequentie van de rapportages die Bewerker aan de Onderwijsinstelling oplevert over de beveiligingsmaatregelen. Deze maatregelen liggen in het verlengde van de beveiligingsmaatregelen die de Onderwijsinstelling moet treffen.
5. De Bewerker stelt de Onderwijsinstelling in staat om te kunnen voldoen aan zijn wettelijke verplichting om toezicht te houden op de naleving door de Bewerker van de technische en organisatorische beveiligingsmaatregelen alsmede op de naleving van de in artikel 8 genoemde verplichtingen ten aanzien van Datalekken. Naast rapportages door de Bewerker kan dat aan de hand van, maar niet beperkt tot, een geldige certificering of een gelijkwaardig controle- of bewijsmiddel.
6. In aanvulling op artikel 7, lid 4 heeft de Onderwijsinstelling te allen tijde het recht om, in overleg met de Bewerker en met inachtneming van een redelijke termijn, op eigen kosten, de door Bewerker genomen technische en organisatorische beveiligingsmaatregelen te laten toetsen door een onafhankelijke Register EDP auditor. Partijen kunnen in onderling overleg afspreken dat de audit wordt uitgevoerd door een door Bewerker in te schakelen gecertificeerde en onafhankelijke auditor die een derden-verklaring (TPM) afgeeft. De Onderwijsinstelling wordt geïnformeerd over de uitkomsten van de audit.

Artikel 8: Datalekken

1. Bewerker heeft een passend beleid voor de omgang met Datalekken.
2. Indien Onderwijsinstelling dan wel Bewerker een Datalek vaststelt, dan zal deze de andere Partij onverwijld informeren. Bewerker verstrekt ingeval van een Datalek alle relevante informatie aan Verantwoordelijke met betrekking tot het Datalek, waaronder informatie over eventuele ontwikkelingen rond het Datalek, en de maatregelen die de Bewerker treft om aan zijn kant de gevolgen van het Datalek te beperken en herhaling te voorkomen. Aanvullend informeren Partijen elkaar onverwijld indien blijkt dat de inbreuk op de beveiliging waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van Betrokken zoals bedoeld in artikel 34a, lid 2, AVG.
3. Bewerker stelt bij een Datalek de Verantwoordelijke in staat om passende vervolgstappen te (laten) nemen ten aanzien van het Datalek Bewerker dient hierbij aansluiting te zoeken bij de bestaande processen die Verantwoordelijke daartoe heeft ingericht. Partijen nemen zo spoedig mogelijk alle redelijkerwijs benodigde maatregelen om (verdere) schending of inbreuken betreffende de Verwerking de Persoonsgegevens, en meer in het bijzonder (verdere) schending van de AVG of andere regelgeving betreffende de Verwerking van de Persoonsgegevens, te voorkomen of te beperken.
4. In geval van een Datalek, voldoet Onderwijsinstelling aan eventuele wettelijke meldingsplichten. Partijen kunnen in onderling overleg bepalen of, en zo ja hoe, Bewerker een melding aan de Autoriteit Persoonsgegevens kan verrichten. Op verzoek van de Onderwijsinstelling kan Bewerker Onderwijsinstelling hierbij bijstaan en adviseren. De Onderwijsinstelling zal de Betrokkenen, indien wettelijk vereist, informeren over een dergelijke inbreuk. Partijen zullen te goeder trouw in onderling overleg afspraken maken over de redelijke verdeling van de eventuele kosten die verbonden zijn aan het voldoen aan de meldingsplichten.
5. Over incidenten met betrekking tot de beveiliging, anders dan een Datalek, die vallen buiten het bereik van artikel 1 sub e, informeert de Bewerker de Onderwijsinstelling conform de afspraken zoals neergelegd in Bijlage 2.

Artikel 9: Procedure rechten betrokkenen

1. Een klacht of verzoek van een Betrokkene met betrekking tot de Verwerking van de Persoonsgegevens wordt door de Bewerker onverwijld doorgestuurd naar de Onderwijsinstelling, die verantwoordelijk is voor de afhandeling van het verzoek.
2. Bewerker verleent Onderwijsinstelling – voor zover redelijkerwijs mogelijk - volledige medewerking om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de AVG, meer in het bijzonder de rechten van Betrokkenen zoals een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming van Persoonsgegevens. Partijen zullen te goeder trouw overleggen over de redelijke verdeling van de eventuele kosten die hiermee gemoeid zijn.

Artikel 10: Verwerking buiten de Europese Economische Ruimte

1. Partijen zien er op toe dat voor zover Persoonsgegevens buiten de Europese Economische Ruimte (verder: EER) worden Verwerkt, dit alleen plaatsvindt conform wettelijke voorschriften, en eventuele verplichtingen die in dit verband op Onderwijsinstellingen rusten. Indien gegevens buiten de EER worden verwerkt wordt dit in Bijlage 1 aangegeven, inclusief een opgave van de landen waar de gegevens worden verwerkt.

Artikel 11: Inschakeling Subbewerker

1. Bewerker kan een Subbewerker inschakelen, van wie de identiteit en vestigingsgegevens zullen worden opgenomen in de Privacy Bijsluiter.
2. Bewerker verplicht iedere Subbewerker contractueel de geheimhoudingsverplichtingen, meldingsverplichtingen en beveiligingsmaatregelen na te leven met betrekking tot de Verwerking van Persoonsgegevens welke verplichtingen en maatregelen minimaal dienen te voldoen aan het bepaalde in deze Bewerkersovereenkomst.
3. Bewerker verplicht iedere Subbewerker contractueel om Persoonsgegevens niet verder te verwerken anders dan in het kader van deze Bewerkersovereenkomst is overeengekomen.

Artikel 12: Bewaartermijnen en vernietiging Persoonsgegevens

1. Onderwijsinstelling zal Bewerker adequaat informeren over (wettelijke) bewaartermijnen die van toepassing zijn op de Verwerking van Persoonsgegevens door Bewerker. Bewerker zal de Persoonsgegevens niet langer Verwerken dan overeenkomstig deze bewaartermijnen.
2. Onderwijsinstelling verplicht Bewerker om de in opdracht van Onderwijsinstelling Verwerkte Persoonsgegevens bij de beëindiging van de Bewerkersovereenkomst te (doen) vernietigen, tenzij de Persoonsgegevens langer bewaard moeten worden, zoals in het kader van (wettelijke) verplichtingen, dan wel op verzoek van de Onderwijsinstelling. De Onderwijsinstelling kan op eigen kosten een controle laten uitvoeren of vernietiging heeft plaatsgevonden.
3. Bewerker zal Onderwijsinstelling (schriftelijk of elektronisch) bevestigen dat vernietiging van de Verwerkte persoonsgegevens heeft plaatsgevonden.
4. Bewerker zal alle Subbewerkers die betrokken zijn bij de Verwerking van de Persoonsgegevens op de hoogte stellen van een beëindiging van de Bewerkersovereenkomst en zal waarborgen dat alle Subbewerkers de Persoonsgegevens (laten) vernietigen.

Artikel 13: Tegenstrijdigheid en wijziging Bewerkersovereenkomst

1. In het geval van tegenstrijdigheid tussen de bepalingen uit deze Bewerkersovereenkomst en de bepalingen van de Product- en Dienstenovereenkomst, dan zullen de bepalingen van deze Bewerkersovereenkomst leidend zijn.
2. Indien Partijen van de artikelen in de Model Bewerkersovereenkomst door omstandigheden moeten afwijken, of deze willen aanvullen, dan zullen deze wijzigingen en/of aanvullingen door Partijen worden beschreven en gemotiveerd in een overzicht dat als Bijlage 3 aan deze Bewerkersovereenkomst zal worden gehecht. Het bepaalde in dit lid geldt niet voor aanvullingen en/of wijzigingen van de Bijlagen 1 en 2.
3. Bij belangrijke wijzigingen in het product en/of de (aanvullende) diensten die van invloed zijn op de Verwerking van de Persoonsgegevens wordt, alvorens de Onderwijsinstelling de keuze hiertoe aanvaardt, de Onderwijsinstelling in begrijpelijke taal geïnformeerd over de consequenties van deze wijzigingen. Onder belangrijke wijzigingen wordt in ieder geval verstaan: de toevoeging of wijziging van een functionaliteit die leidt tot een uitbreiding ten aanzien van de te Verwerken Persoonsgegevens, de doeleinden waaronder de Persoonsgegevens worden Verwerkt en het inschakelen van een (andere) Subbewerker. De wijzigingen zullen in Bijlage 1 worden opgenomen.
4. Wijzigingen in de artikelen van de Bewerkersovereenkomst kunnen uitsluitend in gezamenlijkheid worden overeengekomen.

5. In het geval enige bepaling van deze Bewerkersovereenkomst nietig, vernietigbaar of anderszins niet afdwingbaar is of wordt, blijven de overige bepalingen van deze Bewerkersovereenkomst volledig van kracht. Partijen zullen in dat geval met elkaar in overleg treden om de nietige, vernietigbare of anderszins niet afdwingbare bepaling te vervangen door een uitvoerbare alternatieve bepaling. Daarbij zullen partijen zoveel mogelijk rekening houden met het doel en de strekking van de nietige, vernietigde of anderszins niet afdwingbare bepaling.

Artikel 14: Duur en beëindiging

1. De looptijd van deze Bewerkersovereenkomst is gelijk aan de looptijd van de tussen Partijen gesloten Product- en Dienstenovereenkomst, inclusief eventuele verlengingen daarvan.
2. Deze Bewerkersovereenkomst eindigt van rechtswege bij de beëindiging van de Product- en Dienstenovereenkomst. De beëindiging van deze Bewerkersovereenkomst zal Partijen niet ontslaan van hun verplichtingen die voortvloeien uit deze Bewerkersovereenkomst die naar hun aard worden geacht ook na beëindiging voort te duren.

BIJLAGE 1: PRIVACY BIJSLUITER [naam product/dienst]

Scholen maken in toenemende mate gebruik van digitale toepassingen binnen het onderwijs. Bij het gebruik en levering van deze producten en diensten zijn gegevens nodig die te herleiden zijn tot personen (zoals leerlingen). Scholen moeten met Bewerkers afspraken maken over het gebruik van die Persoonsgegevens. Deze bijsluiter geeft scholen informatie over de dienstverlening die bewerker verleent en welke persoonsgegevens de Bewerker daarbij verwerkt. Alles bij elkaar eigenlijk over de vraag "wie, wat, waar, waarom en hoe" wordt omgegaan met de privacy van de betrokken personen wiens gegevens worden uitgewisseld.

Het gebruik van deze Privacy Bijsluiter helpt Onderwijsinstellingen om beter te begrijpen wat de werking van het product en/of dienst is en welke gegevens daarvoor worden uitgewisseld.

In het kader van de herkenbaarheid is het wenselijk dat Bewerkers zo veel mogelijk op uniforme wijze gebruik maken van de Privacy Bijsluiter. Afwijkingen van dit model zijn weliswaar mogelijk, maar dienen bij voorkeur beperkt te blijven. Indien de ruimte in deze bijlage onvoldoende is om de benodigde informatie te beschrijven, is het mogelijk de informatie op te nemen in separate Bijlage(n), welke als volgt genummerd worden: "Bijlage 1A", "Bijlage 1B", etc.. Deze Bijlagen worden aan de Bewerkersovereenkomst gehecht.

A. Algemene informatie

Naam product en/of dienst	:
Naam Bewerker en vestigingsgegevens	:
Beknopte uitleg en werking product en dienst	:
Link naar leverancier en/of productpagina	:
Doelgroep (zoals PO/VO, onderbouw/bovenbouw)	:
Gebruikers	: leerlingen/ouders/verzorgers/docenten

B. De specifieke diensten

Omschrijving van de specifiek verleende diensten en bijbehorende Verwerkingen

1. Verwerkingen die een onlosmakelijk onderdeel vormen van de aangeboden dienst.

a. [….]
b. [….]
[….]

2. Omschrijving van de optionele Verwerkingen die de bewerker aanbiedt

Toelichting: Het gaat hier om aanvullende diensten en bijhorende Verwerkingen die geen onlosmakelijk onderdeel vormen van de aangeboden dienst. Dit zijn bijvoorbeeld optionele diensten voor de Onderwijsinstelling die behulpzaam kunnen zijn voor de Onderwijsinstelling t.b.v. het primaire (leer)proces en administratieve werkzaamheden

De Onderwijsinstelling dient een keuze te maken (opdracht te geven) voor het afnemen van deze diensten. Dat kan door de keuze schriftelijk aan te geven in deze bijlage (bijvoorbeeld door het aanvinken van een tick-box☑).

Instemming kan ook plaatsvinden doordat de Onderwijsinstelling in de praktijk de dienst activeert, bijvoorbeeld door een product of dienst aan of uit zetten. De Onderwijsinstelling die op deze wijze de keuze maakt, dient dit op basis van eerder verstrekte informatie (zoals bijvoorbeeld opgenomen in deze bijsluiter) te kunnen doen.

a. [….]
b. [….]
[….]

C. Doeleinden voor het verwerken van gegevens

De Bewerker dient in deze Bijsluiter expliciet aan te geven of deze:

- □ I. leverancier is van een digitaal product en/of digitale dienst bestaande uit leerstof en/of toetsen, of
- □ II. (tevens) leverancier is van een School- en Leerlinginformatiemiddel.

Ad I. Indien de Bewerker leverancier is van een digitaal product en/of digitale dienst bestaande uit Leermiddelen en Toetsen, dan zijn de mogelijke doelstellingen van deze producten en diensten omschreven in het daarop betrekking hebbende onderdeel van artikel 5 lid 1 van het Convenant Digitale Onderwijsmiddelen en Privacy 2.0. Deze hoeven in deze Bijsluiter verder niet benoemd te worden.

Ad II. (Alleen) indien de bewerker (tevens) leverancier is van een digitaal product en/of digitale dienst bestaande uit een School- en Leerlinginformatiemiddel dan dient in deze Privacy Bijsluiter expliciet te worden aangegeven voor welke doeleinden er Persoonsgegevens worden verwerkt bij het gebruik van het product en/of de dienst. De Bewerker dient hierbij zo veel mogelijk aansluiting te zoeken bij de in artikel 5 lid 2 van het Convenant Digitale Onderwijsmiddelen en Privacy 2.0 opgenomen lijst met doeleinden.

D. Categorieën en soorten persoonsgegevens

Omschrijving en opsomming categorieën Persoonsgegevens die gebruikt worden:

Eventuele optionele Persoonsgegevens (die worden niet standaard gevraagd en opgeslagen):

Soorten van gegevens (zoals bijzondere gegevens, of financiële gegevens):

E. Algemene informatie over getroffen beveiligingsmaatregelen:

Voor de genomen veiligheidsmaatregelen wordt kortheidshalve verwezen naar Bijlage 2 bij de Bewerkersovereenkomst.

Specifieke beveiligingsmaatregelen voor deze dienst/product [indien van toepassing]:

Eventuele certificeringen:

Audits/derden-verklaringen:

Plaats/Land van opslag en Verwerking van de Persoonsgegevens:

F. Subbewerkers

Bewerker maakt voor dienst/product gebruik van de volgende Subbewerkers:

[partijnaam, beknopte omschrijving taak/dienst waaruit blijkt welke informatie wordt Verwerkt door deze Subbewerker]

Plaats/Land van opslag en Verwerking van de Persoonsgegevens (indien de Persoonsgegevens buiten de EER worden verwerkt wordt apart opgave gedaan van de landen waar de Persoonsgegevens worden verwerkt).

G. Contactgegevens

Voor vragen of opmerkingen over deze bijsluiter of de werking van dit product of deze dienst, kunt u terecht bij: [contactgegevens].

H. Versie [versie nummer en datum laatste aanpassing]

Deze privacy bijsluiter maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 2.0, een initiatief van de PO-Raad, VO-raad, de verschillende betrokken ketenpartijen (GEU, KBB-e en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: http://ww.privacyconvenant.nl.

BIJLAGE 2: Technische en organisatorische beveiligingsmaatregelen

De Bewerker is overeenkomstig de AVG en artikel 7 Bewerkersovereenkomst verplicht technische en organisatorische maatregelen te nemen ter beveiliging van de Verwerking van Persoonsgegevens.

Indien de ruimte in deze bijlage onvoldoende is om de benodigde informatie te beschrijven, is het mogelijk de informatie op te nemen in separate Bijlage(n), welke als volgt genummerd worden: "Bijlage 2A", "Bijlage 2B", etc.. Deze Bijlagen worden aan de Bewerkersovereenkomst gehecht.

Omschrijving van de maatregelen zoals bedoeld in artikel 7.2 Bewerkersovereenkomst

I. Omschrijving van de maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Verwerking van Persoonsgegevens.

Meer in het bijzonder de uitwerking welke (groepen) medewerkers van de Bewerker toegang hebben tot welke Persoonsgegevens, inclusief een omschrijving van handelingen die deze medewerkers uit mogen voeren met de persoonsgegevens.

a. (groepen van) medewerkers die toegang hebben tot welke Persoonsgegevens:

b. handelingen die deze medewerkers uitvoeren met de Persoonsgegevens:

II. Omschrijving van de maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag, Verwerking, toegang of openbaarmaking.

Meer in het bijzonder de uitwerking van de door Bewerker getroffen technische en organisatorische (beveiligings-)maatregelen en de daarbij gehanteerde beveiligingsnorm.

[beschrijving beveiliging applicatie/platform]

[beschrijving wijze van identificatie/authenticatie/autorisatie en beveiliging daarvan]

[beschrijving beveiliging van wijze van uitwisseling/transport van gegevens]

III. Omschrijving van de maatregelen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan de Onderwijsinstelling.

[zoals een periodieke analyse van (security) incidenten, het periodiek uitvoeren van een extern/intern kwetsbaarhedenonderzoek (ethical hack) of het periodiek uitvoeren van controles op beveiliging van systemen]

Rapportage (artikel 7.4 van de Bewerkersovereenkomst

Bewerker rapporteert periodiek met een frequentie van […] maal per jaar, uiterlijk op […] aan Verantwoordelijke over de door Bewerker genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin.]

[contactgegevens helpdesk/servicedesk voor beveiligingsincidenten]

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging

Afspraken over het informeren in geval van Datalekken en/of incidenten met betrekking tot beveiliging, met name over

- De wijze waarop monitoring en identificatie van incidenten plaatsvindt,
- De wijze waarop informatie wordt gedeeld:
  - Op welke manier (via e-mail, telefoon);
  - Aan wie gericht (contactpersonen en contactgegevens);
  - Met wie kan (bij vervolgacties) contact worden opgenomen.
- Informatie die in ieder geval over een incident gedeeld moet worden
  - De kenmerken van het incident, zoals: datum en tijdstip constatering, samenvatting incident, kenmerk en aard incident (op wat voor onderdeel van de beveiliging ziet het, hoe heeft het zich voorgedaan, heeft het betrekking op lezen, kopiëren, veranderen, verwijderen/vernietigen en/of diefstal van persoonsgegevens);
  - De oorzaak van het beveiligingsincident;
  - De maatregelen die getroffen zijn om eventuele/verdere schade te voorkomen;
  - Benoemen van betrokkenen die gevolgen kunnen ondervinden van het incident, en de mate waarin;
  - De omvang van de groep betrokkenen;
  - Het soort gegevens dat door het incident wordt getroffen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens of leerprestaties).
- Eventuele afspraken of, en zo ja hoe, Bewerker een melding aan de Autoriteit Persoonsgegevens kan verrichten.

Versie

[versie nummer en datum laatste aanpassing]

Deze privacy bijsluiter maakt onderdeel uit van de afspraken die zijn gemaakt in het Convenant Digitale Onderwijsmiddelen en Privacy 2.0, een initiatief van de PO-Raad, VO-raad, de verschillende betrokken ketenpartijen (GEU, KBB-e en VDOD) en het ministerie van Onderwijs, Cultuur en Wetenschap. Meer informatie hierover vindt u hier: http://ww.privacyconvenant.nl.

c. Checklist privacy

Zet een kruisje onder het antwoord dat van toepassing is.

	OK	Niet OK	Uitleg op:
Leerlingenadministratie:			
Ouders weten wat bijgehouden wordt en waarom			3
Ouders weten waartoe het geven van cijfers dient			3
Alle gegevens worden alleen gebruikt voor het doel waarvoor ze zijn verzameld			3
Er worden niet meer gegevens verzameld dan nodig is om onderwijs te kunnen geven.			3.4
Het is ouders bekend dat ze inzage hebben in de geregistreerde gegevens en dat ze correctie kunnen verlangen			3.5
Vijf jaar na uitschrijving van de leerling worden de gegevens van de leerling verwijderd.			10.3
Twee jaar nadat de leerling van school is, wordt het leerlingdossier verwijderd, voor overstap naar SBO geldt een bewaartermijn van 3 jaar.			10.3
Vertrekkende leerkrachten worden direct in Parnassys op “niet actief”gezet.			12
Wanneer een leerkracht vertrekt, wordt de mogelijkheid om in te loggen in het schoolnetwerk en diverse schoolgerelateerde websites stopgezet (Inspectie, Mijn Vensters, schoolwebsite, …)			12
Het Office365-account van vertrekkende leerkrachten wordt ontoegankelijk gemaakt.			12
Leermateriaal			
Er is een bewerkersovereenkomst voor alle software waarbij leerlinggegevens worden uitgewisseld, ondertekend door het bevoegd gezag (CvB)			4
Beeldmateriaal			
Bij de aanmelding wordt ouders toestemming gevraagd voor elk gebruik van beeldmateriaal van hun kind. Kinderen waarvoor geen toestemming is, worden niet op de website, schoolkrant o.i.d. geplaatst. Jaarlijks worden ouders eraan herinnerd dat die toestemming eventueel ingetrokken kan worden.			7
Sociale media			
Leerlingen maken in schoolverband geen gebruik van sociale media zolang dat qua leeftijd niet is toegestaan (Facebook bijv. 12 jaar)			8
Zowel leerlingen als leerkrachten houden zich volledig aan het protocol Sociale Media			Protocol (bijlage)
Overstap naar andere school			
Ouders kunnen kennis nemen van de registraties van hun kind en kunnen correctie verlangen van de gegevens, alsmede van hetgeen doorgegeven wordt aan de vervolgschool.			9
Gegevensbeveiliging			
We gebruiken voldoende complexe wachtwoorden waar het om beveiliging van leerlingengegevens gaat.			10
Er hangen/liggen geen briefjes met gebruikersnamen/wachtwoorden op een zichtbare plaats en opgeslagen wachtwoorden bevinden zich altijd achter een beveiligde inlog op de pc.			11.2
Bij het verlaten van de werkplek meldt men zich steeds af of wordt op zijn minst de computer “gelockt”. Wanneer men in de klas wordt opgevolgd door een collega, meldt men zich af.			10
Documentenhiërarchie: directie/locatieleider – IB-er – leerkracht – leerlingen. Men kan steeds de eigen documenten zien en die van degene(n) die in het rijtje na hem komt, maar naar links toe zijn de documenten niet toegankelijk.			10.2
Er ligt geen privacygevoelig materiaal “voor het grijpen”: cijferlijsten etc.			11.2

We werken nooit onder andermans inlog en we laten ook nooit anderen onder onze eigen inlog werken.			11.2
Schoolmail lezen op je mobiel, tablet of thuispc? Dan is die op zijn minst beveiligd met een pincode, tekenpatroon of wachtwoord.			11.2
We slaan geen privacygevoelige gegevens op op de pc. Alleen op de server of in Sharepoint			11.3
Thuis bestanden van school bekijken en bewerken. De oude apparatuur wordt voor de afvoer leeg gemaakt met een speciaal programma of de harde schijf wordt mechanisch vernietigd.			11.3, 11.4
We laten onze kinderen niet op de schoolpc spelen onder onze eigen inlog (of die van de groep).			13
Functionaris gegevensbescherming			
De school heeft een functionaris voor de gegevensbescherming (FG), met duidelijk omschreven taken en ingeschreven bij de Autoriteit Persoonsgegevens.			14
Mocht een datalek voorkomen, dan melden we dat bij de FG. Samen oordelen we of het lek gemeld moet worden bij de Autoriteit Persoonsgegevens en de betrokkene(n).			13.3