Handboek Informatiebeveiliging en privacy

Versie 0.9, 23 maart 2018

Inhoudsopgave

Inleiding

Informatie en ict zijn noodzakelijk in de uitvoering van het onderwijs. Omdat we met persoonsgegevens van medewerkers, leerlingen en anderen werken, is privacywetgeving daarop van toepassing. Deze wetgeving bepaalt niet alleen onder welke voorwaarden persoonsgegevens gebruikt mogen worden, maar geeft ook aan dat er passende technische en organisatorische maatregelen op het gebied van informatiebeveiliging en privacy (afgekort: IBP) genomen moeten worden om persoonsgegevens te beschermen. Hiervoor is er binnen Innoord een IBP-beleidsplan opgesteld. Dit plan is op te vragen bij de bovenschools ict-coördinator.

Dit handboek is bedoeld om uitvoering te geven aan het IBP-beleidsplan. In het handboek staan richtlijnen, procedures, afspraken en praktische handreikingen die nodig zijn om informatiebeveiliging en privacy goed te regelen. Deze maatregelen nemen we niet alleen omdat de wet dit voorschrijft, maar ook op basis van de normen en waarden die wij vanuit onze visie op onderwijs met elkaar delen en uitdragen:

Ieder kind heeft een talent en elk talent is even belangrijk. Ongeacht afkomst, cultuur, IQ, opvoeding of geloof. Het is de kunst dat talent te vinden en tot bloei te laten komen. En dat talent te versterken. Dat schept zelfvertrouwen, zelfstandigheid en zelfbewustzijn. En dat positieve zelfbeeld zorgt later voor actieve wereldburgers die volwaardig meedoen in de maatschappij.

Het handboek is onderverdeeld in twee delen voor afzonderlijke doelgroepen:

Deel A - Alle medewerkers
Dit deel bevat de algemene informatie die voor alle medewerkers van Innoord van belang is. Van alle medewerkers wordt verwacht dat zij op de hoogte zijn van de afspraken die hierin vermeld staan en hier ook naar handelen. In dit deel wordt o.a. antwoord gegeven op de volgende vragen:

- Welke afspraken gelden er voor mij als het gaat om de verwerking van leerlinggegevens?
- Waar moet ik mij aan houden bij het gebruik van sociale media?
- Welke gegevens bewaart de school van mij en anderen en waarom?
- Waar moet ik op letten bij het gebruik van beeldmateriaal en online diensten?
- Waar moet ik op letten bij het uitwisselen van gegevens met andere partijen?
- Als ik gegevens kwijt ben of ik heb een vermoeden van misbruik, bij wie moet ik dan zijn?
- Waar moet ik persoonsgegevens of persoonlijke informatie opslaan?

Deel B – Schoolleiders en leidinggevenden
In dit deel is informatie terug te vinden die vooral van belang is voor de schoolleider: hoe zorg ik ervoor dat het IBP-beleid op mijn school goed geregeld is? In dit deel wordt o.a. antwoord gegeven op de volgende vragen:

- Wat moet ik met ouders regelen rondom privacy?
- Welke afspraken moet ik maken met mijn medewerkers in het kader van privacy?
- Wat moet ik afspreken met medewerkers in het kader van geheimhouding?
- Wat moet ik weten over datalekken?
- Wat moet ik weten over cameratoezicht?
- Wat moet ik weten als het gaat om het verlenen van toegang tot persoonsgegevens?
- Hoe lang moet ik persoonsgegevens bewaren?
- Welke afspraken maak ik over devices die in bruikleen worden gegevens?
- Wat moet ik weten over externe partijen die namens de school persoonsgegevens verwerken?
- Welke rollen en verantwoordelijkheden t.a.v. IBP zijn er binnen de schoolorganisatie belegd?
- Welke technische maatregelen moet ik geregeld hebben binnen de school?
- Hoe kan ik aantonen dat ik IBP op orde heb?

Deel A
Informatie voor alle medewerkers

Gedragsregels Privacy

Privacy op school gaat over de bescherming van gegevens van personen. Dit wordt geregeld in de Algemene Verordening Gegevensbescherming (voorheen de Wet Bescherming Persoonsgegevens).

Binnen Innoord worden gegevens van zowel leerlingen, ouders als medewerkers verwerkt. Welke gegevens dit zijn en voor welke doeleinden deze worden verwerkt staat omschreven in het privacyreglement, zie **bijlage A.**

Voor een veilig schoolklimaat is het belangrijk dat de afspraken rondom informatiebeveiliging en privacy door alle werknemers worden nageleefd en uitgedragen. Daarom zijn er gedragsregels opgesteld waaraan alle medewerkers van Innoord zich dienen te houden.

De afspraken zijn verdeeld in twee onderdelen:

A. Waar en hoe verwerk ik persoonsgegevens?
B. Hoe houd ik indringers op afstand?

Hieronder volgen per onderdeel de gedragsregels die voor iedereen gelden bij de verwerking van gegevens van zowel leerlingen, ouders als die van medewerkers.

A. Waar en hoe verwerk ik persoonsgegevens?

1. **Privacywetgeving**
   Ken de belangrijkste begrippen en uitgangspunten van privacy en de wet. Wij gebruiken hiervoor de 5 vuistregels voor privacy van Kennisnet. Om persoonsgegevens te mogen verwerken (verzamelen, uitwisselen, etc.) kent de AVG een aantal uitgangspunten. Deze voorwaarden gelden voor elke school en zijn samengevat tot 5 vuistregels:

   a. *Doel en doelbinding*
   Persoonsgegevens worden altijd verzameld met een vooraf vastgesteld en concreet doel. Zoals: onderwijs geven en begeleiden, leerlingen , voldoen aan de wet. Persoonsgegevens mogen alleen worden verwerkt om het vooraf vastgestelde doel te bereiken. Bijvoorbeeld: Een telefoonnummer voor noodgevallen.

   b. *Grondslag*
   Persoonsgegevens mogen alleen verwerkt worden als de AVG hier een grond voor noemt. Eris een wettelijke grondslag als:
   - er een wettelijke plicht bestaat om deze gegevens te verstrekken. Bijv. voor bekostiging, inspectie, overdrachtsdossier, etc.;
   - er toestemming is verkregen van de ouders/verzorgers. Bijv. voor de begeleiding van een leerling door externe onderwijsspecialisten, foto's op website, etc.;

- de partij een publiekrechtelijke taak heeft. Bijv. de uitwisseling van informatie met samenwerkingsverbanden;
- dit nodig is voor het uitvoeren van een overeenkomst met de ouders/verzorgers. Bijv. voor de TSO van kinderen;
- er sprake is van een gerechtvaardigd belang, zoals het goed laten werken van digitale leermiddelen. Bijv. voor Basispoort en educatieve uitgeverijen.

c. *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 en het doel kan niet met minder dan deze verzamelde gegevens worden bereikt. Het gaat er dus om dat scholen uitsluitend gegevens verzamelen die écht nodig zijn om het doel te bereiken.

d. *Transparantie en rechten van de betrokkene*
De betrokkene (dus: degene van wie de persoonsgegevens worden verwerkt) is vooraf in begrijpelijke taal geïnformeerd over wat er precies aan informatie wordt verwerkt en wat het doel daarvan is. De betrokkenen moeten op de hoogte worden gesteld van hun rechten als het gaat om de verwerking van persoonsgegevens door de school/de stichting.

e. *Data-integriteit*
Kloppen de persoonsgegevens die ik gebruik nog steeds? Zijn de gegevens op het juiste moment, op de juiste plaats en voor de juiste mensen beschikbaar? Heb ik onjuiste gegevens gecorrigeerd of verwijderd?

2. **Uitwisselen gegevens**
Als je gegevens uitwisselt, houd dan rekening met bovenstaande punten. Kijk hier voor een overzicht van partijen met wie je (wel en niet) gegevens mag uitwisselen en de wijze waarop dat moet gebeuren. In bepaalde gevallen heb je ook toestemming nodig. Verstuur persoonsgegevens bij voorkeur niet als bijlage per mail, verstuur in plaats hiervan een link met de online bewaarplaats van de benodigde gegevens.

3. **Bewaren van persoonsgegevens**
Persoonsgegevens worden opgeslagen op de daarvoor aangewezen plaatsen. Bekijk voor meer info hierover het onderdeel Document- en datamanagement.

4. **Rechten ouders**
Ouders hebben rechten als het gaat om de privacy van hun kind. Denk aan recht op inzage, correctie of verwijdering van de persoonsgegevens.

5. **Publiceren beeldmateriaal**
Foto's, video's of persoonlijke informatie van en over leerlingen (en ouders) publiekelijk delen? Zorg altijd dat je schriftelijke toestemming hebt van de ouders. Lees **hier** hoe dit wordt geregeld.

B. Hoe houd ik indringers op afstand?

6. **Account en wachtwoord**
   Je wachtwoord en account zijn privé en worden niet gedeeld met anderen. Dit betekent:
   a. Als je weggaat bij je computer vergrendel je je computer (Windowstoets + L)
   b. Laat anderen nooit onder je account werken.
   c. Schrijf je wachtwoord nooit op, maar gebruik een wachtwoordkluis. Lees hier voor meer info over wachtwoordkluizen.

7. **Mobiele devices**
   Bewaar laptops of tablets altijd op een veilige plek, zeker tijdens vakantieperiodes. Het is een open deur, maar toch gebeurt het heel erg makkelijk. Maak elkaar er dus op attent als je een laptop of tablet onbeheerd ziet liggen. Als je computer gestolen wordt, heeft dat gevolgen voor de school en de leerling.

8. **Phisingmail**
   Klik alleen op linkjes en open alleen bijlagen in e-mails van betrouwbare afzenders en pas op met het downloaden van bestanden. Virussen kunnen makkelijk worden binnengehaald via (phising)mails. In het criminele circuit is dit een veelgebruikte methode om aan jouw gegevens te komen. Ook kunnen de gegevens op je computer versleuteld worden (ransomeware).

Gebruik Sociale media

Sociale media kunnen een waardevolle toevoeging zijn op de manier waarop wij met collega's, ouders, leerlingen en anderen communiceren. Zo bieden ze talrijke mogelijkheden tot interactie zoals het ouderportaal, posts, blogs en fora.
Innoord is zich ervan bewust dat veel collega's, zowel privé als zakelijk, participeren in sociale media. Het is daarom belangrijk dat de invloed van sociale media niet wordt onderschat en op een verantwoorde wijze wordt gebruikt. Want alles wat online wordt gezegd – of het nu in woorden of met beelden is – kan Innoord beïnvloeden.

1. **Identificeer jezelf**
   Een belangrijk principe is openheid en eerlijkheid. Als je online schrijft over Innoord, gebruik dan je echte naam, vermeld voor wie je werkt en wat je functie is. Schrijf vanuit jezelf, in de eerste persoon en maak duidelijk dat je op persoonlijke titel schrijft. Voeg zo nodig een tekst toe als: 'De hier gepubliceerde uitingen vertegenwoordigen uitsluitend mijn persoonlijke meningen en opvattingen en komen niet noodzakelijkerwijs overeen met die van Innoord'.

2. **Neem de bestaande richtlijnen in acht**
   Zorg ervoor dat jouw online activiteiten niet botsen met de regels van Innoord op het gebied van gedrag, privacy, vertrouwelijkheid en de richtlijnen voor pers en publiciteit. Het is voor medewerkers van Innoord niet toegestaan standpunten en/of overtuigingen uit te dragen die in strijd zijn met de missie en visie van de school. Als je uit naam van Innoord sociale media gebruikt volg dan de huisstijl zoals het logo.

3. **Zet je expertise in**
   Zorg ervoor dat je deskundig bent in de onderwerpen waarover je schrijft. Zeker als het te maken heeft met Innoord en de dienstverlening. Baseer je op objectieve en controleerbare feiten.

4. **Neem verantwoordelijkheid**
   Elke medewerker is persoonlijk verantwoordelijk voor zijn of haar online gedrag en de content die hij of zij op internet plaatst. Doe dit op een verantwoorde wijze. Schrijf niet negatief over anderen. Als je verwijst naar relevante partijen, plaats dan waar mogelijk een link naar hun website. En indien je over gevoelige of omstreden onderwerpen schrijft, zorg dan dat je hiervoor van tevoren toestemming hebt.

5. **Wees kritisch**
   Innoord beschouwt het niet als zijn taak om alle online bijdragen van medewerkers te controleren. Het is dan ook belangrijk dat je zelf kritisch nadenkt over de mogelijke impact die een online bijdrage kan hebben, niet alleen op jezelf, maar ook op Innoord. Deel alleen kennis en informatie over de school als het geen vertrouwelijke of persoonlijke informatie betreft en andere betrokkenen en de naam van de school niet schaadt.Wel worden online publicaties over Innoord gemonitord. Mochten we daarbij een ongeoorloofde publicatie tegenkomen, dan kan je leidinggevende je verzoeken de publicatie van internet te verwijderen of aan te

passen. Als het niet mogelijk is een vermelding te plaatsen, dan distantieert Innoord zich van de publicatie.

6. **Gebruik bronvermelding**
   Zorg altijd voor een duidelijke bronvermelding wanneer je naar andere publicaties en/of onderzoeken verwijst. Respecteer auteurs- en portretrechten, trademarks en copyrights op muziek, video, tekst en foto's e.d.

7. **Alleen op persoonlijke titel**
   Uitspraken van medewerkers op internet kunnen misbruikt of onjuist geïnterpreteerd worden. Communiceer dan ook uitsluitend op persoonlijke titel en niet als woordvoerder van Innoord, tenzij je hiervoor toestemming hebt.

8. **Geen perscontact, zonder overleg**
   Er is een mogelijkheid dat je via sociale netwerken in contact komt met journalisten. Voor online mediacontacten gelden dezelfde regels als voor offline perscontacten. Raadpleeg altijd je leidinggevende.

9. **Communiceer respectvol**
   Online discussies maken soms emoties los. Blijf altijd fatsoenlijk, professioneel en respecteer andermans mening, cultuur, normen en waarden. Waak voor taalgebruik dat als beledigend of kwetsend kan worden ervaren. Wees voorzichtig met het aangaan van discussies.

10. **Vergeet niet: Google onthoudt alles**
    Alles wat je online publiceert blijft lang bestaan. Houd dit in gedachte voordat je iets op internet plaatst.

11. **Bij twijfel neem contact op**
    Als je twijfels hebt over een post, commentaar of reactie op het internet neem dan contact op met je leidinggevende. Indien nodig, corrigeer snel.

12. **Deel geen informatie over personen**
    Doe dit vooral in persoon of desnoods via de telefoon. Wat je communiceert via social media kan makkelijk anders worden geïnterpreteerd door de lezer als je hier niet alert op bent.

In het verlengde van bovenstaande is het ook van belang dat leerlingen zich bewust zijn van risico's en er goede afspraken met hen gemaakt worden in het kader van privacy. In **bijlage I** is een voorbeeld opgenomen van dergelijke afspraken. Van iedere school wordt verwacht dat ze een dergelijk protocol hebben en toepassen.

Privacyreglement

Het privacyreglement maakt duidelijk (transparant) aan de personen van wie gegevens worden verzameld (ook wel betrokkenen genoemd) waarvoor de verzamelde gegevens nodig zijn en welke gegevens dit zijn (doel en doelbinding uit de vuistregels).

Ook is hierin te lezen wie binnen de school toegang heeft tot deze gegevens, hoe de gegevens zijn beveiligd en met wie ze uitgewisseld mogen worden.

Het reglement is in te zien via de website www.innoord.nl/privacy Het reglement is ook als **bijlage A** toegevoegd bij dit handboek.

Ouders worden via het inschrijfformulier en via de website van de scholen gewezen op het privacyreglement.

Toestemming

Beeldmateriaal
Ouders, maar ook medewerkers, moeten altijd toestemming geven voor het gebruik van hun beeldmateriaal of die van hun kinderen. Die toestemming moet specifiek zijn. Dat betekent dat het voor ouders en medewerkers duidelijk moet zijn voor welk gebruik van het beeldmateriaal ze toestemming geven. Bijvoorbeeld voor het gebruik op de website, in een nieuwsbrief of de schoolgids. Ouders en medewerkers moeten ook de mogelijkheid hebben deze toestemming weer in te trekken.

De school moet een veilige omgeving zijn voor alle kinderen (en hun ouders) en zij moeten niet het risico lopen ongewenst gefotografeerd te worden.
Daarom wordt, voorafgaand aan een activiteiten, aan ouders gevraagd om terughoudend te zijn met het maken van foto's en video's en is het niet toegestaan om foto- of video-opnames die gemaakt zijn op school te delen via sociale media of te gebruiken voor commerciële doeleinden.

Wanneer er activiteiten georganiseerd worden, zijn er vaak ouders die foto's of video's maken bijvoorbeeld bij feestelijke gelegenheden. We maken hierbij onderscheid tussen twee situaties:

- Ouders in algemene zin op het terrein van Innoord, bijvoorbeeld op het schoolplein. Als je ouders hier foto's of video's ziet maken, spreek ze hier dan op aan en wijs ze op de privacy van (andere) leerlingen. Echter is dit niet helemaal tegen te gaan en is er een grote mate van eigen verantwoordelijkheid van de ouders.
- Ouders die meegaan op schoolactiviteiten. Dit vereist duidelijke afspraken over het maken van beeldmateriaal. Zorg dat ouders alleen foto's en video's maken van kinderen wier ouders hiervoor specifiek toestemming hebben gegeven.

Het maken van foto's of video-opnamen van een leerling door (een medewerker van) Innoord geschiedt altijd op basis van toestemming van ouders/voogden. Deze toestemming wordt in ieder geval eens per schooljaar aan ouders gevraagd. Ook bij de inschrijving van een leerling wordt hier toestemming voor gevraagd.

Het is op de Innoord scholen gebruikelijk dat er tijdens de lessen video-opnamen worden gemaakt. Deze opnamen zijn bestemd om het lesgeven van de groepsleerkracht te verbeteren en worden niet buiten school gebruikt.

Af en toe worden er foto's video-opnamen gemaakt die gebruikt kunnen worden als voorlichtingsmateriaal. Als een kind hierop te zien is, kunnen deze opnamen alleen met toestemming van de ouder(s)/voogd(en) als zodanig worden gebruikt.

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

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

Uitwisseling persoonsgegevens

Wanneer je gegevens uit wil wisselen met externen, zoals bijvoorbeeld de logopedist, een arbo- of schoolarts, jeugdzorg of een schoolbegeleidingsdienst dan is het nodig om toestemming te vragen van ouders. Zorg dat je de toestemming registreert en hou daarbij ook rekening met de verdeling van het ouderlijk gezag. Voor de uitwisseling van leerlinggegevens met het samenwerkingsverband of een andere school gelden aparte afspraken. Kijk hieronder in de tabel met welke partijen je gegevens mag uitwisselen en op welke manier.

Verstrekking aan	Doel	Uitwisseling toegestaan	Wijze waarop	Toestemming nodig?
Dienst Uitvoering Onderwijs	Bekostiging*	Ja	Koppeling ParnasSys	Nee
Educatieve uitgeverijen en Basispoort	Gebruik digitale leermiddelen	Ja	Koppeling ParnasSys	Nee
Basisscholen of scholen voor voortgezet onderwijs	Overdracht leerlingdossier (na aanmelding)*	Ja	Koppeling OSO	Nee (wel inzage)
Externe Onderwijsspecialisten	Zorgbegeleiding van een leerling	Ja	Verstrekken account	Ja
Stagiaires	Opleiden	Nee	n.v.t.	Nee
Samenwerkingsverband	Toelaatbaarheidsverklaring afgeven*	Ja, zie ook: https://passendonderwijsenprivacy.nl	n.t.b.	Nee (wel overeenkomst met stagiaire)
TSO	Tussenschoolse opvang	Ja	n.t.b.	Ja
Activiteitencommissie	Innen ouderbijdrage	Ja	n.t.b.	Ja
GGD/JGZ	Bezoek schoolarts	Nee	n.v.t.	n.v.t.
Inspectie van het onderwijs	Toezicht*	Ja	Via ISD (internet schooldossier)	Nee
Administratiekantoor	Salarisadministratie en HR-management	Ja	n.t.b.	Nee
Leerplicht Gemeente	Controle verzuim	Ja	Verzuimloket	Nee

* Wettelijk verplicht

Datalekken

Zijn er leerlinggegevens verloren gegaan? Is je laptop gestolen? Heb je last van een virus waardoor je niet meer bij je bestanden kunt? Of vertrouw je iets niet? Dan ben je verplicht dit zo snel mogelijk te melden via je schooldirecteur in verband met de meldplicht datalekken.

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

Voorbeelden van datalekken zijn:

- een e-mail die aan een verkeerd persoon geadresseerd is
- een kwijtgeraakte USB-stick
- inloggegevens die openbaar zijn geworden
- een gestolen iPad
- een gehackte computer
- kwijtgeraakte documenten

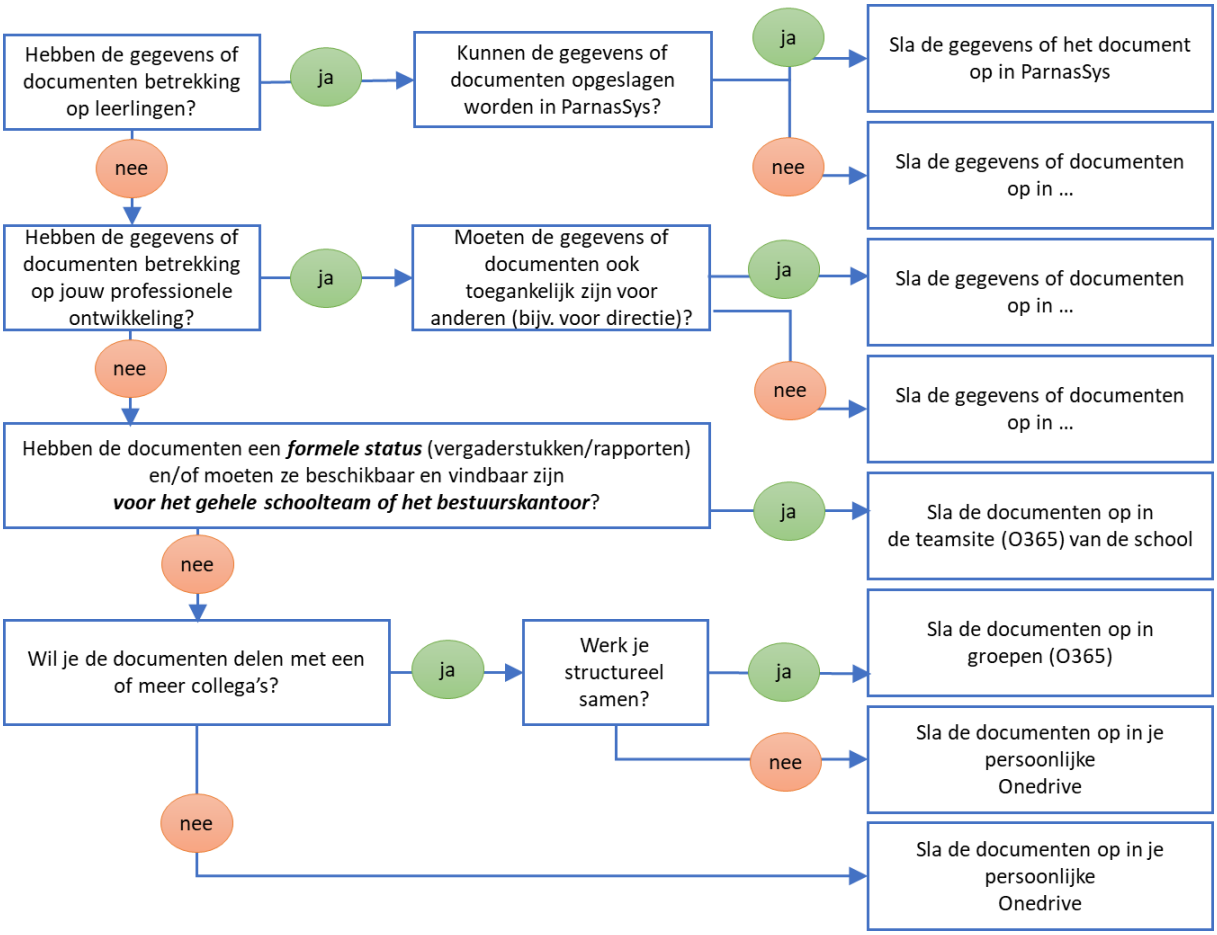
Beoordelen datalek
Het bevoegd gezag van de school is verantwoordelijk voor de bescherming van persoonsgegevens van leerlingen en personeel en moet bepalen of er een melding gedaan moet worden bij de Autoriteit Persoonsgegevens. Om dit te kunnen beoordelen dient het beslismodel op de volgende pagina te worden gehanteerd.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

Document- en datamanagement

Om ervoor te zorgen dat we binnen de school onze documenten en gegevens (data) overzichtelijk en veilig opgeslagen hebben, zijn er afspraken over wat we waar bewaren. Op deze manier zijn documenten eenvoudiger terug te vinden, maar kunnen ze ook beter afgeschermd en geback-upt worden.

In het schema hieronder kun je nagaan op welke plek je gegevens en documenten op moet slaan.



Deel B
Informatie voor schoolleiders en leidinggevenden

Ouders en privacy

Privacyreglement
Ouders hebben het recht om te weten welke gegevens er van hen en van hun kinderen worden verzameld door de school en voor welke doeleinden deze gegevens verzameld worden. Met het privacyreglement voldoet het bestuur van Innoord aan zijn wettelijke informatieplicht, mits deze ook actief wordt aangeboden aan de ouders[1]. Daarom is het voor scholen belangrijk om het privacyreglement met ouders te communiceren.

In **bijlage B** en **bijlage C** is een tekst opgenomen die door alle scholen van Innoord gebruikt wordt om ouders via de website en de schoolgids te wijzen op het privacyreglement van de school. Het kan in sommige gevallen nodig zijn om deze tekst uit te breiden indien er op school aanvullende bijzondere persoonsgegevens verwerkt worden. Ouders kunnen het reglement ook opvragen bij de directie van de school.

Toestemming
Voor het gebruik van foto- en filmopnames van leerlingen en medewerkers is schriftelijke toestemming vereist. Het handigste is om de toestemming voor het gebruik van foto-en filmopnames direct bij de inschrijving van een leerling of indiensttreding van een werknemer te regelen.
Om dit voor leerlingen te regelen is binnen Innoord een toestemmingsformulier beschikbaar gesteld. De tekst is te vinden in **bijlage D**. Hierop geven ouders aan of zij toestemming geven voor het gebruik van beeldmateriaal en voor welke doeleinden.
Als schoolleider is het belangrijk om ouders jaarlijks te herinneren (bijvoorbeeld via de nieuwsbrief en in de schoolgids) dat deze toestemming herroepen of alsnog verleend kan worden. Dit betekent ook dat wanneer toestemming wordt ingetrokken, het materiaal van het betreffende medium moet worden verwijderd.

Wanneer je gegevens uit wil wisselen met externen, zoals bijvoorbeeld de logopedist, een arbo- of schoolarts, jeugdzorg of een schoolbegeleidingsdienst dan is het nodig om toestemming te vragen van ouders. Zorg dat je de toestemming registreert en hou daarbij ook rekening met de verdeling van het ouderlijk gezag.

Dit betekent ook dat wanneer toestemming wordt ingetrokken, het materiaal van het betreffende medium moet worden verwijderd.

[1] Ouders kan desgewenst ook gelezen worden als verzorgers.

Protocol melden datalekken

Inleiding
Het Protocol informatiebeveiligingsincidenten en datalekken is gebaseerd op het model van Kennisnet.

Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het tijdig melden, oplossen en het voorkomen van beveiligingsincidenten en datalekken in de toekomst.

Gebruikte termen

- Beveiligingsincident: een beveiligingsincident is een gebeurtenis die ervoor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- Datalek: Een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- Betrokkene: De persoon van wie de persoonsgegevens zijn gelekt.

Wet- en regelgeving datalekken
Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplichting melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van deze melding kan leiden tot een fikse boete.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in de leerlingadministratie of digitale leermiddelen. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan moet de school met deze bewerkers aanvullende afspraken over het melden van datalekken.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten is dat persoonsgegevens verloren zijn gegaan. Er is persoonlijke informatie ‘gelekt’. Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop de adresgegevens van klas 3b, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een bewerker voor de school. Er kan worden afgesproken dat een bewerker **namens** de verantwoordelijke de melding doet, maar dat gebeurt dan onder verantwoordelijkheid van het schoolbestuur. Dat moet wel worden afgesproken, anders zal de verantwoordelijke zelf de melding moeten doen.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens.

Rollen en verantwoordelijkheden
Er zijn tenminste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of datalek succesvol af te handelen:

1. **Ontdekker (medewerker)**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt (directeur)**; een aanspreekpunt binnen de school waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder (functionaris gegevensbescherming)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus (ict coördinator of externe ict-dienstverlener)**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

Stappenplan

1. **Ontdekken**
   De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt dit het bij het Meldpunt (de directeur).

2. **Inventariseren**
   Het Meldpunt bepaalt dan of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de Ontdekker en/of de Technicus. De volgende informatie wordt daarna vastgelegd:
   - Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
   - Datum/periode van het beveiligingsincident
   - Aard van het beveiligingsincident
   - Wanneer van toepassing (bij een datalek):
     - Omschrijving van de groep betrokkenen
     - Aantal betrokkenen
     - Type persoonsgegevens in kwestie
     - Worden de gegevens binnen een keten gedeeld

3. **Beoordelen**
   Wanneer het Meldpunt voldoende informatie heeft verzameld, en een datalek vermoed, stuurt deze de Melder een verzoek om de verzamelde informatie te bekijken. De Melder beoordeelt in overleg met de bestuurder de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkenen vereist is.

   De volgende informatie wordt vastgelegd door de Melder:
   - Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
   - Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?

- Wordt het datalek aan betrokkenen gemeld? Waarom niet?
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', hou je rekening met het type gegevens, en met de hoeveelheid gegevens. Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, moet er gemeld worden.

Van die ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen is bijvoorbeeld sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn maar ook wanneer de gelekte gegevens "gevoelig" zijn zoals bijvoorbeeld bijzondere persoonsgegevens over gezondheid, over de financiële of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene (denk aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).

4. **Repareren**
   De Technicus wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus van Innoord legt onderstaande vast:
   - Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.
   - Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?

5. **Melden**
   Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Melder dit binnen twee werkdagen doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken:
   https://datalekken.autoriteitpersoonsgegevens.nl/

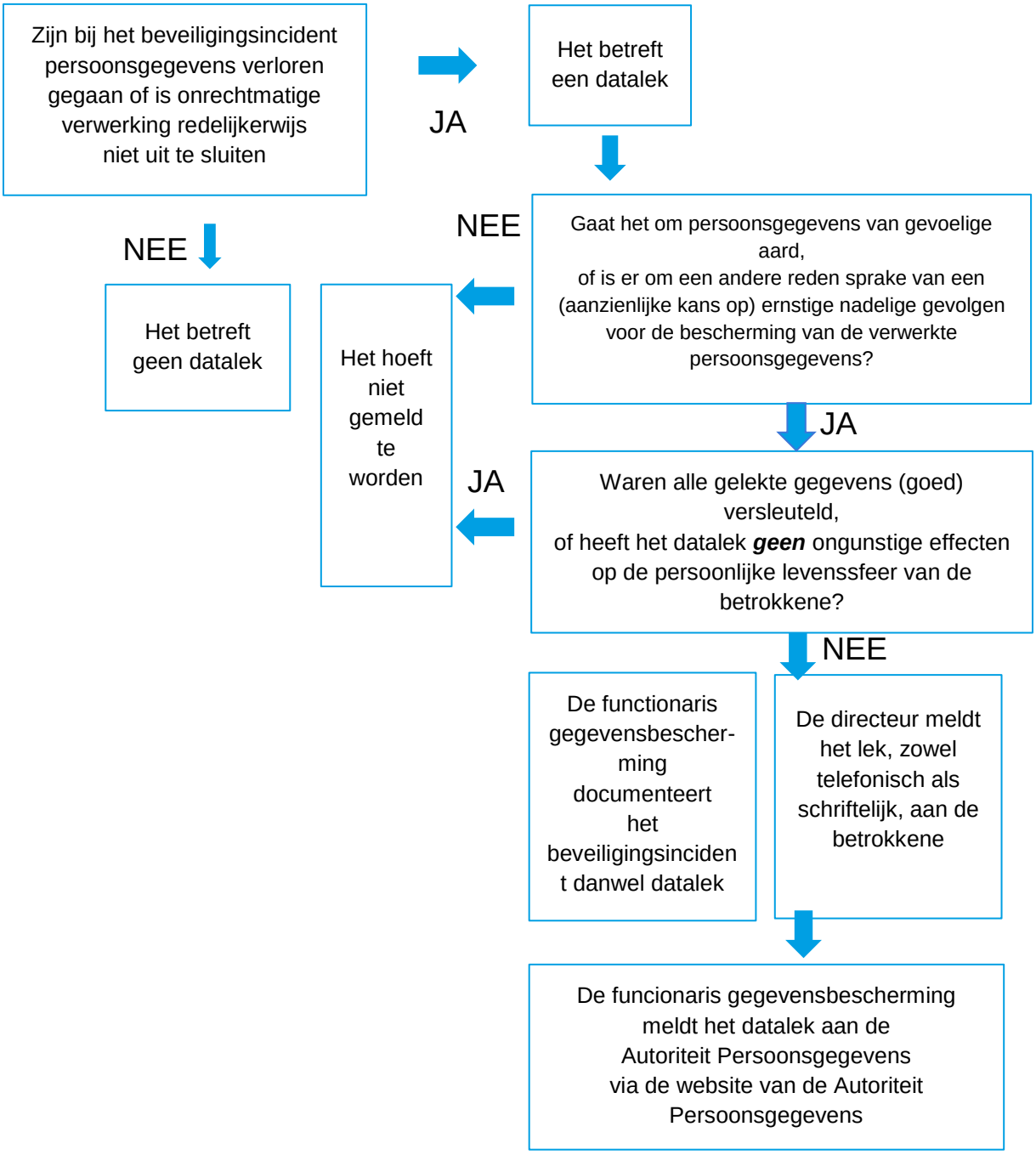
6. **Vastleggen**
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door het Meldpunt waarmee het incident is afgesloten. Het Meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.

7. **Informeren betrokkene: leerling en/of zijn ouders**
   Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan ervan worden uitgaan dat leken van gevoelige aard gemeld moeten worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of

ontoegankelijk voor anderen, dan hoeft dat toch niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.

Monitoring beveiligingsincidenten en datalekken. Alle beveiligingsincidenten en datalekken worden geregistreerd in een overzicht. Hiervoor wordt gebruik gemaakt van het formulier in **bijlage E**.

Onderstaand beslismodel kan worden gebruikt om te **achterhalen of zich een datalek heeft voorgedaan en of dit moet worden gemeld**. De functionaris gegevensbescherming overlegt met de bestuurder:


Zijn bij het beveiligingsincident persoonsgegevens verloren gegaan of is onrechtmatige verwerking redelijkerwijs niet uit te sluiten
JA
Het betreft een datalek
NEE
Gaat het om persoonsgegevens van gevoelige aard,
of is er om een andere reden sprake van een (aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens?
NEE
Het betreft geen datalek
Het hoeft niet gemeld te worden
JA
JA
Waren alle gelekte gegevens (goed) versleuteld,
of heeft het datalek ***geen*** ongunstige effecten op de persoonlijke levenssfeer van de betrokkene?
NEE
De functionaris gegevensbescher-ming documenteert het beveiligingsinciden t danwel datalek
De directeur meldt het lek, zowel telefonisch als schriftelijk, aan de betrokkene
De funcionaris gegevensbescherming meldt het datalek aan de Autoriteit Persoonsgegevens via de website van de Autoriteit Persoonsgegevens

Toegangsbeleid

Niet alle medewerkers hebben toegang nodig tot (alle) leerlinggegevens. Per rol is vastgesteld welke gegevens kunnen worden ingezien en gewijzigd, waarbij is gekeken wat die rol nodig heeft aan gegevens om zijn of haar werkzaamheden uit te kunnen voeren. Gegevens die daarbij niet noodzakelijk zijn, kan die rol ook niet inzien of wijzigen.

Uitgangspunten

- Gegevens van leerlingen en medewerkers worden opgeslagen in de daarvoor aangewezen bewaarplaatsen (zie onderdeel Document- en datamanagement).
- De afspraken met betrekking tot toegang tot en het verwerken van persoonsgegevens door de verschillende rollen binnen <naam schoolbestuur> staan hieronder beschreven in een zogenaamde autorisatiematrix.
- Alle accounts die worden verstrekt dienen te voldoen aan deze autorisatiematrix.
- De directeur van de school is verantwoordelijk voor het verstrekken van de juiste toegang (lees: accounts met de juiste rollen en rechten). De directeur ziet er ook op toe dat de accounts worden ingetrokken na het beëindigen van een arbeids- of samenwerkingscontract of het wijzigen van functies. Daarnaast worden de accounts van systemen met persoonsgegevens periodiek gecontroleerd.
- Naast het toepassen van de autorisatiematrix worden de volgende beveiligingsmaatregelen toegepast op systemen waarin persoonsgegevens worden gebruikt:
- Inloggegevens worden via het e-mailadres van <naam schoolbestuur> verstrekt aan de medewerker en nooit gedeeld met anderen.
- Inloggegevens worden periodiek (minstens 1x per jaar) vernieuwd.
- Er wordt technisch afgedwongen (waar mogelijk) om sterke wachtwoorden te gebruiken.

Autorisatiematrix

Er zijn 2 type autorisatiematrixen opgenomen in bijlage I: Een matrix gericht op de systemen waarin gegevens van leerlingen worden verwerkt en een matrix gericht op de verwerking van gegevens van medewerkers. Deze matrixen dienen vertaald te worden naar de rollen en rechtenstructuur van de diverse applicaties, zoals dat hieronder is gedaan voor ParnasSys.

Functies/rollen	Rol in ParnasSys	Werkzaamheden	Niveau van toegang[2]:
Bovenschools			
Algemene directie	Monitororganisatie beheerder	Sturing en beleid	Stichting
…			
School			
Leerkrachten	Leerkracht	Verzorgen onderwijs	Groep
Invalleerkracht	Leerkracht beperkt	Verzorgen onderwijs	Groep
Lio-stagiaire	Leerkracht beperkt	Verzorgen onderwijs	Groep
Directeur	Applicatiebeheerder	Sturing en beleid	School
Intern begeleider	Intern begeleider	Leerlingzorg	Subgroep

Administratief medewerker	Administratie / leerkracht[3]	Administratietaken	School
Extra rollen op schoolniveau			
Beheerder ParnasSys[4]	Applicatiebeheerder	Beheer	School

[1] Zie bijlage F voor toegangsrechten die standaard per rol zijn ingesteld in ParnasSys

[2] De volgende toegangsniveaus worden onderscheiden:

- Alle leerlingen in een specifieke **groep**
- Alle leerlingen per **school** of op **meerdere scholen**
- Alle leerlingen binnen de **stichting**

[3] Indien de administratief medewerker aanmeldformulieren en overdrachtsdocumenten van het kinderdagverblijf moeten invoeren, moeten zij ook de rol leerkracht hebben op groepsniveau.

[4] Deze rol kan bij Directeur of ICT-er belegd worden, afhankelijk van het taakbeleid van de school.

Bewaartermijnen

Vanuit de privacywetgeving zijn er geen concrete bewaartermijnen voor persoonsgegevens vastgesteld. Wel dient de organisatie hiervoor richtlijnen te hebben. Hierbij is het van belang om na te gaan hoe lang de gegevens nodig zijn voor het doel waarvoor deze zijn verzameld. In andere wetten zijn in sommige gevallen wel bewaartermijnen opgenomen waaraan organisaties zich moeten houden.

Innoord hanteert mede op basis hiervan de bewaartermijnen voor persoonsgegevens zoals hieronder aangegeven.

Wanneer de bewaartermijn verstreken is moeten de betreffende gegevens vernietigd worden.

Gegevens	**Verplichte bewaartermijn**	**Onderbouwing**
Gegevens over verzuim en afwezigheid	Maximaal 5 jaar nadat een leerling is uitgeschreven	Artikel 9 Bekostigingsbesluit WPO.
Gegevens in- en uitschrijving (noodzakelijk voor berekening van bekostiging)	Maximaal 5 jaar nadat een leerling is uitgeschreven	Artikel 9 Bekostigingsbesluit WPO.
Gegevens die nodig zijn om te berekenen hoeveel bekostiging de school krijgt	Minimaal 7 jaar na afloop van het schooljaar waarop de bekostiging betrekking heeft	Artikel 172 lid 3 WPO
Gegevens in het leerlingdossier	Maximaal 2 jaar nadat een leerling is uitgeschreven en 3 jaar als er sprake is van een verwijzing naar het speciaal onderwijs.	Website Autoriteit Persoonsgegevens
Medische gegevens in het leerlingdossier	n.t.b.	

Gegevens met betrekking tot bezwaar-, klachten- of gerechtelijke procedure.	Maximaal 5 jaar nadat leerling is uitgeschreven	
Camerabeelden t.b.v. toezicht	Maximaal 4 weken, tenzij er een incident is vastgelegd.	Website Autoriteit Persoonsgegevens
Gegevens in personeelsdossier met betrekking tot fiscale bewaarplicht	Maximaal 5 jaar na uitdiensttreding	Artikel 52 lid 4 Algemene wet inzake rijksbelastingen
Overige gegevens in het personeelsdossier	Maximaal 2 jaar na uitdiensttreding	
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk door personeel en leerlingen	Maximaal 6 maanden	
Sollicitatiebrief, formulier, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek	Maximaal 4 weken zonder toestemming, maximaal 1 jaar met toestemming van de sollicitant, maximaal 2 jaar na uitdiensttreding voor benoemde collega.	

Afspraken over mobiele devices in bruikleen en privé devices

De school leent afhankelijk van de functie of aard van de werkzaamheden mobiele device uit aan haar medewerkers. Dit kan gaan om een smartphone, tablet of een laptop. De devices zijn voorzien van beveiliging, zodat gegevens goed beschermd zijn. De devices zijn naast anti-virus o.a. voorzien van back-up functionaliteit, encryptie en worden na inname weer opgeschoond.

Aanvullend hierop wil de school nog een aantal afspraken schriftelijk vastleggen over het gebruik van het device wanneer deze in bruikleen wordt gegeven aan een medewerker. Deze afspraken zijn vastgelegd in **bijlage F** van dit handboek.

Verwerkersovereenkomsten

In de privacywetgeving is bepaald dat het schoolbestuur als Gegevensverantwoordelijke afspraken moet maken met alle leveranciers van de school die leerlinggegevens verwerken in zogenaamde Verwerkersovereenkomsten. Het gaat hierbij bijvoorbeeld om uitgevers van digitaal lesmateriaal, leveranciers van toetsen, onderwijsadviesdiensten, etc.

Een uitzondering hierop vormt de uitwisseling van gegevens met de overheid (DUO) in het kader van bekostiging of toezicht of het Samenwerkingsverband in het kader van passend onderwijs.

De verwerkersovereenkomsten worden waar mogelijk bovenschools afgesloten. Hiervoor is in 2017 een inventarisatie gedaan van de lopende contracten van de scholen binnen Innoord.

Wanneer een school een contract afsluit met een nieuwe leverancier zal er een nieuwe verwerkersovereenkomst gesloten moeten worden. De school is verplicht om nieuwe contracten door te geven aan het bestuur.

Wanneer het gaat om een leverancier die alleen een contract heeft met een individuele school, is de school zelf verantwoordelijk voor het afsluiten van de verwerkers-overeenkomst. Wanneer het een contract met meerdere scholen betreft, dan wordt dit bovenschools geregeld. De school dient in alle gevallen afstemming te zoeken met het bestuurssecretariaat.

Voor het afsluiten van verwerkersovereenkomsten wordt gebruik gemaakt van de meest actuele model verwerkersovereenkomst, die te vinden is via https://www.privacyconvenant.nl

Via het bestuurssecretariaat is een overzicht op te vragen van de leveranciers waar het bestuur op dit moment een verwerkersovereenkomst mee heeft. Ook voor vragen over het afsluiten van verwerkersovereenkomsten of het doorgeven hiervan, kan men terecht bij het bestuurssecretariaat.

Rollen en verantwoordelijkheden

Binnen het vaststellen en uitvoeren van het IBP-beleid zijn verschillende rollen en verantwoordelijkheden vastgesteld binnen Innoord. Deze zijn beschreven in het IBP-beleidsplan.

Dit handboek is bedoeld om praktische uitvoering te geven aan het IBP-beleid, met name ten aanzien van de organisatorische maatregelen. Voor de technische maatregelen voor informatiebeveiliging en privacy dienen afzonderlijke plannen opgesteld te worden.

In het verlengde van de rollen en verantwoordelijkheden in het IBP-beleidsplan, zijn de volgende rollen en verantwoordelijkheden bepaald ten aanzien van het vaststellen van de inhoud en (de controle op) de toepassing van dit handboek.

Onderwerp	Verantwoordelijk voor	Rol/functie
Privacyreglement	Vaststellen	Bestuurder en GMR/RvT
	Communicatie met ouders	Directeur
Gebruik beeldmateriaal en online diensten	Toestemming vragen aan ouders en registreren	Directeur
Uitwisseling persoonsgegevens	Bepalen met welke partijen persoonsgegevens uitgewisseld mogen worden en op welke wijze.	Directieoverleg
	Toestemming vragen aan ouders en registreren	Directeur
Gedragscode	Vaststellen	Bestuurder en GMR/RvT
	Bewustwording en toezien op toepassing gedragscode	Directeur
	Toepassen gedragscode	Medewerkers
	Opstellen en toepassen protocol voor leerlingen	Directeur
Document- en datamanagement	Toepassen van technische beveiligingsmaatregelen (backup, encryptie, etc.)	Bovenschoolse ICT-er
	Vaststellen bewaarplaatsen	Directie/IB
	Vaststellen bewaartermijnen	Bestuurder
	Vernietiging persoonsgegevens conform bewaartermijnen	Directeur
Toegangsbeleid	Verstrekken en intrekken accounts conform autorisatiematrixen	Directie en bestuurder (voor staf)
	Toepassen technische beveiligingsmaatregelen (o.a. automatisch vernieuwen en sterkte wachtwoord)	Bovenschoolse ICT-er
Verwerkersovereenkomsten	Doorgeven nieuwe verwerkers (leveranciers) aan	Directeur

	bestuurssecretariaat	
	Afsluiten verwerkersovereenkomsten voor meerdere scholen	Bestuurssecretariaat
	Afsluiten verwerkersovereenkomsten voor individuele scholen	Directeur
Datalekken	Protocol vaststellen	Bestuurder en GMR/RvT
	Datalekken doorgeven aan Meldpunt	Medewerkers (Ontdekkers)
	Verzamelen meldingen en benodigde informatie	Directeur (Meldpunt) i.o.m. (bovenschools) ICT-coördinator of externe ICT-dienstverlener (Technicus)
	Melden en registreren	Functionaris Gegevensbescherming (FG)
	Afweging maken tot melding Autoriteit Persoonsgegevens	FG i.o.m. Bestuurder
	Melding maken bij Autoriteit Persoonsgegevens	Functionaris Gegevensbescherming
Devices in bruikleen	Afsluiten gebruikersovereenkomst voor devices die in bruikleen worden gegeven.	Directeur
Handboek Privacy	Controle en toezicht op toepassing handboek	Bestuurder

Checklist beveiliging ICT

Fysieke beveiliging en continuïteit van ict

- ☐ Persoonsgegevens worden uitsluitend verwerkt in een gesloten, fysiek beveiligde omgeving met bescherming tegen bedreigingen van buitenaf.
- ☐ Persoonsgegevens worden uitsluitend verwerkt op apparatuur waarbij maatregelen zijn genomen om de apparatuur fysiek te beveiligen en de continuïteit van de dienstverlening te verzekeren.
- ☐ Er worden periodiek back-ups gemaakt ten behoeve van de continuïteit van de dienstverlening. Deze back-ups worden vertrouwelijk behandeld, bewaard in een gesloten omgeving en na het verstrijken van de bewaartermijn vernietigd.
- ☐ De locaties waar gegevens worden verwerkt worden periodiek getest, onderhouden en periodiek beoordeeld op veiligheidsrisico's

De netwerk-, server- en applicatiebeveiliging

- ☐ De netwerkomgeving waarbinnen gegevens worden verwerkt is strikt beveiligd. Daarbij worden verkeersstromen gescheiden en zijn maatregelen geïmplementeerd tegen misbruik en aanvallen.
- ☐ De omgeving waarbinnen persoonsgegevens worden verwerkt wordt gemonitord.
- ☐ Op systemen worden periodiek de laatste (beveiligings)patches en updates geïnstalleerd.
- ☐ Penetratietests en vulnerability assesssments worden periodiek uitgevoerd.
- ☐ Niet (meer) gebruikte informatie wordt verwijderd.
- ☐ Op wachtwoorden worden cryptografische maatregelen toegepast om deze gegevens veilig op te slaan.
- ☐ Er wordt voor inlogprocessen gebruik gemaakt van versleutelde verbindingen. De uitwisseling van persoonsgegevens aan derden in opdracht van Innoord vindt versleuteld plaats.

Netwerkcomponenten

- ☐ De netwerkcomponenten binnen de scholen van Innoord hebben enkel tot doel dat er gebruik kan worden gemaakt van de digitale omgeving via Unilogic, internet, copiers en printers en WIFI. Alle wifi-punten worden automatisch geüpdatet.
- ☐ Alle netwerkpunten (switches en routers) worden geüpdatet indien nodig. Alle netwerkcomponenten die password protected ingesteld kunnen worden zijn beveiligd.

Controle en toezicht

Jaarlijks wordt onderstaande (niet uitputtende) controlelijst ingevuld door alle scholen om na te gaan of het handboek is geïmplementeerd. De resultaten worden gerapporteerd aan de bestuurder.

#	Maatregelen met betrekking tot privacy en informatiebeveiliging	Ja*/ Nee	Waaruit blijkt dit?
1	Het privacyreglement wordt door de school jaarlijks onder de aandacht gebracht van ouders en medewerkers.		
2	Voor de publicatie van foto- en filmbeelden en online diensten is door de school vooraf toestemming vastgelegd.		
3	Met alle leveranciers die namens de school persoonsgegevens verwerken is een verwerkersovereenkomst afgesloten.		
4	Voor de uitwisseling van persoonsgegevens met derden, niet zijnde verwerkers, is toestemming vastgelegd.		
5	Het protocol datalekken is bij de medewerkers bekend. Men weet wat er van hen verwacht wordt.		
6	Toegang tot software en systemen met persoonsgegevens op school worden verleend conform de vastgestelde toegangsmatrixen.		
7	De afspraken over de bewaarplaatsen van gegevens en informatie (Document- en datamanagement) worden nageleefd.		
8	Er wordt middels een gedragscode en een protocol voor leerlingen structureel en regelmatig aandacht besteed aan de zorgvuldige verwerking van persoonsgegevens.		
9	Bij uitdiensttreding worden alle accounts ingetrokken en apparatuur ingenomen.		
10	Voor alle door de school uitgegeven apparatuur aan medewerkers zijn gebruikersovereenkomsten afgesloten.		
11	Fysieke ruimtes op school met persoonsgegevens van gevoelige aard (op papier of op server) zijn beveiligd tegen onbevoegde toegang.		
12	Er wordt voldaan aan de checklist beveiliging ICT		

Bijlagen

A. Privacyreglement Innoord

1. Aanhef	Dit reglement is voor Innoord, gevestigd aan Papaverweg 34, 1032 KJ te Amsterdam.	**Wat betekent dit in de praktijk** Dit reglement is voor Innoord.
2. Definities		
Persoonsgegevens	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;	Alle gegevens die gaan over mensen en waaraan je een mens als individu kunt herkennen.
Verwerking van persoonsgegevens	Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;	Alles wat je met persoonsgegevens doet zoals: verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorsturen, beschikbaar maken, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen.
Bijzonder persoonsgegeven	Een persoonsgegeven dat iets zegt over iemand zijn godsdienst, levensovertuiging, ras, politieke gezindheid of zijn gezondheid;	Een persoonsgegevens dat iets zegt over meer gevoelige onderwerpen zoals informatie over gezondheid, godsdienst, seksuele voorkeur of ras.
Betrokkene	Degene op wie een persoonsgegeven betrekking heeft al dan niet vertegenwoordigd door diens wettelijk vertegenwoordiger. In dit reglement gaat het om de leerlingen**;**	De betrokkene is de leerling over wie de persoonsgegevens iets zeggen heeft.
Wettelijk vertegenwoordiger	Indien de betrokkene de leeftijd van zestien jaren nog niet heeft bereikt, wordt de betrokkene vertegenwoordigd door zijn wettelijk vertegenwoordiger. Meestal zal dit een ouder zijn maar het kan hier ook gaan om een voogd;	Als de leerling nog geen 16 jaar is, dan beslissen zijn ouders over de privacy van de leerling.
Verantwoordelijke	De verantwoordelijke stelt vast welke persoonsgegevens er verwerkt worden én wat het doel is van die verwerking. Dat wil zeggen de gemeente of (openbare of privaatrechtelijke) rechtspersoon waar de school onder valt: het bevoegd gezag. Wanneer er in dit reglement gesproken wordt over de Verantwoordelijke dan wordt daarmee het bevoegd gezag van Innoord bedoeld.	Het bevoegd gezag van Innoord geeft aan waarvoor en hoe de persoonsgegevens verwerkt moeten worden. Het is mogelijk dat een schooldirecteur van een locatie de dagelijkse kwesties rondom privacy op school afhandelt, maar het bevoegd gezag blijft eindverantwoordelijk voor de verwerking van persoonsgegevens voor alle scholen die onder het

		bevoegd gezag vallen.
Bewerker	Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;	Het bedrijf, instelling of leverancier die in opdracht van de Innoord de persoonsgegevens verwerkt.
Derde	Ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken;	Iedereen die niet bij de verwerking betrokken is.
School	De verantwoordelijke onderwijsinstelling / bevoegd gezag, in dit geval Innoord.	De verantwoordelijke onderwijsinstelling / bevoegd gezag
3. Reikwijdte en doelstelling	1. Dit reglement stelt regels over de verwerking van persoonsgegevens van leerlingen van de scholen die onder Innoord vallen. 2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door Innoord worden verwerkt. Dit reglement heeft tot doel: a. de persoonlijke levenssfeer van de betrokkenen te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens; b. vast te stellen welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt; c. de zorgvuldige verwerking van persoonsgegevens te waarborgen; d. de rechten van betrokkene te waarborgen.	Dit reglement gaat over het gebruik van persoonsgegevens van leerlingen. Er kan voor gekozen worden om dit reglement uit te breiden naar medewerkers van Innoord: in dat geval wordt in de tekst overal achter ‘leerling’ de tekst ‘en medewerkers’ toegevoegd. Dit reglement geeft uitleg over het gebruik van persoonsgegevens en heeft tot doel bewustwording te creëren
4. Doelen van de verwerking van persoonsgegevens	Bij de verwerking van persoonsgegevens houdt Innoord zich aan de relevante wetgeving waaronder de Wet bescherming persoonsgegevens.	Bij de verwerking van persoonsgegevens houdt Innoord zich aan de wet
Doelen	De verwerking van persoonsgegevens vindt plaats voor: a. de organisatie of het geven van het onderwijs, de begeleiding van leerlingen, deelnemers of studenten, dan wel het geven van studieadviezen; b. het verstrekken of ter beschikking stellen van leermiddelen; c. het bekend maken van informatie over de organisatie en leermiddelen als bedoeld, onder a en b, alsmede informatie over de leerlingen, deelnemers of studenten, bedoeld in het eerste lid, op de eigen website;	Persoonsgegevens worden alleen gebruikt voor: a. de organisatie of het geven van het onderwijs, het begeleiden van leerlingen en het geven van studieadviezen; b. het aanbieden van leermiddelen; c. het bekendmaken van informatie over de school, leermiddelen of leerlingen op de eigen website zolang dit gaat over het organiseren of geven van onderwijs

	d. het bekendmaken van de activiteiten van de instelling of het instituut op de eigen website; e. het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, waaronder begrepen het in handen van derden stellen van vorderingen; f. het behandelen van geschillen en het doen uitoefenen van accountantscontrole; g. het onderhouden van contacten met de oud-leerlingen, oud-deelnemers of oud-studenten van een school die onder Innoord valt; h. de uitvoering of toepassing van een andere wet.	of het geven van studieadviezen. d. het bekendmaken van schoolactiviteiten op de eigen website; e. de administratie van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten. f. het behandelen van geschillen en het laten uitvoeren van accountantscontrole; g. het onderhouden van contacten met oud-leerlingen van een school van Innoord; h. de uitvoering of toepassing van een andere wet.
5. Vrijstelling meldingsplicht	De in artikel 4 genoemde gegevensverwerkingen vallen onder het vrijstellingsbesluit AVG en hoeven niet worden aangemeld bij de Autoriteit Persoonsgegevens.	De wet verplicht om het verwerken van persoonsgegevens aan te melden bij de toezichthouder Autoriteit Persoonsgegevens. Voor scholen is hiervoor een uitzondering gemaakt als de verwerking plaatsvindt voor de doelen zoals die zijn omschreven in artikel 4.
6. Doelbinding	Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. Een school die onder Innoord valt verwerkt niet meer gegevens dan noodzakelijk is om die vastgestelde doelen te bereiken.	Persoonsgegevens mogen alleen gebruikt worden om het gestelde doel te bereiken. Gegevens mogen dus wel worden gebruikt voor een nevendoel, maar dan moet dat wel samenhangen met de oorspronkelijke doeleinden waarvoor de gegevens verzameld zijn.
7. Soorten gegevens	De door (scholen van) Innoord gebruikte categorieën van persoonsgegevens worden in bijlage 1 opgesomd.	In bijlage 1 staan welke persoonsgegevens door (scholen van) Innoord worden verwerkt om het gestelde doel te bereiken.
8. Grondslag verwerking	Verwerking van persoonsgegevens gebeurt alleen op grond van: a. Toestemming: in het geval de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend b. Overeenkomst: in het geval de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van	Persoonsgegevens mogen alleen gebruikt worden wanneer: Er toestemming voor gegeven is door de betrokkene; Het gebruik van de gegevens nodig is om een overeenkomst uit te (gaan) voeren; De wet het gebruik van de gegevens vereist; Er sprake is van vitaal belang;

	een overeenkomst c. Wettelijke verplichting: in het geval de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan Innoord onderworpen is d. Vitaal belang: e. Publiekrechtelijke taak: in het geval de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt f. Gerechtvaardigd belang:	De gegevens gebruik worden voor het uitvoeren van onze publiekrechtelijke taak: onderwijs geven Er sprake is van gebruik met een gerechtvaardigd belang
9. Bewaartermijnen	Innoord bewaart de gegevens niet langer dan dat zij noodzakelijk zijn voor het vervullen van het doel waarvoor zij zijn verkregen, tenzij er een andere wettelijke verplichting is die het langer bewaren van de gegevens verplicht stelt. Zie bijlage 2 voor een overzicht van de bewaartermijnen.	Innoord bewaart de gegevens niet langer dan dat ze nodig zijn om het doel te bereiken tenzij er een wettelijke bewaarplicht geldt.
10. Toegang	Innoord verleent slechts toegang tot de in de administratie en systemen van de Orionschool opgenomen persoonsgegevens aan: a. de bewerker en de derde die onder rechtstreeks gezag van Innoord staat; b. de bewerker die gemachtigd is om persoonsgegevens te verwerken;' c. derden die op grond van de wet toegang moet worden verleend, waarbij alleen toegang wordt verleend aan de gegevens waartoe volgens de wet toegang toe moet worden gegeven.	Alleen personen of bedrijven die onder rechtstreeks gezag van de school staan krijgen als dat nodig is toegang tot de gegevens
11. Beveiliging en geheimhouding	a. De scholen die onder Innoord vallen nemen passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. b. De scholen die onder Innoord vallen zorgen ervoor dat medewerkers niet meer inzage of toegang hebben tot de persoonsgegevens dan zij strikt noodzakelijk nodig hebben voor de goede uitoefening van hun werk. c. Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek en de kosten van de tenuitvoerlegging. Daarbij houdt de	Innoord neemt beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens gestolen of onrechtmatig gebruikt worden. De beveiliging voorkomt ook dat de gegevens door alle medewerkers voor allerlei andere doelen gebruikt ('misbruikt') kunnen worden. De school zorgt ervoor dat de toegang tot de administratie en systemen beperkt is: niet alle medewerkers hoeven noodzakelijkerwijs inzage te hebben in de gehele administratie.

	school rekening met de concrete risico's die van toepassing kunnen zijn op de verwerkte persoonsgegevens. d. Iedereen die betrokken is bij de uitvoering van dit reglement, en daarbij de beschikking krijgt over persoonsgegevens die vertrouwelijk zijn of geheim moeten worden gehouden (zoals bijvoorbeeld zorggegevens), en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift een geheimhoudingsplicht geldt, is verplicht tot geheimhouding van die persoonsgegevens daarvan.	De school zorgt dat de gegevens voldoende beveiligd zijn, en dat de beveiliging bijgewerkt blijft. Daarbij wordt ook rekening gehouden met de speciale beveiligingsrisico's die op de school van toepassing zijn (dan kunnen bijvoorbeeld beveiligingsincidenten uit het verleden zijn). Ook moet hier gedacht worden aan het meenemen van laptops of usb-sticks naar huis: is er gedacht dat die persoonsgegevens dan ook voldoende beveiligd zijn bij verlies? Voor iedereen die binnen Innoord de beschikking krijgt over persoonsgegevens, is verplicht die vertrouwelijk te behandelen. Voor medewerkers geldt meestal (al) een geheimhoudingsclausule die in de arbeidsovereenkomst is opgenomen.
12. Verstrekken gegevens aan derden	Wanneer daartoe een wettelijke plicht bestaat kan Innoord de persoonsgegevens verstrekken aan derden. Het verstrekken van persoonsgegevens aan derden kan ook plaatsvinden na toestemming van de betrokkene. Zie bijlage 3 voor een overzicht van derden aan wie Innoord gegevens verstrekt.	Als de wet dat verplicht kan de school de persoonsgegevens aan derden geven. Dit kan ook als de betrokkene aan school toestemming geeft om zijn persoonsgegevens aan een derde te geven
13. Sociale media	Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt in het 'sociale-mediaprotocol' van Innoord.	Er kan voor gekozen worden om hier één of meerdere bepalingen op te nemen over het gebruik van internet of sociale media. Het is ook mogelijk dit op te nemen in aparte gedragsregels of een protocol.
14. Rechten betrokkenen	1. De AVG geeft de betrokkene een aantal rechten. Innoord erkent deze rechten en handelt in overeenstemming met deze rechten.	Innoord houdt zich bij het verwerken van persoonsgegevens aan alle van toepassing zijnde wet- en regelgeving, ook op het gebied van rechten van betrokkenen
Inzage en overdracht	a. Elke betrokkene heeft recht op inzage en overdracht van de door (een school van) Innoord verwerkte persoonsgegevens die op hem/haar betrekking hebben. Innoord mag voor het inwilligen van dit verzoek een kostprijs verbinden van maximaal € 5,-. Wanneer het verzoek wordt afgewezen dan worden er geen	Iedere betrokkene kan bij Innoord opvragen welke over persoonsgegevens er over hem/haar worden verwerkt. Innoord mag hier maximaal € 5,- voor vragen. Er kan voor gekozen worden om de inzage

	kosten in rekening gebracht. (De betreffende school van) Innoord kan vragen om een geldig identiteitsbewijs ter verificatie van de identiteit van de verzoeker	gratis te laten geschieden. In rekening brengen voor kosten die gemaakt worden om dit verzoek uit te voeren. Wijst de school het verzoek af dan worden er geen kosten in rekening gebracht. De school kan vragen om een geldig identiteitsbewijs om de identiteit van de verzoeker vast te stellen.
Verbetering, aanvulling, verwijdering en afscherming	b. Betrokkene kan een verzoeken doen tot verbetering, aanvulling, verwijdering of afscherming van zijn persoonsgegevens, tenzij dit onmogelijk blijkt of een onredelijke inspanning zou vergen.	Als je niet wilt dat je gegevens gebruikt worden of wanneer je wilt dat deze verbeterd, aangevuld, verwijderd of afgeschermd worden dan kun je dit aangeven. De school moet aan dit verzoek gehoord geven tenzij dat het niet mogelijk is het verzoek uit te voeren of wanneer het uitvoeren daarvan heel veel moeite zou kosten.
Verzet	c. Voor zover (een school van) Innoord persoonsgegevens gebruikt op de grond van artikel 8 onder e en f, dan kan de betrokkene zich verzetten tegen verwerking van persoonsgegevens op basis van diens persoonlijke omstandigheden.	Als de school persoonsgegevens verwerkt, en daarvoor geen grondslag heeft in de wet, of geen toestemming heeft, dan kan de betrokkene verzet instellen tegen het gebruik van die gegevens.
Termijn	2. (De school van) Innoord dient binnen een termijn van 4 weken na ontvangst van een verzoek hieraan schriftelijk gehoor te geven dan wel deze schriftelijk, gemotiveerd af te wijzen. De school kan de betrokkene laten weten dat er meer tijd nodig en deze termijn verlengen met maximaal 4 weken.	Binnen 4 weken naar het indienen van een verzoek moet Innoord het verzoek uitvoeren of uitleggen waarom ze het verzoek niet (gaan) uitvoeren.
Uitvoeren verzoek	3. Indien het verzoek van de betrokkene wordt gehonoreerd, draagt (de school van) Innoord zorg voor het zo spoedig mogelijk doorvoeren van de verzochte wijzigingen.	Wanneer de school akkoord gaat met het verzoek dan doet zij dit zo snel mogelijk
Intrekken toestemming	4. Voor zover voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming ten allen tijden door de wettelijk vertegenwoordiger worden ingetrokken.	Als u toestemming heeft gegeven voor het gebruik van persoonsgegevens, dan kunt u dit op ieder moment weer intrekken.
15. Transparantie	1. (De school van) Innoord informeert de betrokkene over de verwerking van zijn persoonsgegevens. Indien het type verwerking dat vraagt,	Wanneer de wet dat verplicht, worden betrokkene geïnformeerd over het gebruik van hun

	informeert (de school van) Innoord iedere betrokkene apart over de details van die verwerking. 2. (De school van) Innoord informeert de betrokkene – op hoofdlijnen – ook over de afspraken die gemaakt zijn met derden en bewerkers die persoonsgegevens van de betrokkene ontvangen.	persoonsgegevens. Dat kan via bijvoorbeeld de schoolgids of de website. Indien dat nodig is, dan worden de (ouders van de) leerlingen individueel geïnformeerd, bijvoorbeeld in het geval van verwerking van gezondheidsgegevens.
16. Klachten	1. Wanneer u van mening bent dat het doen of nalaten van (een school van) Innoord niet in overeenstemming is met de AVG of zoals dat is uitgewerkt in dit reglement is, dan dient u zich te wenden tot de bestuurder van Innoord. 2. Overeenkomstig de Wpb kan de betrokkene zich eveneens wenden tot de rechter of het College bescherming persoonsgegevens.	Heeft u een klacht over de omgang met persoonsgegevens of over dit reglement dan kunt u dat bij Innoord aangeven. In het veld [invullen] wordt ingevuld tot wie de betrokkene zich kan wenden voor het indien van een klacht. Er kan voor gekozen worden om de reguliere klachtenprocedure van de school te volgen. In dat geval wordt de tekst gebruikt: “Wanneer u van mening bent dat het doen of nalaten van Innoord niet in overeenstemming is met de AVG of zoals dat is uitgewerkt in dit reglement is, dan kunt u daarvoor de klachtenprocedure volgens zoals die geldt voor Innoord.”.
17. Onvoorziene situatie	Indien er zich een situatie voordoet die niet beschreven is in dit reglement dan neemt de verantwoordelijke de benodigde maatregelen.	Dit reglement voorziet niet in alle gevallen, wanneer er zoiets gebeurt dan is het aan het bevoegd gezag om daarover te beslissen.
18. Wijzigingen reglement	1. Dit reglement wordt na instemming van de GMR vastgesteld door de verantwoordelijke. De verantwoordelijke maakt dit reglement openbaar via internet. De verantwoordelijke heeft het recht dit reglement, na instemming van de GMR te wijzigingen.	Innoord kan in overleg met de GMR dit reglement wijzigen. Het reglement wordt openbaar gemaakt via bijvoorbeeld de website, schoolgids of wordt uitgereikt aan betrokkenen die nieuw worden ingeschreven.
19. Slotbepaling	Dit reglement wordt aangehaald als “het privacyreglement” van Innoord en treedt in werking op **1 oktober 2017**	Dit reglement noemen we “het privacyreglement” en geldt vanaf 1 oktober 2017.

Bijlage 1 bij privacyreglement

Categorieën persoonsgegevens die binnen Innoord verwerkt worden.

1. Leerlingen

Geen andere persoonsgegevens van een leerling worden verwerkt dan:

a. naam, voornamen, voorletters, geslacht, geboortedatum, adres, postcode, woonplaats;
b. het persoonsgebonden nummer;
c. nationaliteit en geboorteplaats;
d. gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling;
e. gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor het onderwijs;
f. gegevens betreffende de aard en het verloop van het onderwijs, alsmede de behaalde studieresultaten;
g. gegevens met het oog op de organisatie van het onderwijs en het verstrekken of ter beschikking stellen van leermiddelen;
h. gegevens met het oog op het berekenen, vastleggen en innen van de ouderbijdrage of de bijdrage voor TSO;
i. andere dan de onder a tot en met i bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een wettelijke regeling.

2. Ouders, voogden, verzorgers van leerlingen

Geen andere persoonsgegevens van ouders, voogden, verzorgers van leerlingen worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens;
b. nationaliteit en geboorteplaats;
c. hoogst genoten opleiding; behaald diploma; diplomajaar; naam en plaats van de instelling waar het diploma is behaald;
d. beroep;
e. relatie tot het kind;
f. burgerlijke staat.

3. Sollicitanten

Geen andere persoonsgegevens van sollicitanten worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer, e-mailaccount en soortgelijke voor communicatie benodigde gegevens, alsmede bank- en girorekeningnummer van de betrokkene;

b. b. een administratienummer dat geen andere informatie bevat dan bedoeld onder a;
c. nationaliteit en geboorteplaats;
d. gegevens betreffende gevolgde en te volgen opleidingen, cursussen en stages;
e. gegevens betreffende de functie waarnaar gesolliciteerd is;
f. gegevens betreffende de aard en inhoud van de huidige dienstbetrekking, alsmede betreffende de beëindiging ervan;
g. gegevens betreffende de aard en inhoud van de vorige dienstbetrekkingen, alsmede betreffende de beëindiging ervan;
h. andere gegevens met het oog op het vervullen van de functie, die door de betrokkene zijn verstrekt of die hem bekend zijn;
i. andere dan de onder a tot en met i bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet.

4. Medewerkers

Geen andere persoonsgegevens van medewerkers worden verwerkt dan:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer, e-mailaccount en soortgelijke voor communicatie benodigde gegevens, alsmede bank- en girorekeningnummer van de betrokkene;
b. een administratienummer dat geen andere informatie bevat dan bedoeld onder a;
c. nationaliteit en geboorteplaats;
d. gegevens als bedoeld onder a, van de ouders, voogden of verzorgers van minderjarige werknemers;
e. gegevens betreffende gevolgde en te volgen opleidingen, cursussen en stages;
f. gegevens betreffende de functie of de voormalige functie, alsmede betreffende de aard, de inhoud en de beëindiging van het dienstverband;
g. gegevens met het oog op de administratie van de aanwezigheid van de betrokkenen op de plaats waar de arbeid wordt verricht en hun afwezigheid in verband met verlof, arbeidsduurverkorting, bevalling of ziekte, met uitzondering van gegevens over de aard van de ziekte;
h. gegevens die in het belang van de betrokkenen worden opgenomen met het oog op hun arbeidsomstandigheden;
i. gegevens, waaronder begrepen gegevens betreffende gezinsleden en voormalige gezinsleden van de betrokkenen, die noodzakelijk zijn met het oog op een overeengekomen arbeidsvoorwaarde;
j. gegevens met oog op het organiseren van de personeelsbeoordeling en de loopbaanbegeleiding, voor zover die gegevens bij de betrokkenen bekend zijn;
k. andere dan de onder a tot en met j bedoelde gegevens waarvan de verwerking wordt vereist ingevolge of noodzakelijk is met het oog op de toepassing van een andere wet.

Bijlage 2 bij het privacyreglement

Gegevens	**Verplichte bewaartermijn**	**Onderbouwing**
Gegevens over verzuim en afwezigheid	Maximaal 5 jaar nadat een leerling is uitgeschreven	Artikel 9 Bekostigingsbesluit WPO.
Gegevens in- en uitschrijving (noodzakelijk voor berekening van bekostiging)	Maximaal 5 jaar nadat een leerling is uitgeschreven	Artikel 9 Bekostigingsbesluit WPO.
Gegevens die nodig zijn om te berekenen hoeveel bekostiging de school krijgt	Minimaal 7 jaar na afloop van het schooljaar waarop de bekostiging betrekking heeft	Artikel 172 lid 3 WPO
Gegevens in het leerlingdossier	Maximaal 2 jaar nadat een leerling is uitgeschreven en 3 jaar als er sprake is van een verwijzing naar het speciaal onderwijs.	Website Autoriteit Persoonsgegevens
Medische gegevens in het leerlingdossier	n.t.b.	
Gegevens met betrekking tot bezwaar-, klachten- of gerechtelijke procedure.	Maximaal 5 jaar nadat leerling is uitgeschreven	
Camerabeelden t.b.v. toezicht	Maximaal 4 weken, tenzij er een incident is vastgelegd.	Website Autoriteit Persoonsgegevens
Gegevens in personeelsdossier met betrekking tot fiscale bewaarplicht	Maximaal 5 jaar na uitdiensttreding	Artikel 52 lid 4 Algemene wet inzake rijksbelastingen
Overige gegevens in het personeelsdossier	Maximaal 2 jaar na	

	uitdiensttreding	
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk door personeel en leerlingen	Maximaal 6 maanden	
Sollicitatiebrief, formulier, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek	Maximaal 4 weken zonder toestemming, maximaal 1 jaar met toestemming van de sollicitant, maximaal 2 jaar na uitdiensttreding voor benoemde collega.	

Bijlage 3 bij het privacyreglement

Verstrekking aan	Doel	Grondslag
Dienst Uitvoering Onderwijs	Bekostiging*	Wettelijke plicht
Educatieve uitgeverijen en Basispoort	Gebruik digitale leermiddelen	Gerechtvaardigd belang
Basisscholen of scholen voor voortgezet onderwijs	Overdracht leerlingdossier (na aanmelding)*	Wettelijke plicht
Externe Onderwijsspecialisten	Zorgbegeleiding van een leerling	Toestemming
Stagiaires	Opleiden	Gerechtvaardigd belang
Samenwerkingsverband	Toelaatbaarheidsverklaring afgeven*	Wettelijke plicht
TSO	Tussenschoolse opvang	Toestemming
Activiteitencommissie	Innen ouderbijdrage	Toestemming
GGD/JGZ	Bezoek schoolarts	Toestemming
Inspectie van het onderwijs	Toezicht*	Wettelijke plicht
Administratiekantoor	Salarisadministratie en HR-management	Gerechtvaardigd belang
Leerplicht Gemeente	Controle verzuim	Wettelijke plicht

B. Tekst voor in de schoolgids

Privacy en leerlinggegevens

Ter bescherming van de privacy van leerlingen, hun ouders en medewerkers betracht Innoord de grootst mogelijke zorgvuldigheid. Van medewerkers, ouders en leerlingen wordt daarom verwacht dat zij zich houden aan onderstaande maatregelen.

Hoe gaan wij om met de informatie van en over leerlingen
Over de ingeschreven leerlingen verzamelt de school alle informatie die noodzakelijk is om hen zo goed mogelijk kunnen begeleiden bij het doorlopen van de school en om zo nodig extra ondersteuning te kunnen bieden. Deze informatie wordt (digitaal) opgeslagen in het leerlingdossier (alle geregistreerde informatie over een leerling).

Omdat wij deze gegevens over leerlingen verzamelen, vallen we onder de Wet Bescherming Persoonsgegevens. Deze wet is bedoeld om ervoor te zorgen dat de gegevens over personen zorgvuldig worden gebruikt (geheimhoudingsplicht) en wordt misbruik ervan tegen gegaan. Het leerlingdossier is alleen toegankelijk voor de begeleiders van een leerling ín de school.

In de school wordt regelmatig over leerlingen gesproken, bijvoorbeeld in de rapportvergadering, de leerlingbespreking en het interne zorgoverleg. Dit overleg is nodig om de vorderingen van de leerlingen te volgen, problemen te signaleren en afspraken te maken over de begeleiding. Voor leerlingen die extra begeleiding of ondersteuning nodig hebben, wordt samengewerkt met externe deskundigen. Als we een leerling willen bespreken met deze externen wordt daarvoor eerst aan ouders/verzorgers toestemming gevraagd.

Er zijn bij onze scholen een groot aantal disciplines nauw betrokken bij de ontwikkeling en ondersteuning van onze leerlingen. Dit betekent echter niet dat onze scholen alle gegevens in haar bezit hebben. Het gaat hierbij om:

- de medische dossiers vallen onder het beheer van de schoolarts
  het medisch verslag tbv. de CvB maakt onderdeel uit van ons leerlingvolgsysteem ParnasSys
- de overige gegevens, zoals verslagen van onderzoek en besprekingen, vallen onder het beheer van de directie. Alle dossiers mogen slechts onder toezicht worden ingezien. Ouders hebben uiteraard het recht deze in te zien
- de schooldossiers worden drie jaar na het schoolverlaten van de leerling vernietigd
- het beschikbaar stellen van dossiergegevens aan derden kan slechts plaatsvinden na toestemming van ouders/wettelijk vertegenwoordigers
- de school kan slechts na toestemming van ouders overgaan tot het opvragen van dossiergegevens bij derden

Zie voor verdere gegevens over de Algemene Verordening Gegevensberscherming
https://autoriteitpersoonsgegevens.nl

Hoe gaan wij om met informatie van en over ouders

Over de ouders van ingeschreven leerlingen verzamelt de school alle informatie die noodzakelijk is om hen zo goed mogelijk kunnen begeleiden bij het doorlopen van de school en om zo nodig extra zorg te kunnen bieden. Deze informatie wordt (digitaal) opgeslagen in het leerlingdossier.

Hoe gaan wij om met informatie van en over medewerkers

Over de medewerkers die bij ons werkzaam zijn en zijn geweest verzamelt het schoolbestuur alle informatie die noodzakelijk is voor hun aanstelling en bezoldiging. Deze informatie wordt (digitaal) opgeslagen in het personeelsdossier (alle geregistreerde informatie over het personeelslid).

Hoe gaan wij om met sociale media

Met een betrekking tot de omgang met sociale media is een 'gedragscode voor het gebruik van sociale media' opgesteld dat alle medewerkers hebben ontvangen. Op alle Innoord scholen worden leerlingen onderwezen in de omgang met sociale media. Zie onderstaand kader met de richtlijnen.

Hoe gaan wij om met het maken en gebruiken van foto's en video's.

Het is op de Innoord scholen gebruikelijk dat er tijdens de lessen video-opnamen worden gemaakt. Deze opnamen zijn bestemd om het lesgeven van de groepsleerkracht te verbeteren en worden niet buiten school gebruikt.

Af en toe worden er foto's video-opnamen gemaakt die gebruikt kunnen worden als voorlichtingsmateriaal. Als een kind hierop te zien is, kunnen deze opnamen alleen met toestemming van de ouder(s)/voogd(en) als zodanig worden gebruikt. Toestemming van ouders is eveneens vereist als hun kind gefilmd wordt voor privé doeleinden. Hierbij valt te denken aan ouders die willen filmen tijdens bijvoorbeeld het vieren van een verjaardag op school. Dan dient er vooraf toestemming te zijn van de directie van onze school.

Het maken van foto's of video-opnamen van een leerling door (een medewerker van) Innoord geschiedt altijd op basis van toestemming van ouders/voogden. Deze toestemming wordt in ieder geval eens per schooljaar aan ouders gevraagd. Ook bij de inschrijving van een leerling wordt hier toestemming voor gevraagd.

Wat vragen wij van ouders

Voorzieningen zoals bijvoorbeeld digitale camera's, mobiele telefoons en tablets zorgen ervoor dat ouders op schoolbijeenkomsten veel foto's en video-opnames kunnen maken. Wij kunnen dat niet verbieden. Wij vragen echter voorafgaand aan dergelijke events of ouders er aan willen denken dat lang niet alle ouders van leerlingen en medewerkers het op prijs stellen dat deze beelden op sociale media geplaatst worden. En verzoeken hen om alleen opnames waar uitsluitend hun eigen kind op staat via sociale media te verspreiden.

C. Tekst voor op de website (Responsible disclosure)

Bij <naam school> vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is.

Wij vragen je een bijdrage te leveren aan de veiligheid van ict-systemen en het beheersen van de kwetsbaarheid van ict-systemen. Dat kun je doen door de door jou ontdekte kwetsbaarheden op verantwoorde wijze bij <naam school> te melden. Als je een zwakke plek in één van onze systemen hebt gevonden horen wij dit graag zo snel mogelijk, zodat we aanvullende (beveiligings)maatregelen kunnen treffen.

Wij vragen je:

- Je bevindingen te melden via privacy@<naam school.nl>.
- De door jou ontdekte kwetsbaarheid niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of (persoons)gegevens van derden in te kijken, te verwijderen of aan te passen.
- Je bevinding/probleem niet met anderen te delen totdat de kwetsbaarheid is verholpen en alle (vertrouwelijke) gegevens die zijn verkregen door de kwetsbaarheid direct na het verhelpen daarvan te wissen.
- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden.
- Voldoende informatie te geven om de kwetsbaarheid te reproduceren zodat wij deze zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

Wij zeggen toe dat:

- We reageren zo spoedig mogelijk op jouw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing.
- Als je je aan bovenstaande voorwaarden houdt, wij geen aangifte van een strafbaar feit zullen doen of andere juridische stappen tegen je ondernemen betreffende de melding.*
- Wij jouw melding vertrouwelijk behandelen en je persoonsgegevens zonder jouw toestemming niet zullen delen met derden of verder zullen verwerken, tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Melden onder een pseudoniem is mogelijk.
- Wij je op de hoogte houden van de voortgang van het verhelpen van de kwetsbaarheid.
- In berichtgeving over de gemelde kwetsbaarheid wij je, indien je dit wenst, zullen vermelden als ontdekker van de kwetsbaarheid. Wij streven ernaar alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

* Let op: het feit dat <naam school> geen aangifte tegen jou zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar jouw handelen gehouden kan worden dan wel dat je strafrechtelijk kunt worden veroordeeld.

D. Toestemmingsformulier

Toelichting in het kader van privacywetgeving
De gegevens die u heeft ingevuld op het inschrijfformulier, worden opgeslagen in de leerlingadministratie van onze school. Uiteraard worden deze gegevens vertrouwelijk behandeld. Op onze administratie is de Wet bescherming persoonsgegevens van toepassing. Dit betekent onder andere dat de gegevens door ons worden beveiligd, en dat de toegang tot de administratie is beperkt tot alleen personeel die de gegevens strikt noodzakelijk nodig heeft. U heeft als ouder het recht om de door ons geregistreerde gegevens in te zien (voor zover die informatie betrekking heeft op uw kind). Als de gegevens niet kloppen, dan mag u van ons verwachten dat wij – op uw verzoek - de informatie verbeteren of aanvullen.
Een aantal vragen in dit inschrijfformulier zijn wij wettelijk verplicht aan u te stellen. Zo vragen wij naar uw opleidingsniveau. Dit heeft te maken met de wettelijke 'gewichtenregeling': het aantal leerkrachten aan onze school is mede afhankelijk van het totaal van het 'leerlinggewicht' van onze leerlingen.
Voor meer informatie over de omgang met de privacy van uw kind(eren), verwijzen wij u naar ons privacyreglement [link].

Toestemming
In het kader van privacywetgeving, willen wij u toestemming vragen voor het delen van de volgende persoonsgegevens. U mag natuurlijk altijd terugkomen op de door u gegeven toestemming. Ook mag u op een later moment alsnog toestemming geven.

Foto- en videomateriaal
Op onze school laten wij u met foto's en video's zien waar we mee bezig zijn. Opnames worden gemaakt tijdens verschillende gelegenheden. Ook uw zoon/dochter kan op deze foto's (en soms in video's) te zien zijn. Graag willen we daarom uw toestemming voor het gebruik van beeldmateriaal van uw zoon/dochter. Uw toestemming geldt alleen voor foto's en video's die door ons, of in onze opdracht worden gemaakt. Het maken van foto's door ouders is binnen de school niet toegestaan. Het kan voorkomen dat andere ouders foto's maken tijdens schoolactiviteiten die buiten de school plaatsvinden. De school heeft daar geen invloed op. Wij vragen daarom aan ouders om terughoudend te zijn met het maken van foto's en video's en deze niet te delen via sociale media.

Adressenlijst
Op onze school wordt er, per klas, een lijst gemaakt met de adressen van leerlingen. Deze lijst met contactgegevens is erg praktisch om te overleggen met andere ouders, als de kinderen (buiten schooltijd) willen afspreken of als er vragen zijn rondom school, overblijf, etc. Wij vragen hierbij uw toestemming om de naam van uw kind, diens adres en uw telefoonnummer te mogen delen met de andere ouders van de school. Als u er bezwaar tegen heeft, wordt de naam van uw kind niet gedeeld (en moet u daar zelf voor zorgen). Deze informatie op de klassenlijst mag uitsluitend gebruikt worden voor persoonlijk gebruik onderling, en dus niet voor bijvoorbeeld reclame.

Sociale media
Sociale media spelen een belangrijke rol in het leven van leerlingen en onderwijzend personeel. Het gebruik van sociale media is onderdeel van het gedrag van leerlingen binnen

de school. Sociale media kunnen helpen om het onderwijs te verbeteren en de lessen leuker te maken en om contact te onderhouden met vrienden of klasgenoten. Maar sociale media brengen ook risico's met zich mee, zoals pesten en het ongewild delen van foto's of andere gegevens. Op school besteden we in ons lesprogramma hier aandacht aan. Voor het gebruik van sociale media door uw kind(eren), vragen wij uw toestemming.

Hierbij verklaart ondergetekende, ouders/verzorger van ……., dat:

1 foto's en video's WEL gebruikt mogen worden:
- op het ouderportaal van de school
- in de (digitale) nieuwsbrief
- in de schoolkalender
- in de schoolgids
- op de website van de school
- in folders en flyers ter promotie van de school
- op sociale-media accounts van de school (Whatsapp, Twitter, Facebook)

(kruis aan waar u toestemming voor geeft)

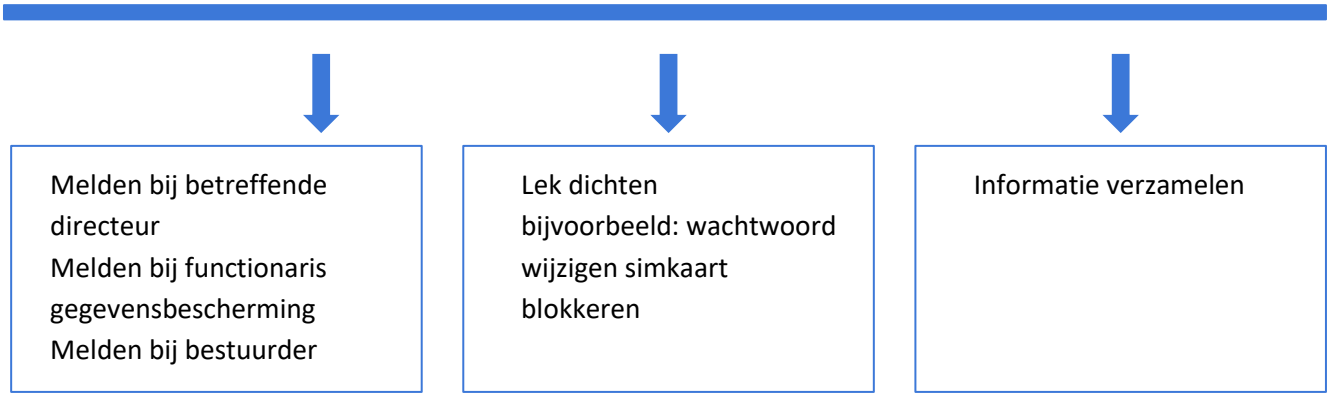
2 haar/zijn naam, adres en telefoonnummer WEL / NIET * gedeeld mag worden met andere ouders

3 hij/zij onder schooltijd WEL / NIET * gebruik mag maken van sociale media t.b.v. onderwijsdoeleinden

(* streep door wat niet van toepassing is)

	Ouder/verzorger 1	Ouder/verzorger 2
Naam:	_____	_____
Datum:	_____	_____
Plaats:	_____	_____
Handtekening:	_____	_____

E. Meldformulier datalekken



Informatie verzamelen

Geef een samenvatting van het incident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.

Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?

Minimaal:	Maximaal:

Omschrijf de groep mensen van wie persoonsgegevens zijn betrokken bij de inbreuk

Wanneer vond de inbreuk plaats?

Datum:	Of tussen (datum) en (datum)	☐ Nog niet bekend

Wat is de aard van de inbreuk? Meerdere antwoorden mogelijk.

- Lezen (vertrouwelijkheid)
- Kopiëren
- Veranderen (integriteit)
- Verwijderen of vernietigen (beschikbaarheid)
- Diefstal
- Nog niet bekend

Om welk type persoonsgegevens gaat het? Meerdere antwoorden mogelijk.

- Naam-, adres- en woonplaatsgegevens
- Telefoonnummers
- E-mailadressen of andere adressen voor elektronische communicatie
- Toegangs- of identificatiegegevens (bijvoorbeeld inlognaam/wachtwoord of klantnummer)
- Financiële gegevens (bijvoorbeeld rekeningnummer, creditcardnummer)
- Burgerservicenummer (BSN) of sofinummer
- Paspoortkopieën of kopieën van andere legitimatiebewijzen
- Geslacht, geboortedatum en/of leeftijd
- Bijzondere persoonsgegevens (bijvoorbeeld ras, etniciteit, criminele gegevens, politieke overtuiging, vakbondslidmaatschap, religie, seksuele leven, medische gegevens)
- Overige gegevens namelijk:

Welke gevolgen kan de inbreuk hebben voor de persoonlijke levenssfeer van de betrokken? Meerdere antwoorden mogelijk.

- Stigmatisering of uitsluiting
- Schade aan de gezondheid
- Blootstelling aan (identiteits)fraude
- Blootstelling aan spam of phishing
- Anders, namelijk:

F. Beleid ambulant werken & mobiele bereikbaarheid

Inleiding
De huidige technologische ontwikkelingen en vragen vanuit de organisatie maken dat een eenduidige harmonisatie van regelingen en secundaire arbeidsvoorwaarden noodzakelijk is. Onderdeel van deze (secundaire) arbeidsvoorwaarden vormt de mogelijkheid van het door Innoord ter beschikking stellen van mobiele telefoons.

Momenteel beschikken een paar medewerkers, uit verschillende functiegroepen, over een mobiele telefoon die door Innoord in bruikleen is gegeven. Een deel van de medewerkers gebruikt de eigen mobiele telefoon en ontvangt hier een vergoeding voor. Daarnaast is er een groep medewerkers, denk aan de Onderwijsconsulenten die de eigen telefoon wel gebruiken, maar er geen vergoeding voor ontvangen.

In deze notitie wordt uiteengezet welke functiegroepen in verband met het specifieke karakter van de werkzaamheden in aanmerking komen voor het in bruikleen krijgen van een mobiele telefoon of vergoeding van abonnement en gebruikskosten. Verder wordt uiteengezet welke functiegroepen in verband met het specifieke karakter van de werkzaamheden in aanmerking komen voor het in bruikleen krijgen van een laptop of tablet.

Fiscale regelgeving
De fiscale regelgeving waaraan vergoedingen en verstrekkingen voor een (mobiele) telefoon en computers onderhevig zijn, worden in deze notitie toegepast. Sinds 1 januari 2011 geldt de Werkkostenregeling (WKR), sinds 2015 is deze verplicht voor alle werkgevers.

Mobiele telefoons: vanaf 2015 kan de werkgever een telefoon, computer, tablet en gereedschap onbelast aan een werknemer verstrekken mits ze daadwerkelijk bij het werk worden gebruikt. De werkgever bepaalt aan welke eisen de voorziening moet voldoen en deze verstrekking mag niet worden uitgeruild in het cafetariamodel. Deze eisen worden het “noodzakelijkheidscriterium” genoemd. De werknemer geeft de voorziening terug of betaalt de restwaarde als hij de voorziening niet meer nodig heeft voor de dienstbetrekking.

Computers (incl. laptops en tablets), mobiele communicatiemiddelen en dergelijke apparatuur verstrekken kan, mits ze voldoen aan het noodzakelijkheidscriterium. Ook hier geldt dat werknemer de voorziening teruggeeft of de restwaarde betaalt als hij de voorziening niet meer nodig heeft voor de dienstbetrekking. Deze vergoedingen of verstrekkingen mogen niet worden gebruikt in een cafetariasysteem. Een werkgever kan wel een budget vaststellen waarmee de werknemer bijvoorbeeld een telefoon mag kopen. Als de werknemer dan een duurdere telefoon wil mag dat. In dat geval moet de werknemer een eigen bijdrage betalen uit zijn netto loon. Vergoedingen en verstrekkingen voor telefoon en vergelijkbare communicatiemiddelen vallen binnen de WKR. Het verstrekken van vergoedingen heeft wel invloed op de vrije ruimte.

Vergoedingen, verstrekkingen en terbeschikkingstellingen worden toegepast conform hetgeen hierboven is beschreven. Alles wat de werknemer vergoedt, verstrekt of ter

beschikking stelt voor zijn dienstbetrekking, is loon. Bepaalde vergoedingen, verstrekkingen en terbeschikkingstellingen zijn geen loon of geen belast loon.

Voorbeeld:
U bestelt een notebook en uw werknemer schiet de rekening voor. U stelt de notebook ter beschikking aan deze werknemer voor thuiswerk. De vergoeding van de rekening aan uw werknemer is een vergoeding voor intermediaire kosten en dus onbelast. Het noodzakelijkheidscriterium moet wel aantoonbaar zijn.

Vergoeding mobiele telefoon
Bij het vaststellen van deze functiegroepen is gekeken naar de aard van de werkzaamheden.

Functie
● Directeuren ● Medewerkers stafbureau ● Ambulante medewerkers (b.v. Onderwijsconsulenten)

De lijst geldt als richtlijn en zal eenmaal vastgesteld door de Bestuurder als leidend gelden. Innoord hanteert als uitgangspunt dat de medewerker de door de organisatie beschikbaar gestelde mobiele telefoon noodzakelijk is voor het uitoefening van de functie.
Dit alles betekent dat telefoon en abonnement in principe onbelast worden vergoed.

Een beperkt aantal medewerkers komt, met het oog op het specifieke karakter van de werkzaamheden, mogelijk in aanmerking voor het in bruikleen krijgen van een mobiele telefoon met abonnement. Dit is ter beoordeling van de Bestuurder. Voor de desbetreffende medewerkers worden de abonnementskosten vergoed en wordt er een gebruikersovereenkomst opgesteld.

Vergoeding laptop of tablet
Een aantal medewerkers komt met het oog op specifieke karakter van de werkzaamheden in aanmerking voor het in bruikleen krijgen van een laptop, dan wel tablet. Bij het vaststellen van deze functiegroepen is gekeken naar de aard van de werkzaamheden.

Functie
● Directeuren ● Medewerkers stafbureau ● Ambulante medewerkers die scholen bezoeken

De lijst geldt als richtlijn en zal eenmaal vastgesteld door de Bestuurder als leidend gelden. Innoord hanteert als uitgangspunt dat de medewerker de door de organisatie beschikbaar gestelde laptop of iPad gebruikt voor zakelijke doeleinden. En dat deze noodzakelijk is bij de functie uitoefening. Dit alles betekent dat de laptop in principe onbelast wordt vergoed.

Contract
Het is verplicht een gebruikersovereenkomst te sluiten met medewerkers die een mobiele telefoon of laptop in bruikleen krijgen. Medewerkers tekenen voor ontvangst en voor de

voorwaarden die in het contract en dit beleid zijn gesteld. In onderstaand voorbeeld (zie **bijlage G**) zijn alle bepalingen opgenomen die op het in bruikleen
geven / nemen van een mobiele telefoon, tablet of laptop van toepassing zijn.

G. Model Gebruikersovereenkomst

De werkgever : <naam>

En de werknemer:
< Naam >
< Geboortedatum >
< Adres >

Verklaren dat zij een gebruikersovereenkomst mobiele telefonie of laptop[2] voor onbepaalde duur zijn aangegaan, in aanmerking nemende dat:

- werkgever aan werknemer een mobiele telefoon of laptop (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;
- deze overeenkomst de nadere gebruiksvoorwaarden bepaalt waaronder werknemer de apparatuur kan gebruiken.

1. Aard en uitvoering
Het type apparatuur en het abonnement worden door werkgever vastgesteld en aangeschaft.

2. Rechten en plichten van werknemer
a) 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.
b) Werknemer is verantwoordelijk voor het in goede en representatieve staat houden van de apparatuur.
c) Het is werknemer verboden de apparatuur te gebruiken voor activiteiten die in strijd zijn met de bedrijfsdoelstellingen of het imago van werkgever kunnen schaden.

3. Gebruik van de apparatuur door werknemer
De werknemer wordt voor de uitoefening van de dienstbetrekking een mobiele telefoon ter beschikking gesteld met abonnement die hij hoofdzakelijk voor zakelijke doeleinden dient te gebruiken.

4. Gebruik van de apparatuur in de auto
Het is werknemer verboden te telefoneren in de auto zonder gebruikmaking van een carkit dan wel een handsfreeset. Niet handsfree bellen zal onder alle omstandigheden worden aangemerkt als bewust roekeloos handelen. Werkgever zal geen aansprakelijkheid aanvaarden voor zaak- of letselschade als gevolg hiervan, tevens zijn boeten voor rekening van werknemer.

[2] Waar laptop staat kan ook Chromebook of vergelijkbaar device gelezen worden. En in sommige gevallen iPad.

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

6. Diefstal en beschadiging
a) Werknemer dient alle zorgvuldigheid in acht te nemen ter voorkoming van beschadiging, diefstal of verlies van de apparatuur.
b) In geval van schade of diefstal van de apparatuur is werknemer verplicht dit zo spoedig mogelijk, doch uiterlijk binnen 24 uur bij werkgever te melden. Werknemer dient verder het gebruik onmiddellijk te laten blokkeren via de klantenservice van de provider of de interne contactpersoon. Als contractant draagt werkgever het risico voor misbruik na diefstal, mits aan het hiervoor gestelde is voldaan.
c) Werknemer kan aansprakelijk worden gesteld voor schade aan de apparatuur ontstaan door verwijtbare nalatigheid of onachtzaamheid.

7. Bewustzijn
a) Werknemer is op de hoogte dat werkgever informatie omtrent het gebruik van de mobiele telefoon kan aanleveren aan de werkgever.
b) Werknemer verklaart zich akkoord dat, indien gehandeld in strijd met de bepalingen van deze gebruikersovereenkomst mobiele telefonie, de naheffingsaanslagen loonheffing en een bedrag ter grootte van de correctie nota's werknemersverzekeringen inclusief eventuele boetes en rente die als gevolg van dit handelen worden opgelegd aan werkgever, zullen worden verhaald op werknemer.
c) Door ondertekening van deze overeenkomst verklaart werknemer dat hij gevolgen van deze overeenkomst en het onderliggende beleid mobiele telefonie heeft begrepen en zich daarmee akkoord verklaart.

Aldus overeengekomen en getekend te <plaats>, <datum>.

<naam werkgever>
Namens deze:

<ondertekening werknemer> <ondertekening werkgever>

H. Cameratoezicht

In het belang van de veiligheid, de gezondheid en het welzijn van leerlingen en medewerkers zijn kunnen scholen ervoor kiezen om camera's op te hangen. Met het cameratoezicht worden de volgende doelen nagestreefd:

- Bewaking in verband met toegang, schade door vandalisme en diefstal
- Herkenning of identificatie van personen die bij gebeurtenissen betrokken zijn geweest
- Bevorderen van het gevoel van veiligheid
- Preventief, ter voorkoming van onwenselijk gedrag
- Ondersteuning bij opsporing van strafbare feiten

Informatievoorziening
De camera's zijn zichtbaar opgehangen, er wordt in principe geen gebruik gemaakt van verborgen camera's. In bijzondere gevallen, bij vermoeden van onrechtmatig handelen van leerlingen of personeel, kan tijdelijk een verborgen camera worden geplaatst.

Bij het betreden van de school wordt gewaarschuwd dat er cameratoezicht wordt uitgevoerd.

Bewaartermijn beelden

- De camerabeelden worden maximaal 4 weken bewaard behoudens voor de beelden van de incidenten die in behandeling zijn. Indien er in de periode geen incidenten hebben plaatsgevonden of zijn gemeld bij de schoolleiding worden de beelden verwijderd.
- Bij geconstateerde incidenten worden de daaraan te relateren camerabeelden pas verwijderd nadat het incident is afgehandeld. Camerabeelden die gebruikt worden in het kader van onderzoek, waarvan aangifte is gedaan bij de politie, worden pas vernietigd na overleg met de politie. De termijn van vier weken is in deze gevallen niet van toepassing.
- Incidenten die het bewaren van beelden noodzakelijk maken, worden geregistreerd en gedocumenteerd in een logboek. Als beelden van een incident worden bekeken, wordt daarvan melding gemaakt in een logboek. Het logboek wordt beheerd door de systeembeheerder.

Bekijken van beelden
Toestemming voor het bekijken van opgeslagen en/of actuele camerabeelden kan alleen gegeven worden door een lid van het managementteam.

Beheer systeem
Systeembeheerders zijn alleen gerechtigd benodigde software te installeren en te controleren op het functioneren van het systeem.

Informatie aan ouders

- Ouders van een leerling die een incident meldt dat het bekijken van camerabeelden noodzakelijk maakt, worden hiervan door de schoolleiding op de hoogte gesteld.
- Indien een leerling – in het belang van het oplossen van een incident – wordt verzocht camerabeelden te bekijken, worden ouders hiervan op de hoogte gesteld. Ouders kunnen het bekijken van de beelden desgewenst bijwonen.
- Ouders van een leerling die na het bekijken van de camerabeelden als “dader” wordt geïdentificeerd, worden hiervan door de schoolleiding op de hoogte gesteld en hebben het recht de beelden binnen de bewaartermijn uit dit protocol te bekijken.
- Camerabeelden die een incident registeren, dat aangifte bij de politie noodzakelijk maakt, kunnen desgevraagd door de politie worden bekeken. Betrokken leerlingen en ouders worden hierover geïnformeerd.

I. ICT en Social media protocol leerlingen

A. Internet en e-mail
We vinden het van groot belang dat je als leerling zo veilig mogelijk online kan werken. Om hiervoor te zorgen, zijn de volgende gedragsregels van belang:

1. Ik gebruik het internet om informatie te zoeken over een onderwerp of werkstuk voor school.
2. Ik vraag toestemming van mijn meester of juf, als ik…
    a. een online game wil spelen
    b. persoonlijke gegevens (naam, adres en je telefoonnummer) moet invullen op een website
    c. bestanden wil downloaden of delen
    d. een e-mail wil versturen
3. Ik deel geen wachtwoorden met anderen.
4. Ik ga voorzichtig om met mails die ik niet vertrouw of waarvan ik de afzender niet ken. Bij twijfel klik ik geen linkjes aan.
5. Ik vertel direct aan mijn meester of juf als ik informatie tegenkom die ik niet prettig vind of waarvan ik weet dat dat niet hoort.
6. Ik weet bij welke instanties/personen ik op school en buiten school terecht kan als ik iets onprettigs heb meegemaakt op het internet waarbij ik me niet veilig voel.
7. Ik bekijk informatie op internet kritisch en kan beoordelen of het echt of nep is.
8. Ik ken de gevolgen van het delen van informatie die niet echt is.

B. Sociale media
Binnen de school gelden de volgende gedragsregels om te zorgen dat de mogelijkheden van sociale media worden gebruikt zonder andere personen of de school te schaden:

9. Ik plaats geen foto’s of verhalen over een ander (leerling, juf of meester, school, ouders of anderen van buiten de school) op sociale media als een ander dit niet goed vindt.
10. Ik plaats geen kwetsende foto’s, verhalen of opmerkingen op sociale media. Ook gebruik ik geen grove taal.
11. Ik doe niet mee aan pesten via de Whats app. Als ik nare berichten ontvang van iemand, dan vertel ik dit op school of thuis.
12. Als ik iemand niet begrijp via de Whats app of andere berichten, dan vraag ik dit rechtstreeks aan diegene.
13. Ik ga zorgvuldig om met mijn eigen identiteit. Ik besef dat ik altijd terug te vinden ben op internet.

C. ICT-apparatuur
De ICT-apparatuur op school (laptop, tablet, 3d-printer, digibord, scanner, etc.) is niet goedkoop, daarom dien je hier voorzichtig mee om te gaan. De volgende gedragsregels zijn daarom van belang:

14. Ik gebruik alleen ICT-apparatuur en software waar ik toestemming voor heb gekregen van de meester of juf. Dat geldt ook voor meegebracht smartphones, etc.

15. Ik ga voorzichtig om met de dure ICT-apparatuur van de school die ik mag gebruiken.
16. Ik gebruik geen meegebrachte USB-sticks van thuis in ICT-apparatuur van de school.

D. Schermtijd

17. Ik ben me bewust van de wereld buiten de online wereld en ik houd de tijd in de gaten als ik achter de computer/laptop of tablet zit.

J. Geheimhoudingsovereenkomst

Ondergetekende:

Naam:
Rol/ functie binnen
Innoord:
Organisatieonderdeel:

Hierna te noemen: Werknemer

Overwegende:

- dat werknemer een dienstverband in het kader van de cao vo heeft met stichting stedelijk voortgezet onderwijs zoetermeer (hierna te noemen Innoord).
- dat werknemer voor de uitvoering zijn of haar functie de beschikking moet hebben over informatie en/ of persoonsgegevens, door Innoord verzameld in haar hoedanigheid als verantwoordelijke in de zin van de algemene verordening gegevensbescherming.
- dat Innoord wil benadrukken dat zij de zorgvuldige omgang met deze gegevens van groot belang vindt en daarom voorwaarden stelt aan het ter beschikking stellen van deze gegevens aan werknemer.
- dat Innoord tevens moet voldoen aan haar wettelijke verplichting tot het treffen van technische en organisatorische beveilingsmaatregelen ten aanzien van deze informatie en/ of persoonsgegevens.
- dat deze verklaring gezien kan worden als regels ten behoeve van een goede gang van zaken, zoals bedoeld in artikel 19.2 van de cao vo. tevens is deze verklaring een nadere precisering van artikel 19.5 geheimhouding in de cao vo.
- dat werknemer door het ondertekenen van deze verklaring erkent dat Innoord deze informatie en/of persoonsgegevens als geheim en vertrouwelijk beschouwt en dat werknemer Innoord schade kan berokkenen door onzorgvuldige omgang met en/ of het onrechtmatig aan derden ter beschikking stellen van deze informatie.

verklaart dat

- de werknemer de informatie en/ of persoonsgegevens alleen zal gebruiken voor de duur van het dienstverband en uitsluitend voor de werkzaamheden binnen de functie van de werknemer.
- de werknemer de informatie en/ of persoonsgegevens niet zonder voorafgaande toestemming van Innoord verstrekt aan derden.
- de werknemer uiterste zorg besteedt aan een deugdelijke en veilige opslag van de informatie en/of persoonsgegeven, ter voorkoming van verlies en/of enige vorm van onrechtmatige verwerking, en hiertoe de richtlijnen en instructies opvolgt die Innoord verstrekt en voorschrijft.
- het voorgaande geldt ook voor door of namens Innoord verstrekte toegang aan werknemer tot ict-systemen en/of ter beschikking gestelde apparatuur.

- de werknemer zich verplicht alle door of namens Innoord verstrekte informatie en/of persoonsgegevens te retourneren aan Innoord, zodra daarom verzocht wordt. de werknemer zal geen kopieën van de informatie bewaren.
- de werknemer erkent dat Innoord te allen tijde rechthebbende en eigenaar blijft van de verstrekte informatie en/of persoonsgegevens.
- de afspraken in deze verklaring ook na beëindiging van het dienstverband geldig blijven.

ondertekening:

plaats:
datum:
naam:
handtekening:

I. Autorisatiematrix

Autorisatiematrix leerlinggegevens

Categorieën persoonsgegevens	Mag ingezien worden door de volgende functiegroepen:	Mag geregistreerd en gewijzigd worden door de volgende functiegroepen:	Mag verwijderd worden door de volgende functiegroepen:	Mag uitgewisseld worden door de volgende functiegroepen:
Contactgegevens huisarts				
Contactgegevens leerling				
Contactgegevens ouder				
Contactgegevens vorige school				
Geslacht				
Identificerende gegevens				
Inschrijfgegevens				
Kopie ID bewijs				
Nationaliteit en geboorteplaats				
NAW-gegevens huisarts				
NAW-gegevens leerling				
NAW-gegevens ouders				
Onderwijs-begeleidings-gegevens				
Overeenkomsten				
Resultaatgegevens				
Sancties				
School- en loopbaangegevens				
Zorgbegeleidingsgegevens				

Autorisatiematrix gegevens medewerkers

Categorieën persoonsgegevens	Mag ingezien worden door de volgende functies:	Mag opgevraagd, toegevoegd en gewijzigd worden door de volgende functiegroepen:	Mag verwijderd worden door de volgende functiegroepen:	Mag uitgewisseld/ gekoppeld worden door de volgende functiegroepen:

Contactgegevens medewerker				
NAW-gegevens medewerker				
Financiën – declaraties (reiskosten)				
Financiën – facturen				
Verzuimgegevens medewerkers				
Overeenkomsten				

Colofon

Auteurs: Tonny Plas en O21, Gouda 2018
tonnyplas.nl
o21.nu