

Informatiebeveiligings- en privacy beleid

Voorbeelddocument

Versie: Januari 2025



**Let op: verwijder deze pagina voor gebruik**

**Over dit voorbeelddocument**

**Dit voorbeelddocument helpt je met het maken van een eigen IBP-beleid. Elke school en elk schoolbestuur is anders. Pas het proces daarom aan aan jouw eigen situatie.**

**Aanpassen van dit voorbeelddocument**

Let bij het aanpassen van het document op het volgende:

* Bij hoofdstukken en paragrafen zijn soms toelichtingen geplaatst. Verwijder deze voordat je het beleid definitief maakt.
* Dit beleid gaat ervan uit dat taken, rollen en functies die nodig zijn om het beleid uit te voeren bij de juiste personen belegd zijn. Is dit niet zo? Ga dan eerst naar fase 1 van het Groeipad.
* Geel gearceerde teksten moet je vervangen door eigen tekst.

**Totstandkoming**

Dit voorbeelddocument is samengesteld door Kennisnet. Binnen het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken.

**Sommige rechten voorbehouden**

Hoewel aan dit document de uiterste zorg is besteed, aanvaardt Kennisnet geen aansprakelijkheid voor eventuele fouten of onvolkomenheden. Ook aanvaardt Kennisnet geen enkele aansprakelijkheid voor schade van welke aard dan ook, ontstaan uit het (onjuiste) gebruik van dit document.



Dit template is opgesteld door Kennisnet en verschijnt onder de licentie [*Creative Commons Naamsvermelding 4.0 Nederland*](https://creativecommons.org/licenses/by/4.0/legalcode.nl).

**Vragen?**

Heb je vragen over dit voorbeelddocument? Kijk voor meer informatie op [*normenkaderibp.kennisnet.nl/groeipad*](file:///Users/jhgerrits/Documents/1.%20Kennisnet%20voorbeeldocumenten/normenkaderibp.kennisnet.nl/groeipad)of stuur een mail naar *ibp@kennisnet.nl**.*

**Documentgeschiedenis**

***Toelichting***

* *Vul in wie het beleid vaststelt.*
* *Geef aan of het document openbaar, vertrouwelijk of geheim is en wie het in die gevallen mogen zien.*

**Revisies**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Review** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Functie** | **Versie** | **Datum** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Documentclassificatie**

|  |  |
| --- | --- |
| **Classificatie** | **Beschrijving** |
| Openbaar | Dit document mag zonder beperkingen worden gedeeld |
| Vertrouwelijk | Dit document mag worden gedeeld met medewerkers van <naam schoolbestuur en eventuele andere organisaties> |
| Geheim | Dit document is exclusief bestemd voor de volgende personen: <bijv. leden MT>. |

**Inhoudsopgave**

[1 Inleiding 6](#_Toc189072267)

[1.1 Onze intentie 6](#_Toc189072268)

[1.2 Doelstelling 6](#_Toc189072269)

[1.3 Reikwijdte 7](#_Toc189072270)

[2 Juridisch kader 7](#_Toc189072271)

[2.1 Wettelijke en reglementaire kaders 7](#_Toc189072272)

[2.2 Normen en standaarden 8](#_Toc189072273)

[3 Eigenaarschap en verantwoordelijkheden 8](#_Toc189072274)

[3.1 Three Lines model 9](#_Toc189072275)

[3.1.1 Eerste lijn: eindverantwoordelijkheid bij het bestuur 9](#_Toc189072276)

[3.1.2 Tweede lijn: adviseren en ondersteunen 9](#_Toc189072277)

[3.1.3 Derde lijn: onafhankelijke controle 10](#_Toc189072278)

[3.2 Medezeggenschap 10](#_Toc189072279)

[4 Beleidsthema’s informatiebeveiliging 10](#_Toc189072280)

[4.1 Risicomanagement 10](#_Toc189072281)

[4.2 Kennis en Afhankelijkheid medewerkers 11](#_Toc189072282)

[4.3 Bedrijfscontinuïteit 11](#_Toc189072283)

[4.4 Back-up en herstel 12](#_Toc189072284)

[4.5 Fysieke beveiliging 13](#_Toc189072285)

[4.6 Systeem- en data-eigenaarschap en configuratiebeheer 13](#_Toc189072286)

[4.7 Classificatie van systemen en data 13](#_Toc189072287)

[4.8 Securitybaseline 14](#_Toc189072288)

[4.9 Bewustwording 15](#_Toc189072289)

[4.10 Incident- en problemmanagement 15](#_Toc189072290)

[4.11 Risicomanagement leveranciers 16](#_Toc189072291)

[4.12 Werkplekken en mobiele apparaten 16](#_Toc189072292)

[4.13 Identiteits- en toegangsbeheer 17](#_Toc189072293)

[4.14 Vulnerabilitymanagement en pentesting 17](#_Toc189072294)

[4.15 Patchmanagement 17](#_Toc189072295)

[4.16 Logging 18](#_Toc189072296)

[4.17 Digitaal sleutelbeheer 18](#_Toc189072297)

[5 Uitgangspunten privacy 20](#_Toc189072298)

[6 Beleidsthema’s privacy 22](#_Toc189072299)

[6.1 Verwerkingsregister 22](#_Toc189072300)

[6.1.1 Legitiem doel en doelbinding 23](#_Toc189072301)

[6.1.2 Grondslag 23](#_Toc189072302)

[6.2 Informatieplicht 24](#_Toc189072303)

[6.3 Toestemming 25](#_Toc189072304)

[6.4 Privacy by design en privacy by default 25](#_Toc189072305)

[6.4.1 Dataminimalisatie 26](#_Toc189072306)

[6.5 Bewaartermijnen 26](#_Toc189072307)

[6.6 Afhandelen van datalekken 26](#_Toc189072308)

[6.7 Data Protection Impact Assessment 27](#_Toc189072309)

[6.8 Uitwisseling persoonsgegevens 27](#_Toc189072310)

[6.9 Rechten van betrokkenen 28](#_Toc189072311)

[7 Verantwoording IBP 29](#_Toc189072312)

[7.1 Naleving AVG 29](#_Toc189072313)

[7.2 Rapportage 29](#_Toc189072314)

[7.3 Beleidsherziening 29](#_Toc189072315)

# Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. Lesmateriaal wordt digitaal aangeboden, toetsingsprogramma’s worden digitaal en de resultaten en ontwikkelingen van leerlingen worden opgenomen in een digitaal leerlingvolgsysteem. Daarnaast wordt ook veel gebruikgemaakt van digitale communicatie tussen de school, leerlingen en ouders/verzorgers. Door deze ontwikkelingen neemt het risico op verstoring van het onderwijs, verlies of misbruik van gegevens en overmatige dataverzameling toe. Het is de verantwoordelijkheid van <naam schoolbestuur> om dat te voorkomen en een veilige leeromgeving te bieden.

Dit beleid voor informatiebeveiliging en privacy (IBP-beleid) beschrijft hoe <naam schoolbestuur> omgaat met de beveiliging van informatie en hoe de verwerking van (persoons)gegevens wordt gewaarborgd en gehandhaafd. In het beleid worden de verschillende rollen en verantwoordelijkheden binnen <naam schoolbestuur> op het gebied van informatiebeveiliging en privacy (IBP) beschreven.

## Onze intentie

<Naam schoolbestuur> draagt de verantwoordelijkheid voor het creëren van een veilige werk- en leeromgeving. Dit houdt in dat <naam schoolbestuur> passende technische en organisatorische maatregelen toepast om informatie te beschermen en ongeoorloofde toegang, verlies of misbruik te voorkomen.

Het recht op privacy is een grondrecht. Iedereen heeft recht op privacy en bescherming van de persoonlijke levenssfeer. Dit geldt vanzelfsprekend ook voor leerlingen, ouders/verzorgers, medewerkers en docenten. <Naam schoolbestuur> is verantwoordelijkheid voor het waarborgen van de privacy van de leerlingen en het personeel. Dit betekent ook dat deze betrokkenen zeggenschap hebben over het gebruik van hun persoonsgegevens, zoals wettelijk bepaald.

Bij <naam schoolbestuur> staat het bieden van goed onderwijs voorop. Om dit te kunnen doen verwerken wij diverse persoonsgegevens van leerlingen, ouders/verzorgers, medewerkers en docenten. <Naam schoolbestuur> vindt het belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. Het goed regelen van informatiebeveiliging en privacy in een beleid is noodzakelijk om de gevolgen van mogelijke informatiebeveiliging- en privacyrisico’s tot een aanvaardbaar niveau terug te brengen en de voortgang van het onderwijs te kunnen waarborgen.

## Doelstelling

***Toelichting***

* *Pas onderstaande generiek omschreven doelstelling aan aan jouw organisatie. Bepaal of de instelling zich conformeert aan een concreet volwassenheidsniveau en neem dit op in de doelstelling.*

Dit IBP-beleid is erop gericht de kwaliteit van de verwerking van (persoons)gegevens en de beveiliging van informatie en systemen te verhogen. Hierbij moet een juiste balans bestaan tussen veiligheid, privacy en functionaliteit. Het uitgangspunt is dat een veilige werk- en leeromgeving wordt gecreëerd, de persoonlijke levenssfeer van de betrokkenen wordt gerespecteerd en <naam schoolbestuur> voldoet aan relevante wet- en regelgeving. Dit gebeurt onder andere door bewustwording te vergroten over het belang van het zorgvuldig omgaan met informatie, systemen en persoonsgegevens.

<Naam schoolbestuur> maakt gebruik van het ‘Normenkader Informatiebeveiliging en Privacy voor het onderwijs’ - oftewel het Normenkader IBP - om inzichtelijk te maken waar de organisatie nu staat en welke maatregelen genomen moeten worden om een veilige werkomgeving te creëren en te voldoen aan de AVG.

## Reikwijdte

Dit beleid is van toepassing op alle leerlingen, docenten, medewerkers, bezoekers, ouders/verzorgers, derde partijen en andere gebruikers die toegang hebben tot of werken met de informatie van <naam schoolbestuur>. Het beleid heeft betrekking op de verwerking van alle soorten gegevens en informatie waaronder; persoonsgegevens, bedrijfsinformatie en technische gegevens. Het is van toepassing op alle gegevensverwerkingen die onder de AVG vallen.

Informatiebeveiliging en privacy maken integraal onderdeel uit van dit IBP-beleid. Informatiebeveiliging is een belangrijke voorwaarde voor privacy. Informatiebeveiliging omvat de beveiliging van *alle* informatie, terwijl privacy gaat over de verwerking van persoonsgegevens.

# Juridisch kader

## Wettelijke en reglementaire kaders

Het juridisch kader voor dit IBP-beleid wordt gevormd door de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet UAVG. Daarnaast kunnen uit andere wet- en regelgeving verplichtingen of instructies voortvloeien voor de verwerking van persoonsgegevens. Voor <naam schoolbestuur> is op dit gebied onder andere de volgende wetgeving van belang:

* Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
* Wet onderwijstoezicht
* Archiefwet en Archiefbesluit
* Leerplichtwet
* Wet medezeggenschap op scholen
* Arbeidsregelgeving en CAO
* Belastingwetgeving
* Telecommunicatiewet en e-privacy wetgeving
* *< Vul aan als meerdere wettelijke of reglementaire kaders van toepassing zijn. >*

Indien een (mogelijke) strijdigheid tussen dit beleid en de AVG en/of gerelateerde wet- en regelgeving bestaat, dan moet voorafgaand aan een verwerking overlegd worden met de afdeling Juridische zaken en de privacy officer.

## Normen en standaarden

***Toelichting***

* *Vul onderstaande alinea aan als er ook andere normenkaders of standaarden van toepassing zijn.*

Als onderwijssector hebben we afgesproken om toe te werken naar één normenkader om aan de minimale vereisten te voldoen voor digitaal veilig onderwijs. Dit is het ‘Normenkader Informatiebeveiliging en Privacy voor het onderwijs’. Dit normenkader beschrijft de regels, principes en standaarden op het gebied van informatiebeveiliging en privacy waaraan <naam schoolbestuur> moet voldoen voor een digitale veilige schoolomgeving.

# Eigenaarschap en verantwoordelijkheden

***Toelichting***

* *In dit hoofdstuk geef je aan hoe de governance van informatiebeveiliging en privacy binnen de school georganiseerd is. Wie zorgt ervoor dat het beleid op de juiste manier wordt uitgevoerd?*
* *In dit voorbeelddocument maken we gebruik van het Three Lines model. Dat is een organisatiemodel dat helpt om de governance van je organisatie op een gestructureerde manier te organiseren. Je kunt dit uiteraard ook anders inrichten.*
* *Let op dat de verschillende functies en rollen die beschreven zijn per organisatie kunnen verschillen. Pas deze functietitels en rollen aan indien jouw organisatie andere termen hanteert.*

Dit hoofdstuk beschrijft hoe de verschillende rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy samenhangen.

## Three Lines model



Informatiebeveiliging en privacy bij <naam schoolbestuur> is ingericht volgens het Three Lines model (3L-model). Het 3L-model is een leidraad bij het inrichten van de governance van een organisatie.

### Eerste lijn: eindverantwoordelijkheid bij het bestuur

***Toelichting***

* *Beschrijf hier uit welke rollen de eerste lijn bestaat. Op een school kunnen dat teamleiders, coördinatoren, schoolleiders, conrectors of het hoofd bedrijfsvoering zijn.*

Het 3L-model heeft als uitgangspunt dat de eerste lijn verantwoordelijk is voor processen, informatie en systemen van de organisatie, de risico's die hieruit voortvloeien en het treffen van de juiste maatregelen om de risico’s te verkleinen. De eerste lijn bestaat uit het bestuur, schoolleiders, en het verdere lijnmanagement van <naam schoolbestuur>

Het bestuur is binnen de eerste lijn eindverantwoordelijk voor informatiebeveiliging en privacy, maar kan bepaalde verantwoordelijkheden beleggen bij andere functies binnen de organisatie. Bij de beschrijving van de beleidsthema’s in hoofdstuk 4 en 6 wordt per thema beschreven wie er verantwoordelijk is.

### Tweede lijn: adviseren en ondersteunen

Naast de eerste lijn moet er een rol zijn die de eerste lijn ondersteunt, adviseert, coördineert en die bewaakt of het management de verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. De tweede lijn bestaat uit security officers, privacy officers, IBP-adviseurs en juridische adviseurs.

### Derde lijn: onafhankelijke controle

***Toelichting***

* *Hier geef je aan wie verantwoordelijk is voor het onafhankelijk toetsen van de samenwerking tussen en het functioneren van de eerste en tweede lijn. Denk aan een interne auditor of de functionaris gegevensbescherming.*

De derde lijn controleert of de eerste en tweede lijn soepel samenwerken en goed functioneren. De derde lijn is onafhankelijk, opereert los van de andere organisatieonderdelen en suggereert waar nodig verbeteringen. De functionaris gegevensbescherming (FG) en de interne auditor vallen binnen de derde lijn. De FG wordt aangesteld door het bestuur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een reglement dat door het bestuur wordt vastgesteld.

## Medezeggenschap

***Toelichting***

* *Hier beschrijf je hoe je als organisatie in een procesbeschrijving hebt vastgelegd hoe en wanneer de medezeggenschapsraad geïnformeerd en betrokken wordt bij wettelijke taken op het gebied van privacy.*
* *Je moet als schoolbestuur de medezeggenschapsraad om instemming vragen voor het vaststellen van dit IBP-beleid.*

<Naam schoolbestuur> betrekt de medezeggenschapsraad (MR) bij besluiten over regelingen en procedures ten aanzien van de bescherming van persoonsgegevens. Het schoolbestuur is eindverantwoordelijk voor het informeren van de medezeggenschapsraad en voor het opstellen van instemmingsprocedures.

# Beleidsthema’s informatiebeveiliging

***Toelichting***

* *De beleidsthema’s zoals beschreven in dit hoofdstuk zijn zo opgesteld dat ze corresponderen met de deelprojecten die binnen het Groeipad opgenomen zijn. Bepaal of dit voor jouw organisatie een goede opzet van de thema’s is.*
* *Let op: indien de organisatie het beheer van IT (deels) heeft uitbesteed dient de beleidstekst bij de technische beleidsthema’s beoordeeld en aangepast te worden naar je eigen situatie. Bepaal of een verwijzingen naar het beleidsthema risicomanagement leveranciers voldoende is.*

In hoofdstuk 4 zijn de beleidsthema’s op het gebied van informatiebeveiliging opgenomen.

## Risicomanagement

***Toelichting***

* *Het Risicomanagementbeleid is in een apart voorbeelddocument beschreven. Zorg dat je hier een verwijzing maakt naar het Risicomanagementbeleid of werk dit beleidsthema hieronder verder uit.*

<Naam schoolbestuur> hanteert een losstaand Risicomanagementbeleid. Zie <naam beleid>.

## Kennis en Afhankelijkheid medewerkers

***Toelichting***

* *Bepaal waar in de organisatie en binnen welke documentatie het waarborgen van kennis en de beschikbaarheid van medewerkers het beste kan worden vastgelegd. Heb je HR-processen al vastgelegd? Dan is het aan te raden om onderstaande eisen zoveel mogelijk binnen deze documentatie op te nemen.*

<Naam schoolbestuur> is voor de beveiliging van informatie en de continuïteit van het onderwijs afhankelijk van de kennis en beschikbaarheid van medewerkers. <Naam schoolbestuur>wil voorkomen dat er onvoldoende kennis aanwezig is bij medewerkers of dat kritieke kennis en vaardigheden onvoldoende aanwezig zijn binnen de organisatie. Taken van sleutelfiguren moeten daarom altijd overgenomen kunnen worden door andere medewerkers. Hiervoor hanteert<naam schoolbestuur> de volgende maatregelen:

* Een back-upplan voor kritieke medewerkers.
* Voldoende training en certificering.
* Een indienst-/uitdiensttredingproces waarin rekening gehouden wordt met aansluiting op het proces voor het beheren van rechten en rollen, de overdracht van kennis en documentatie en screening van medewerkers.

Verantwoordelijkheden:

* <Functietitel> is verantwoordelijk voor het formeel goedkeuren van het back-upplan voor kritieke medewerkers.
* <Functietitel> is verantwoordelijk voor het opstellen en het beheren van het back-upplan voor kritieke medewerkers.
* <Functietitel> is verantwoordelijk voor het opstellen en het beheren van het indienst/ uitdiensttreding proces.

## Bedrijfscontinuïteit

<Naam schoolbestuur> zorgt ervoor dat mogelijke verstoringen van het onderwijs zo snel mogelijk verholpen worden en dat de impact van verstoringen beperkt blijft. Door processen te analyseren worden de meest kritieke applicaties en medewerkers geïdentificeerd, en wordt bepaald welke terugvalopties nu aanwezig zijn. Hierna kunnen maatregelen geïmplementeerd worden om verstoringen zo veel mogelijk te voorkomen of de impact te beperken. Er is een crisismanagementteam aanwezig om snel en adequaat op incidenten te reageren.

<Naam schoolbestuur> hanteert de volgende maatregelen voor bedrijfscontinuïteit:

* **Business impact analyses (BIA) op basis van de processen van de organisatie**. De processen worden op basis van een risicogestuurde aanpak geanalyseerd, waarbij eerst de meest kritieke processen behandeld worden. Nieuwe risico’s die tijdens deze BIA’s geïdentificeerd zijn, worden opgenomen in het risicoregister. Zie hiervoor het risicomanagementbeleid.
* **Een bedrijfscontinuïteitsplan (BCP)**. Een crisismanagementaanpak waaronder periodieke crisisoefeningen maken onderdeel uit van het BCP. Taken en verantwoordelijkheden zijn duidelijk toegewezen in het BCP. Het BCP wordt na een jaarlijkse oefening steeds geactualiseerd.

Verantwoordelijkheden:

* Het bestuur is verantwoordelijk voor het formeel goedkeuren van het bedrijfscontinuïteitsplan.
* <Functietitel> is verantwoordelijk voor het opstellen en het beheren van het bedrijfscontinuïteitsplan.

## Back-up en herstel

***Toelichting***

* *Bepaal of de back-up vereisten vastgesteld worden op basis van de BIV-classificatie.*
* *Heb je het maken van back-ups uitbesteed of is het niet van toepassing? Licht dan toe waarom dit niet van toepassing is en maak een verwijzing naar het beleidsthema Risicomanagement levanciers.*

Om de impact van verstoringen of dataverlies te beperken zorgt <naam schoolbestuur> voor back-ups van systemen en data. Op basis van de BIV-classificatie van systemen worden de back-upvereisten voor de systemen en de data binnen deze systemen vastgesteld. Back-ups worden regelmatig getest om te verifiëren of gegevens kunnen worden hersteld binnen de vastgestelde periode. De volgende uitgangspunten worden hierbij gehanteerd:

* De proceseigenaar is degene die beslist over de continuïteitsvereisten van een dataverwerking of een systeem. Het initiatief voor deze afweging komt van de systeemeigenaar.
* We stellen dezelfde back-upeisen aan diensten van externe leveranciers als aan systemen die we zelf beheren.
* Bij voorkeur maken we bij externe leveranciers gebruik van de back-upfaciliteit die ze zelf bij hun dienst aanbieden. Ontbreekt die of voldoet die niet, dan maken we zelf back-ups van de informatie die we verwerken in de dienst van deze leverancier.
* We evalueren jaarlijks de manier waarop we zelf back-ups maken.

Verantwoordelijkheden:

* <Naam schoolbestuur> stelt een procesbeschrijving op voor back-up en herstel.
* <Functietitel> is verantwoordelijk voor het formeel goedkeuren van de back-up en herstel procesbeschrijving.
* <Functietitel> is verantwoordelijk voor het opstellen en het beheren van de back-up en herstel procesbeschrijving.
* De systeemeigenaar is verantwoordelijk voor het toepassen van het back-up en herstel proces.

## Fysieke beveiliging

***Toelichting***

* *Het fysieke beveiligingsbeleid is in een apart voorbeelddocument beschreven. Zorg dat je hier een verwijzing maakt naar het fysieke beveiligingsbeleid of werk dit beleidsthema hieronder verder uit.*

<Naam schoolbestuur> hanteert een losstaand Fysiek beveiligingsbeleid. Zie <naam beleid>.

## Systeem- en data-eigenaarschap en configuratiebeheer

***Toelichting***

* *Bepaal of jouw organisatie in staat is om data-eigenaarschap te implementeren en dit te beschrijven binnen dit beleidsthema.*
* *Bepaal waar de processen en het eigenaarschap van de processen worden vastgelegd en leg dit vast.*

Om IT-processen te beheren is inzicht nodig in welke systemen worden gebruikt binnen de organisatie. Veel van de IBP-thema’s in dit beleid zijn afhankelijk van dit inzicht. De rol van systeemeigenaar wordt gebruikt om bepaalde verantwoordelijkheden toe te kunnen wijzen die specifiek voor een systeem gelden. De rol van proceseigenaar wordt gebruikt om bepaalde verantwoordelijkheden toe te kunnen wijzen die te maken hebben met een specifiek proces. <Naam schoolbestuur> maakt de keuze om eigenaarschap van data niet vast te leggen, maar zich te beperken tot het beleggen van eigenaarschap van systemen waar deze data in is vastgelegd. Voor het vastleggen van processen en het eigenaarschap van systemen en processen treft <naam schoolbestuur>de volgende maatregelen:

* <Naam schoolbestuur> heeft een configuratiemanagementdatabase (CMDB) waarin alle systemen, het eigenaarschap en andere benodigde eigenschappen bijgehouden worden.
* Systeemeigenaarschap wordt bepaald vóór implementatie van nieuwe systemen. De eigenaren van systemen worden vastgelegd in het CMDB.
* Proceseigenaarschap wordt bepaald en vastgelegd binnen het verwerkingsregister.

Verantwoordelijkheden:

* <Functietitel> is verantwoordelijk voor het opstellen en het beheren van de CMDB.
* De systeemeigenaar van elk systeem is verantwoordelijk voor het vastleggen van de juiste eigenschappen in de CMDB.

## Classificatie van systemen en data

***Toelichting***

* *Beschrijf binnen dit beleidsthema welke BIV-classificatiemethode er gebruikt wordt binnen de organisatie of verwijs naar een document waarin de methode is beschreven.*
* *Is het systeemeigenaarschap nog niet belegd? Beschrijf dan bij de verantwoordelijkheden wie in dat geval de BIV-classificatie uitvoert.*

Om risicogestuurd beslissingen te kunnen nemen is belangrijk om per systeem het benodigde niveau van beschikbaarheid, integriteit en vertrouwelijkheid (BIV) te bepalen. De classificatie is beperkt tot systeemniveau. <Naam schoolbestuur> kiest ervoor om de classificatie niet per individueel dataobject toe te passen. <Naam schoolbestuur> heeft voor elk systeem dat opgenomen is in de CMDB een BIV-classificatie uitgevoerd. Deze BIV-classificatie wordt gebruikt om te bepalen welke maatregelen er voor het betreffende systeem geïmplementeerd moeten worden. Voor het goed toepassen van de BIV-classificatie treft <naam schoolbestuur> de volgende maatregelen:

* De BIV-classificatie wordt uitgevoerd vóór de aanschaf van een nieuw systeem. Zie beleidsthema 4.11.
* De BIV-classificatie wordt vastgelegd in de CMDB.

Verantwoordelijkheden:

* De systeemeigenaar van elk systeem is verantwoordelijk voor het uitvoeren van de BIV-classificatie en het vastleggen hiervan in de CMDB.

## Securitybaseline

***Toelichting***

* *Beschrijf binnen dit beleidsthema welke securitybaseline er gehanteerd wordt binnen de organisatie en leg dit vast.*

Een securitybaseline voor IT-systemen is vastgesteld om het risico van ongeoorloofde toegang tot IT-middelen te beperken. <Naam schoolbestuur> maakt gebruik van het certificeringsschema ROSA als securitybaseline voor IT-systemen in eigen beheer. De securitybaseline is formeel vastgelegd, wordt periodiek geactualiseerd en wordt goedgekeurd door het schoolbestuur. De toepassing van de securitybaseline voor IT-middelen wordt periodiek beoordeeld op naleving. Afwijkingen van de baselines zijn gedocumenteerd en goedgekeurd.

Verantwoordelijkheden:

* <Functietitel> is verantwoordelijk voor het formeel goedkeuren van de securitybaseline.
* De systeemeigenaar van elk systeem is verantwoordelijk voor het voldoen aan de securitybaseline en het vastleggen van afwijkingen op de baseline.

## Bewustwording

Beleid en technische maatregelen zijn niet voldoende om risico’s op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hierin ook een belangrijke factor. Daarom wordt het bewustzijn van medewerkers over de verantwoordelijkheden die ze hebben voortdurend aangescherpt, zodat de kennis van bestaande risico’s wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Hiervoor neemt <Naam schoolbestuur> de volgende maatregelen:

* Er is een bewustwordingsprogramma dat <invullen herzieningstermijn> herzien wordt waarin de bewustwordingsactiviteiten en de verantwoordelijkheden voor deze activiteiten beschreven worden.

Verantwoordelijkheden:

* <Naam schoolbestuur> is verantwoordelijk voor het formeel goedkeuren van het bewustwordingsprogramma.
* <Functietitel> is verantwoordelijk voor het opstellen en het beheren van het bewustwordingsprogramma

## Incident- en problemmanagement

***Toelichting***

* *Het afhandelen van kan ook als los proces opgesteld zijn. Pas onderstaand beleidsthema en beleidsthema 6.6 Afhandelen van datalekken aan, als het afhandelen van datalekken in een aparte procesbeschrijving opgenomen is.*

Incidentmanagement is het proces voor het melden van incidenten binnen de organisatie. Sommige incidenten kunnen een datalek tot gevolg hebben. Incidenten binnen de organisatie zijn nooit helemaal uit te sluiten. Een helder beschreven incidentmanagementproces is aanwezig om incidenten op tijd te herkennen en ze adequaat af te handelen. De manier waarop dat gebeurt is vastgelegd in een procesbeschrijving waarbij de volgende onderwerpen minimaal terugkomen:

* **Een centraal punt** voor het melden van incidenten**.**
* **Incidentenregister:** Binnen dit incidentenregister wordt er duidelijk onderscheid gemaakt tussen datalekken en andere type incidenten.
* **De classificatie van incidenten:** Bij elk incident moet worden vastgesteld om wat voor type incident het gaat (beveiliging, privacy, etc.)
* **De afhandeling van het incident**: Het is duidelijk wie bij welk type incident betrokken moeten worden en wie verantwoordelijk is voor het afhandelen van de incidenten.
* **Problemmanagement:** Indien incidenten regelmatig terugkomen worden deze aangemerkt als een *known error*. De procesbeschrijving beschrijft de vervolgstappen voor een terugkerend incident.
* **Monitoren en rapporteren:** Afhandeling van incidenten en problemen worden gemonitord. Hierover wordt periodiek gerapporteerd.

Verantwoordelijkheden:

* <Functietitel> is verantwoordelijk voor het formeel goedkeuren van de incidentmanagemenprocesbeschrijving.
* <Functietitel> is verantwoordelijk voor het opstellen en het beheren van de incidentmanagementprocesbeschrijving.
* <Functietitel> is verantwoordelijk voor het inrichten en beheren van het incidentenregister.

## Risicomanagement leveranciers

***Toelichting***

* *Heb je nog geen leveranciersmanagementproces uitgewerkt? Dan kun je ervoor kiezen de extra risicomanagementstappen in een apart proces uit te werken. Heb je al wel een leveranciersmanagementproces uitgewerkt? Verwerk dan de extra risicomanagementstappen in deze procesbeschrijving*.
* *Bepaal of er gebruik wordt gemaakt van de securitybaseline voor het bepalen aan welke eisen de leveranciers moeten voldoen.*

<Naam schoolbestuur>besteedt een deel van de IT uit aan leveranciers, maar blijft eindverantwoordelijk voor beveiliging van informatie en persoonsgegevens. Om ervoor te zorgen dat ook leveranciers zich houden aan de technische maatregelen die volgen uit de securitybaseline zijn bepaalde stappen toegevoegd aan het leveranciersmanagementproces.

* Er is een lijst met maatregelen opgesteld op basis van de securitybaseline van <naam schoolbestuur>
* Er is een leveranciersmanagementproces waar de volgende stappen onderdeel van zijn:
	+ Voor de aanschaf van een nieuw systeem wordt een BIV-classificatie uitgevoerd.
	+ Op basis van deze BIV-classificatie en de lijst met maatregelen worden aanbestedingseisen opgesteld.
	+ Er wordt een periodieke controle gedaan op het voldoen aan de aanbestedingseisen.

Verantwoordelijkheden:

* <Functietitel> is verantwoordelijk voor het formeel goedkeuren van de leveranciersmanagementprocesbeschrijving.
* <Functietitel> is verantwoordelijk voor het opstellen en het beheren van de leveranciersmanagementprocesbeschrijving.
* De systeemeigenaar is verantwoordelijk voor de periodieke controle op het voldoen aan de aanbestedingseisen.

## Werkplekken en mobiele apparaten

Persoonsgegevens en andere informatie uit systemen die binnen onze organisatie worden gebruikt, worden ontsloten via verschillende apparaten zoals laptops, tablets, smartphones en desktop-pc's. Deze apparaten brengen risico’s met zich mee op het gebied van beveiliging, dataverlies en compliance. Daarom treft <naam schoolbestuur> de volgende maatregelen:

* <Naam schoolbestuur> hanteert een richtlijn voor het gebruik van werkplekken en mobiele apparaten.

**Verantwoordelijkheden:**

* <Functietitel> is verantwoordelijk voor het formeel goedkeuren van de richtlijn voor het gebruik van werkplekken en mobiele apparaten.
* <Functietitel> is verantwoordelijk voor het opstellen en het beheren van de richtlijn voor het gebruik van werkplekken en mobiele apparaten.

## Identiteits- en toegangsbeheer

***Toelichting***

* *Het Identiteits- en toegangsbeheer (IAM) beleid is in een apart voorbeelddocument beschreven. Zorg dat je hier een verwijzing maakt naar het IAM-beleid of werk dit beleidsthema hieronder verder uit.*
* *Mocht dit deel uitbesteed zijn of niet van toepassing zijn, geef dan een toelichting waarom dit niet van toepassing is en maak een verwijzing naar het beleidsthema 4.11 Risicomanagement levanciers.*

<Naam schoolbestuur>heeft een apart IAM-beleid. Zie hiervoor <naam beleid>.

## Vulnerabilitymanagement en pentesting

***Toelichting***

* *Beschrijf binnen dit beleidsthema hoe kwetsbaarheden binnen systemen en het IT-landschap beperkt worden.*
* *Zorg dat een aanpak voor pentesting op hoofdlijnen opgenomen is in dit beleidsthema of dat hiervoor een richtlijn/procesbeschrijving opgesteld wordt.*
* *Beschrijf de verantwoordelijkheden.*
* *Mocht dit deel uitbesteed zijn of niet van toepassing zijn, geef dan een toelichting waarom dit niet van toepassing is en maak een verwijzing naar het beleidsthema 4.11 Risicomanagement levanciers.*

Vulnerabilitymanagement en pentesting vormen een essentieel onderdeel voor het verminderen van risico’s, het voorkomen van ongeautoriseerde toegang tot IT-systemen en het beschermen van gegevens tegen mogelijke dreigingen.

## Patchmanagement

***Toelichting***

* *Bepaal of de vereisten voor het patchen van systemen vastgesteld worden op basis van de BIV-classificatie.*
* *Mocht dit deel uitbesteed zijn of niet van toepassing zijn, geef dan een toelichting waarom dit niet van toepassing is en maak een verwijzing naar het beleidsthema 4.11 Risicomanagement levanciers.*

Met patchmanagement verhelp je kwetsbaarheden in systemen, applicaties en hardware. Het doel is om de beveiliging, stabiliteit en prestaties van IT-omgevingen te waarborgen door het tijdig testen en implementeren van patches. Hiervoor neemt <naam schoolbestuur> de volgende maatregel:

* <Naam schoolbestuur> **>** heeft een proces voor het inrichten van patchmanagement.

Verantwoordelijkheden:

* <Functietitel> is verantwoordelijk voor het formeel goedkeuren van de procesbeschrijving patchmanagement.
* <Functietitel> is verantwoordelijk voor het opstellen en het beheren van de procesbeschrijving patchmanagement.
* De systeemeigenaar is verantwoordelijk voor tijdig testen en implementeren van patches.

## Logging

***Toelichting***

* *Bepaal of de vereisten voor logging binnen systemen vastgesteld worden op basis van de BIV-classificatie.*
* *Mocht dit deel uitbesteed zijn of niet van toepassing zijn, geef dan een toelichting waarom dit niet van toepassing is en maak een verwijzing naar het beleidsthema 4.11 Risicomanagement levanciers.*

Loggegevens bieden inzicht in de activiteiten van systemen en spelen een sleutelrol bij het detecteren, onderzoeken en voorkomen van beveiligingsincidenten. Om loggegevens vast te leggen neemt <naam schoolbestuur> de volgende maatregel:

* <Naam schoolbestuur> heeft een procesbeschrijving voor het vastleggen van loggegevens binnen systemen.

Verantwoordelijkheden:

* <Functietitel> is verantwoordelijk voor het formeel goedkeuren van de procesbeschrijving voor logging.
* <Functietitel> is verantwoordelijk voor het opstellen en het beheren van de procesbeschrijving voor logging.

## Digitaal sleutelbeheer

***Toelichting***

* *Beschrijf binnen dit beleidsthema of je organisatie zelf cryptografische sleutels beheert en hoe er omgegaan wordt met encryptie van data.*
* *Mocht dit deel uitbesteed zijn of niet van toepassing zijn, geef dan een toelichting waarom dit niet van toepassing is en maak een verwijzing naar het beleidsthema 4.11 Risicomanagement levanciers.*

<Naam organisatie> gebruikt encryptie voor de volgende doeleinden:

* **Bescherming van vertrouwelijke gegevens:** Door het toepassen van sterke versleutelingstechnieken bij opslag, verzending en verwerking van gegevens.
* **Verificatie van identiteit:** Gebruik van cryptografische methoden zoals digitale handtekeningen en certificaten om betrouwbare communicatie te waarborgen.
* **Waarborgen van gegevensintegriteit:** Detecteren van wijzigingen in gegevens.

Om encryptie toe te passen treft <naam schoolbestuur> de volgende maatregel:

* <Naam organisatie> hanteert een procesbeschrijving voor het beheer van digitale sleutels.

Verantwoordelijkheden:

* <Functietitel> is verantwoordelijk voor het formeel goedkeuren van de procesbeschrijving digitaal sleutelbeheer.
* <Functietitel> is verantwoordelijk voor het opstellen en het beheren van de procesbeschrijving voor digitaal sleutelbeheer.

# Uitgangspunten privacy

Het algemene uitgangspunt in dit IBP-beleid is dat persoonsgegevens in overeenstemming met de AVG en gerelateerde wet- en regelgeving op zorgvuldige wijze worden verwerkt. Om aan dit uitgangspunt te voldoen verwerkt <naam schoolbestuur> persoonsgegevens in overeenstemming met de privacyvuistregels die in verderop in dit hoofdstuk worden uiteengezet. <Naam schoolbestuur> treft verdiepende maatregelen om de beleidsthema’s in dit IBP-beleid in te vullen.

Persoonsgegevens

Persoonsgegevens zijn gegevens die direct of indirect over iemand gaan en dus naar een persoon te herleiden zijn, zoals een naam of e-mailadres. Naast gewone persoonsgegevens - denk aan contactgegevens en onderwijsnummers - onderscheidt de AVG bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens. Daarnaast bestaat een categorie ‘gevoelige’ persoonsgegevens die niet expliciet in de AVG is benoemd. Dit zijn persoonsgegevens die vanwege hun aard privacygevoelig zijn en daarom extra bescherming verdienen.

* **Bijzondere persoonsgegevens** zijn gegevens die te maken hebben met bijvoorbeeld ras of etnische afkomst, gezondheid, religie of seksueel gedrag. De verwerking van deze gegevens is verboden, tenzij een wettelijke uitzondering bestaat zoals toestemming van de betrokkene.
* **Strafrechtelijke gegevens** zijn gegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten. De verwerking van deze gegevens is ook verboden, tenzij hiervoor een wettelijke uitzondering geldt.
* **Gevoelige persoonsgegevens** zijn gegevens die een groter privacyrisico vormen dan gewone persoonsgegevens. Denk aan financiële gegevens, burgerservicenummers (BSN), beoordelingen of gegevens van kwetsbare leerlingen.

**NB**: Nummers ter identificatie van een persoon, zoals het BSN, mogen alleen worden gebruikt voor specifieke doeleinden die in de wet zijn vastgelegd. Een onderwijsnummer (persoonsgebonden nummer) is gelijk aan het BSN.

Privacyvuistregels

Bij het verwerken van persoonsgegevens houdt <naam schoolbestuur> rekening met onderstaande vuistregels. Door deze basisprincipes te volgen zorgen we ervoor dat we kunnen voldoen aan de AVG.

1. **We verwerken persoonsgegevens rechtmatig en transparant**

<Naam schoolbestuur> verzamelt en gebruikt persoonsgegevens op een eerlijke en transparante manier. Persoonsgegevens worden alleen verwerkt als daarvoor een wettelijke grondslag bestaat in de AVG. We leggen altijd duidelijk uit waarom we bepaalde gegevens nodig hebben, wat we ermee doen en hoe lang we deze gegevens bewaren. Daarom informeren we ouders en leerlingen tijdig over het gebruik van hun persoonsgegevens, via een transparante privacyverklaring. Dit gebeurt bijvoorbeeld op het moment van inschrijving van een leerling.

1. **We verwerken persoonsgegevens voor specifieke doeleinden**

<Naam schoolbestuur> verwerkt persoonsgegevens alleen wanneer vooraf de specifieke doeleinden voor de verwerking zijn bepaald. Deze doeleinden worden vastgelegd. Persoonsgegevens worden niet voor andere, niet-verenigbare, doelen verwerkt. We zullen dus niet persoonsgegevens verzamelen omdat die wellicht ooit van pas gaan komen. We doen dit alleen met vooraf bepaalde, duidelijke en gerechtvaardigde doelen, zoals het plannen van onderwijs en communiceren met leerlingen en ouders over de voortgang en schoolactiviteiten.

1. **We verwerken alleen noodzakelijke persoonsgegevens**

<Naam schoolbestuur> verzamelt alleen persoonsgegevens die noodzakelijk zijn voor het doel waarvoor ze worden verwerkt. We vragen dus niet om meer gegevens dan we daadwerkelijk nodig hebben en hanteren hierbij het uitgangspunt ‘zo min mogelijk’. We onderzoeken altijd of we met minder gegevens of enkel met anonieme gegevens kunnen werken. Zo vragen we bij de inschrijving van een leerling alleen om de gegevens die relevant zijn voor het kunnen bieden van onderwijs en bewaren we geen overbodige gegevens die niet nodig zijn voor onze schoolactiviteiten.

1. **We zorgen dat persoonsgegevens juist en actueel zijn**

<Naam schoolbestuur> treft maatregelen om ervoor te zorgen dat persoonsgegevens correct en actueel zijn. Onjuiste of achterhaalde gegevens worden geactualiseerd of verwijderd. Leerlingen en ouders kunnen op een laagdrempelige manier doorgeven dat persoonsgegevens incorrect zijn en/of gewijzigd moeten worden. Onze processen en systemen worden zo ingericht dat de juistheid van gegevens zoveel mogelijk wordt afgedwongen en gecontroleerd.

1. **We bewaren persoonsgegevens niet langer dan nodig**

<Naam schoolbestuur> bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor ze zijn verzameld. Zodra gegevens niet meer nodig zijn, worden ze verwijderd of geanonimiseerd. We houden ons hierbij aan vooraf vastgestelde bewaartermijnen. Zo wordt het leerlingendossier (inclusief rapporten en schoolprestaties) na uitschrijving van een leerling niet langer bewaard dan nodig is voor administratieve en onderwijsdoeleinden en dus zo spoedig mogelijk verwijderd, in ieder geval binnen 2 jaar na uitschrijving.

1. **We zorgen voor een passende bescherming van persoonsgegevens**

We kunnen de privacy van leerlingen, ouders en medewerkers alleen goed beschermen als we op een veilige manier met hun persoonsgegevens omgaan. We zijn daarom verantwoordelijk voor het treffen van passende technische en organisatorische beveiligingsmaatregelen. Die maatregelen moeten ervoor zorgen dat de persoonsgegevens op een passende wijze worden beveiligd en worden beschermd tegen verlies, vernietiging, beschadiging of onrechtmatige verwerking. Dit doen we bijvoorbeeld door het gebruik van veilige systemen voor de opslag van leerlinggegevens en het opleiden van personeel in het veilig omgaan met gevoelige gegevens.

1. **We kunnen aantonen dat we voldoen aan de AVG**

We zijn verantwoordelijk voor het naleven van bovengenoemde vuistregels en kunnen daarmee aantonen dat we voldoen aan de belangrijkste uitgangspunten van de AVG. Dit doen we bijvoorbeeld door het bijhouden van een verwerkingsregister en het uitvoeren van *Data Protection Impact Assesments* (DPIA’s) voor gegevensverwerkingen met een hoog privacyrisico.

1. **We kunnen ons ethisch verantwoorden**

Bij het beoordelen van verwerkingen van persoonsgegevens houdt <naam schoolbestuur> niet alleen rekening met de vereisten uit de AVG (‘*mogen we dit?*’), maar nadrukkelijk ook met ethische aspecten (‘*willen we dit*?). Het gaat hierbij dus niet om de vraag of we iets ‘mogen’ of ‘kunnen’, maar juist om de vraag of we iets zouden moeten ‘willen’ als school. Ethische aspecten spelen in het bijzonder een rol bij verwerkingen die privacyrisico’s kunnen opleveren, bijvoorbeeld bij het gebruik van meekijksoftware of schermcontroles. Dit moet ook worden bezien vanuit een ethisch afwegingskader. We stellen ons dan ook eerst de vraag of we het kunnen uitleggen aan leerlingen en ouders.

# Beleidsthema’s privacy

## Verwerkingsregister

***Toelichting***

* *Om te voldoen aan de AVG moet je kunnen aantonen dat je in een verwerkingsregister informatie bijhoudt over de verwerkingsactiviteiten die in je organisatie plaatsvinden.*
* *Daarnaast heb je een procedure nodig voor het opnemen van wijzigingen in het verwerkingsregister.*

<Naam schoolbestuur> heeft maatregelen getroffen om aantoonbaar te voldoen aan de eisen uit de AVG. Dit houdt onder meer in dat <naam schoolbestuur> kan aantonen dat de verwerking van persoonsgegevens voldoet aan de uitgangspunten uit de AVG. <Naam schoolbestuur> geeft onder meer invulling aan haar verantwoordingsplicht door een overzicht bij te houden met informatie over de persoonsgegevens die zij verwerkt. Dit heet het verwerkingsregister. Dit register bevat bijvoorbeeld informatie over de leerlingenadministratie of het HR-systeem. Het bijhouden van het verwerkingsregister zorgt voor een goed overzicht van welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt. Het register stelt <naam schoolbestuur> in staat te voldoen aan haar verantwoordingsplicht.

Het verwerkingsregister bevat van afzonderlijke verwerkingsactiviteiten informatie over onder meer de doeleinden voor de verwerking, de toepasselijke grondslag onder de AVG, een beschrijving van de betrokkenen, een beschrijving van de persoonsgegevens, de toepasselijke bewaartermijnen en de ontvangers waarmee persoonsgegevens worden gedeeld.

### Legitiem doel en doelbinding

***Toelichting***

* *Controleer of onderstaande doeleinden en persoonsgegevens relevant en volledig zijn en vul aan waar nodig.*

Persoonsgegevens worden alleen verwerkt als een specifiek, vooraf bepaald doel is vastgesteld door <naam schoolbestuur> Dit doel moet duidelijk en in begrijpelijke taal aan de betrokkenen worden uitgelegd. Persoonsgegevens mogen niet voor andere doeleinden worden gebruikt.

<Naam schoolbestuur> verwerkt persoonsgegevens om haar verplichtingen als onderwijsinstelling na te kunnen komen. Het schoolbestuur verwerkt persoonsgegevens in de eerste plaats om onderwijs te kunnen bieden aan haar leerlingen en om activiteiten die hieraan ondersteunend zijn te kunnen uitvoeren. Hierbij valt te denken aan verwerkingen in het kader van het aanmeldproces, om te communiceren met leerlingen en ouders/verzorgers, het bijhouden van de leerlingenadministratie, het maken van roosters en om de voortgang bij te houden. Ook verwerkt het schoolbestuur persoonsgegevens van haar medewerkers in haar rol als werkgever. <Naam schoolbestuur> verwerkt bij deze werkzaamheden verschillende (categorieën) persoonsgegevens, waaronder contactgegevens, naam, geboortedatum en gegevens betreffende de aard en het verloop van het onderwijs. <Naam schoolbestuur> verwerkt deze persoonsgegevens op basis van grondslagen uit de AVG, bijvoorbeeld omdat sprake is van een wettelijke taak of verplichting, een gerechtvaardigd belang of op basis van toestemming.

Als gegevens toch voor een ander doel nodig zijn, dan mag dit alleen als dat doel verenigbaar is met het oorspronkelijke doel. Om te bepalen of dit het geval is, moet onder andere worden gekeken naar:

* De relatie tussen het nieuwe en het oorspronkelijke doel.
* De context waarin de gegevens zijn verzameld en de redelijke verwachtingen van de betrokkenen.
* Het soort persoonsgegevens; gevoelige gegevens verdienen extra bescherming.
* De mogelijke gevolgen voor betrokkenen.
* Bescherming van de gegevens, zoals versleuteling of pseudonimiseren.

Voor elke nieuwe verwerking moet <naam schoolbestuur> de rechtmatigheid, zorgvuldigheid en noodzaak opnieuw beoordelen. De specifieke doeleinden worden voorafgaand aan de verwerking bepaald en vermeld in de privacyverklaring om betrokken te informeren. Ook worden de doeleinden opgenomen in het verwerkingsregister. Voordat gegevens voor een ander doel worden gebruikt, vindt overleg plaats met de privacy officer en indien nodig ook met de functionaris gegevensbescherming.

### Grondslag

<Naam schoolbestuur> moet voor iedere verwerking van persoonsgegevens een geldige reden hebben. De AVG noemt dit een grondslag. <Naam schoolbestuur> verwerkt persoonsgegevens alleen op basis van de in de AVG genoemde grondslagen:

* de betrokkene heeft **toestemming** verleend, bijvoorbeeld voor het maken en delen van foto’s of video’s.
* de verwerking is noodzakelijk voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is, bijvoorbeeld het verwerken van salaris om de arbeidsovereenkomst met werknemers na te komen.
* de verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting,** bijvoorbeeld het delen van salarisinformatie met de Belastingdienst voor de uitvoering van de belastingwetgeving.
* de verwerking is noodzakelijk om **de vitale belangen** van de betrokkene te beschermen, bijvoorbeeld bij een levensbedreigende situatie waarbij het noodzakelijk is dat bepaalde gegevens van een leerling acuut aan hulpverleners moeten worden doorgeven.
* de verwerking is noodzakelijk om uitvoering te geven aan een **taak van algemeen belang**, hierbij gaat het om wettelijk vastgestelde taken en bevoegdheden**.** Zo heeft <naam schoolbestuur> de wettelijke taak om onderwijs te bieden.
* de verwerking is noodzakelijk voor de behartiging van een **gerechtvaardigd belang** van <naam schoolbestuur>of van een derde. Denk hierbij aan het verwerken van medewerkersgegevens voor het opstellen van managementrapportages ten behoeve van beleidsontwikkeling of het gebruik van bewakingscamera’s op het schoolplein.

De toepasselijke grondslag wordt vooraf vastgesteld, bijvoorbeeld middels een DPIA, en benoemd in de privacyverklaring om betrokken te informeren. Ook wordt de toepasselijke grondslag opgenomen in het verwerkingsregister.

## Informatieplicht

***Toelichting***

* *Hier beschrijf je hoe informatie over de gegevensverwerking eenvoudig, toegankelijk en in begrijpelijke taal beschikbaar is, zodat het duidelijk is voor de betrokkenen waarom en hoe persoonsgegevens worden verwerkt. Bij het gebruik van geautomatiseerde besluitvorming of profilering hou je rekening met strengere eisen op het gebied van informeren.*

<Naam schoolbestuur> verwerkt persoonsgegevens op een behoorlijke en transparantie manier. Dit is in begrijpelijke taal inzichtelijk voor de betrokkenen. <Naam schoolbestuur> informeert leerlingen en medewerkers voorafgaand aan de gegevensverwerking op transparante wijze via een duidelijke privacyverklaring. Deze privacyverklaring wordt gepubliceerd op de website. Daarnaast informeert de school medewerkers en sollicitanten ook via een aparte privacyverklaring. Hiermee zorgt <naam schoolbestuur> ervoor dat betrokkenen weten welke persoonsgegevens worden verwerkt en voor welke doeleinden dit gebeurt. Ook zijn ze op de hoogte van de rechten die ze hebben.

Wordt gebruikt gemaakt van geautomatiseerde besluitvorming of profilering? Dan gelden extra strenge regels, ook op het gebied van transparantie. Dat betekent onder andere dat medewerkers en leerlingen goed moeten worden geïnformeerd over het gebruik hiervan en duidelijk moet worden uitgelegd op basis van welke criteria het besluit tot stand is gekomen. Ook moet de mogelijkheid bestaan een nieuw besluit te nemen waarbij een mens de gegevens beoordeelt. Op die manier beschermen we medewerkers en leerlingen tegen onrechtmatige verwerking.

## Toestemming

***Toelichting***

* *Maak je gebruik van toestemming als grondslag? Zorg dan dat aan de wettelijke eisen voor toestemming wordt voldaan, zoals het kunnen aantonen dat toestemming is gegeven.*

Bij het gebruik van toestemming als grondslag gelden een aantal voorwaarden:

* Toestemming moet op een begrijpelijke en toegankelijke manier worden gevraagd, in duidelijke taal en niet verborgen in algemene voorwaarden of lange teksten.
* Toestemming moet vrijwillig worden gegeven en moet ook weer gemakkelijk ingetrokken kunnen worden.
* <Naam schoolbestuur> moet kunnen aantonen dat toestemming is verkregen, bijvoorbeeld door logs of ondertekende formulieren.
* Voor kinderen onder de 16 jaar moet een wettelijke vertegenwoordiger toestemming geven. Dit geldt ook voor personen onder curatele, bewind of mentorschap. <Naam schoolbestuur> verifieert of deze vertegenwoordiger daadwerkelijk toestemming heeft gegeven.

Leerlingen (of hun wettelijke vertegenwoordigers) worden in bepaalde situaties om toestemming gevraagd. Denk aan de situatie dat <naam schoolbestuur> foto’s of video’s van leerlingen maakt en publiceert. Dit mag alleen als de school vooraf toestemming heeft verkregen. Omdat een gezagsrelatie bestaat tussen <naam schoolbestuur> en haar leerlingen en medewerkers, moet goed worden beargumenteerd waarom toestemming in specifieke gevallen in vrijheid kan worden gegeven. <Naam schoolbestuur> gaat daarom terughoudend om met het gebruik van deze grondslag. Voordat toestemming als grondslag wordt gebruikt, vindt overleg plaats met de privacy officer en indien nodig ook met de functionaris gegevensbescherming.

## Privacy by design en privacy by default

***Toelichting***

* *Privacy by design houdt in dat je**een zo vroeg mogelijk stadium passende technische en organisatorische maatregelen inbouwt om te voldoen aan de regels uit de AVG. Privacy by default houdt in dat instellingen standaard privacyvriendelijk staan ingesteld.*

*Privacy by design* betekent dat <naam schoolbestuur> bij de ontwikkeling, het ontwerp, de selectie en het gebruik van toepassingen, diensten en producten zo vroeg mogelijk rekening houdt met privacyrisico’s en passende waarborgen inbouwt om de privacy van betrokkenen te beschermen. Neemt <naam schoolbestuur> bijvoorbeeld een leerlingvolgsysteem in gebruik? Dan moet in een vroeg stadium al worden nagedacht over passende toegangsbeperkingen. Leraren horen alleen inzicht te krijgen in de noodzakelijke gegevens van hun eigen leerlingen. *Privacy by default* betekent dat de standaardinstellingen van een product, dienst of proces op de meest privacyvriendelijke instelling staan. Maakt <naam schoolbestuur> bijvoorbeeld een profiel aan op sociale media? Dan mag dit profiel niet standaard openbaar zichtbaar zijn.

Hiermee zorgt <naam schoolbestuur> ervoor dat zo vroeg mogelijk rekening wordt gehouden met privacybeginselen en op die manier privacyrisico’s tijdig worden gemitigeerd.

### Dataminimalisatie

<Naam schoolbestuur> verzamelt alleen gegevens die noodzakelijk zijn voor het doel dat voorafgaand aan de verwerking is vastgesteld. De verzamelde gegevens dienen toereikend, ter zake dienend en niet bovenmatig te zijn. Hiermee voorkomt <naam schoolbestuur> dat te veel gegevens worden verwerkt. Bij de aanmelding van een leerling verzamelt <naam schoolbestuur> bijvoorbeeld alleen de informatie die nodig is om de leerling op de juiste manier in te schrijven. Denk aan naam, geboortedatum, adres en contactgegevens van ouders/verzorgers. Extra informatie, zoals het beroep van de ouders, is niet relevant voor de inschrijving en hoort daarom niet te worden verzameld. Daarnaast moet de verwerking van persoonsgegevens op de minst ingrijpende wijze plaatsvinden. Als het beoogde doel op een privacyvriendelijkere manier kan worden bereikt, dan kiest <naam schoolbestuur> hiervoor. Op deze manier voldoet <naam schoolbestuur> eveneens aan de principes van *privacy by design*.

## Bewaartermijnen

***Toelichting***

* *Persoonsgegevens moeten worden vernietigd wanneer ze niet meer nodig zijn voor de vastgestelde doelen. Dit gebeurt na afloop van de vastgestelde bewaartermijnen. Verwijs naar je bewaar- en vernietingsbeleid voor het bewaren van persoonsgegevens.*

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor zij zijn verzameld. Dit gebeurt in overeenstemming met het bewaar- en vernietigingsbeleid van <naam schoolbestuur>. Na het verlopen van de toepasselijke bewaartermijnen zorgt <naam schoolbestuur> ervoor dat persoonsgegevens tijdig worden vernietigd (of geanonimiseerd). Hierdoor worden persoonsgegevens beter beschermd tegen onnodige verwerking en datalekken. Zo worden bijvoorbeeld overzichten van schoolprestaties en rapporten uiterlijk tot 2 jaar na uitschrijving van een leerling bewaard. Het schooladvies wordt tot uiterlijk 5 jaar na uitschrijving van een leerling bewaard.

## Afhandelen van datalekken

***Toelichting***

* *Vanuit de AVG heb je de verplichting**datalekken adequaat en tijdig af te handelen. In de procedure datalekken beschrijf je hoe je dat doet.*

Voorbeelden van datalekken zijn een gestolen laptop, een verloren usb-stick, of een e-mail met persoonsgegevens die naar de verkeerde persoon is verstuurd. Datalekken moeten direct worden gemeld via <contactpunt naam schoolbestuur toevoegen> en geregistreerd in het interne register voor beveiligingsincidenten en datalekken. Risicovolle datalekken moeten worden gemeld aan de Autoriteit Persoonsgegevens en ook aan de betrokkenen als het datalek waarschijnlijk een hoog risico voor hen oplevert. De privacy officer beoordeelt of zo'n melding nodig is. Dit gebeurt als het nodig is in samenspraak met de functionaris gegevensbescherming.

## Data Protection Impact Assessment

***Toelichting***

* *Voorafgaand aan de verwerking van gegevens moet worden gecontroleerd of de regels uit de AVG worden nageleefd. Bij hoogrisico verwerkingen moet dat met een Data Protection Impact Assessment (DPIA).*

Voor elke nieuwe verwerking van persoonsgegevens, bijvoorbeeld een nieuw proces, technologie of applicatie, controleert <naam schoolbestuur> of de privacybeginselen uit de AVG worden nageleefd. Bij verwerkingen met een hoog privacyrisico wordt eerst een *Data Protection Impact Assessment* (DPIA) uitgevoerd. Een DPIA brengt in kaart hoe groot de kans is dat de privacy van betrokkenen wordt geschaad, waar de risico's liggen en welke gevolgen dit kan hebben. Op basis van de uitkomsten van de DPIA neemt <naam schoolbestuur> maatregelen om deze risico's te mitigeren.

## Uitwisseling persoonsgegevens

***Toelichting***

* *Je mag alleen persoonsgegevens delen met andere partijen als daar een rechtmatige grondslag voor bestaat.*
* *Voordat je gegevens deelt met andere partijen, moet je daar goede afspraken over maken.*

Een verwerker is een partij die in opdracht van <naam schoolbestuur> persoonsgegevens verwerkt, zoals een leverancier van een leerlingadministratiesysteem. Als <naam schoolbestuur> een verwerker inschakelt om persoonsgegevens te verwerken, dan worden privacyafspraken vastgelegd in een verwerkersovereenkomst. Bepaalt <naam schoolbestuur> samen met één of meerdere partijen het doel en middelen voor de verwerking van persoonsgegevens? Dan is sprake van een zogenaamde gezamenlijke verwerkingsverantwoordelijkheid. In dat geval worden ook contractuele afspraken gemaakt rondom de zorgvuldige en veilige verwerking van gegevens.

Persoonsgegevens kunnen ook beschikbaar worden gesteld aan partijen die niet als verwerkers worden aangemerkt, maar als ‘derden’. Deze derden verwerken persoonsgegevens niet in opdracht van een verwerkingsverantwoordelijke, maar voor hun eigen doel. Een verwerkersovereenkomst is daarom ook niet nodig, maar er moet wel een grondslag bestaan om de persoonsgegevens te delen. Denk aan de situatie waarin <naam schoolbestuur> gegevens over medewerkers deelt met de Belastingdienst ten behoeve van de loonaangifte. De Belastingdienst verwerkt deze gegevens voor haar eigen wettelijke doeleinden en handelt niet als verwerker.

Gegevensverwerking buiten de EER

Schakelt <naam schoolbestuur> een verwerker in uit een land buiten de Europese Economische Ruimte (EER) dat geen passend beschermingsniveau biedt? Dan gelden aanvullende voorwaarden. Bij een gegevensdeling buiten de EER moeten namelijk (juridische, technische en organisatorische) waarborgen zijn genomen om het beschermingsniveau ook buiten de EER te laten voldoen aan de AVG, zodat de persoonsgegevens voldoende beschermd blijven. Om dit te bereiken is meer nodig dan alleen het sluiten van een verwerkersovereenkomst. In dat geval maakt <naam schoolbestuur> gebruik van de Europese modelcontracten, de zogenaamde ‘Standard Contractual Clauses’, en neemt <naam schoolbestuur> aanvullende risicogebaseerde beveiligingsmaatregelen. Ook vindt voorafgaand aan de gegevensdeling afstemming plaats met de privacy officer en afdeling informatiebeveiliging om te beoordelen of de getroffen maatregelen voldoende zijn.

**NB**: De bepalingen van de meest recente versie van het convenant ‘Digitale onderwijsmiddelen en privacy’ zijn leidend bij het maken van afspraken met leveranciers, die als verwerkers in opdracht van de school persoonsgegevens verwerken.

## Rechten van betrokkenen

***Toelichting***

* *Je bent vanuit de AVG verplicht leerlingen, docenten en andere medewerkers te faciliteren bij de uitoefening van hun rechten en handelt AVG-verzoeken tijdig en adequaat af.*

Betrokkenen hebben op grond van de AVG recht op controle op de verwerking van hun persoonsgegevens. Een betrokkene kan onder andere gebruikmaken van het recht op inzage, rectificatie, verwijdering en bezwaar. Leerlingen, leraren en andere medewerkers kunnen een verzoek tot uitoefening van deze rechten indienen via: <kanaal indienen AVG-verzoek toevoegen>. Ook hebben betrokkenen het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens.
<Naam schoolbestuur> draagt er zorg voor dat de informatie over het uitoefenen van deze rechten op een transparante manier is verstrekt aan betrokkenen via een privacyverklaring. <Naam schoolbestuur> zal binnen de wettelijke termijnen, uiterlijk binnen één maand, schriftelijk reageren op het verzoek. In uitzonderlijke situaties kan de reactietermijn worden verlengd, maar dan wordt dit wel binnen een maand gecommuniceerd. Voor AVG-verzoeken geldt een identificatieplicht, zodat de identeit van de verzoeker kan worden vastgesteld. Hiertoe kan <naam schoolbestuur> om extra informatie verzoeken, maar zal hierbij terughoudend zijn met het verzoeken om een kopie identiteitsbewijs.

# Verantwoording IBP

## Naleving AVG

Er vindt toezicht plaats door <naam schoolbestuur> op de naleving van de normen uit dit beleid. Van belang is dat <naam functies> hun verantwoordelijkheid nemen en medewerkers aanspreken in geval van tekortkomingen. <Naam schoolbestuur> besteedt in dit verband actief aandacht aan informatiebeveiliging en privacy bij de aanstelling van medewerkers, tijdens functioneringsgesprekken en via bewustwordingscampagnes.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan <naam schoolbestuur> de betrokken verantwoordelijke medewerkers maatregelen opleggen binnen de kaders van de CAO en toepasselijke wetgeving. Voor toezicht op de naleving van de AVG vervult de functionaris gegevensbescherming (FG) een belangrijke rol. De FG kan bijvoorbeeld informatie verzamelen over gegevensverwerkingen en beoordelen of deze aan de AVG voldoen. Ook kan de FG adviezen en aanbevelingen verschaffen aan <naam schoolbestuur>

## Rapportage

***Toelichting***

* *Het schoolbestuur* *kan het monitoren en rapporteren over de toepassing van het beleid delegeren. Denk bijvoorbeeld aan de verschillende verantwoordelijken voor de beleidsthema’s die rapporteren aan het schoolbestuur over de voortgang. Leg vast hoe deze rapportage plaatsvindt.*

<Naam schoolbestuur> heeft de verantwoordelijkheid om het IBP-beleid formeel goed te keuren en te monitoren of het IBP-beleid door de organisatie wordt toegepast. Periodiek <bepaal de frequentie> wordt hierover gerapporteerd in<bepaal waar deze rapportage vastgelegd wordt>.

## Beleidsherziening

Het IBP-beleid wordt door <naam schoolbestuur> eenmaal per <invullen herzieningstermijn> getoetst en indien nodig herzien. Bij een substantiële wijziging van het IBP-beleid of in geval van belangrijke ontwikkelingen of veranderingen in wet- en regelgeving, volgt er indien nodig een beleidswijziging.