

**AVG**

**Informatiebeveiligings- en privacy beleid**

**Stichting jenaplanonderwijs Epe e.o.**

Het informatiebeveiligings- en privacy beleid is aangepast aan de eisen en termen vanuit de AVG. Elke organisatie moet niet alleen de privacy wetgeving naleven, maar moet ook aantoonbaar voldoen aan de AVG.

Bij het template hoort een document met dezelfde inhoud, maar dan voorzien van een aparte toelichting. Die toelichting bevat verdere uitleg en verwijzingen naar onderliggende documenten, afspraken en procedures. Hiermee wordt de ‘kapstokfunctie’ van het beleid inzichtelijker.

**Bron**

 Kennisnet

**Bewerkt voor basisschool t Hoge Land door:**

Johan van der Pols, directeur-bestuurder

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versie** | **Status** | **Datum** | **Auteur** | **Functie** |
| eind | concept | Juni 2020 | Johan van der Pols | Directeur-bestuurder |

**Vastgesteld door Stichting jenaplanonderwijs Epe e.o.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Naam** | **Functie** |
| eind | 16 juni 2020 | Maarten Heere | Voorzitter Raad van Toezicht  |

**Met instemming van de MR van Stichting jenaplanonderwijs Epe e.o.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Naam** | **Functie** |
| eind | 4 juli 2020 | Stijn Snoek | Voorzitter MR  |

[1 Het belang van informatiebeveiliging en privacy 4](#_Toc506118805)

[2 Toelichting informatiebeveiliging en privacy 4](#_Toc506118806)

[2.1 Toelichting informatiebeveiliging 4](#_Toc506118807)

[2.2 Toelichting privacy 4](#_Toc506118808)

[2.3 Vervlechting informatiebeveiliging en privacy 4](#_Toc506118809)

[3 Doel en reikwijdte 4](#_Toc506118810)

[3.1 Doel 4](#_Toc506118811)

[3.2 Reikwijdte 5](#_Toc506118812)

[4 Beleid – Hoe doen we dat? 5](#_Toc506118813)

[5 Uitwerking van het beleid – Wat doen we? 7](#_Toc506118814)

[5.1 Relevante wet- en regelgeving 7](#_Toc506118815)

[5.2 Basisregels bij het omgaan met persoonsgegevens 7](#_Toc506118816)

[5.3 Ondersteunende richtlijnen en procedures 7](#_Toc506118817)

[5.4 Voorlichting en bewustzijn 8](#_Toc506118818)

[5.5 Classificatie en risicoanalyse 8](#_Toc506118819)

[5.6 Incidenten en datalekken 8](#_Toc506118820)

[5.7 Planning en controle 8](#_Toc506118821)

[5.8 Naleving en sancties 8](#_Toc506118822)

[5.9 Logging en monitoring 9](#_Toc506118823)

[6 Organisatie - Wie doet wat? 10](#_Toc506118824)

[6.1 Rollen en verantwoordelijkheden 10](#_Toc506118825)

[Bijlage 1: Ondersteunende richtlijnen en procedures 13](#_Toc506118826)

[Bijlage 2: Organisatie; wie doet wat 18](#_Toc506118827)

# Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ict. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ict. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ict en persoonsgegevens brengt nieuwe kwetsbaarheden en risico’s met zich mee. Het goed regelen van I**nformatie Beveiliging en Privacy** (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico’s tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

# Toelichting informatiebeveiliging en privacy

## Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.

Informatiebeveiliging richt zich op de volgende aspecten:

* Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
* Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
* Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico’s in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

## Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:

*Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.*

## Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis om informatiebeveiliging en privacy binnen Stichting jenaplanonderwijs Epe e.o. te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

# Doel en reikwijdte

## Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

* Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
* Het garanderen van de privacy van alle betrokkenen waarvanStichting jenaplanonderwijs Epe e.o. persoonsgegevens verwerkt, waaronder kinderen, hun ouders/verzorgers en medewerkers
* Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (IBP-beleid) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkenen (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en Stichting jenaplanonderwijs Epe e.o. voldoet aan relevante wet- en regelgeving.

## Reikwijdte

* Het IBP-beleid binnen Stichting jenaplanonderwijs Epe e.o. geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
* Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Stichting jenaplanonderwijs Epe e.o. waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Stichting jenaplanonderwijs Epe e.o. persoonsgegevens verwerkt.
* Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Stichting jenaplanonderwijs Epe e.o. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (b.v. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina’s van) websites en of social media).
* Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
* IBP-beleid heeft binnen Stichting jenaplanonderwijs Epe e.o. raakvlakken met:
* *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
* *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
* *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen
* *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers

# Beleid – Hoe doen we dat?

Stichting jenaplanonderwijs Epe e.o. hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van Stichting jenaplanonderwijs Epe e.o. neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
2. Stichting jenaplanonderwijs Epe e.o. voldoet aan alle relevante wet- en regelgeving.
3. Bij Stichting jenaplanonderwijs Epe e.o. is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van Stichting jenaplanonderwijs Epe e.o. om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming herzien.
4. Stichting jenaplanonderwijs Epe e.o. zal alle betrokkenen helder en actief informeren over de verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.
5. Stichting jenaplanonderwijs Epe e.o. legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Stichting jenaplanonderwijs Epe e.o. voldoet hiermee aan de documentatieplicht.
6. Binnen Stichting jenaplanonderwijs Epe e.o.is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.
7. Stichting jenaplanonderwijs Epe e.o. is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
8. Stichting jenaplanonderwijs Epe e.o. classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico’s die we willen afdekken en de benodigde investeringen en de tenemen maatregelen.
9. Stichting jenaplanonderwijs Epe e.o. sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.
10. Stichting jenaplanonderwijs Epe e.o. verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich ‘fatsoenlijk’ gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Stichting jenaplanonderwijs Epe e.o. heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
11. Informatiebeveiliging en privacy is bij Stichting jenaplanonderwijs Epe e.o. een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
12. Stichting jenaplanonderwijs Epe e.o. kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.
13. Stichting jenaplanonderwijs Epe e.o. neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico’s, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.

Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt Stichting jenaplanonderwijs Epe e.o. aanvullende afspraken vast over de technische maatregelen.

1. Stichting jenaplanonderwijs Epe e.o. zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

# Uitwerking van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de invulling van het beleid.

## Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

* Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
* Wet goed onderwijs en goed bestuur PO/VO
* Wet onderwijstoezicht
* Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
* Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)\*
* Archiefwet
* Leerplichtwet
* Auteurswet
* Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.

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

## Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de **vijf vuistregels** met betrekking tot de omgang met persoonsgegevens te weten:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.
3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie**: de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

## Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

## Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico’s op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico’s wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, kinderen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP, de FG, en de Security Officer met het bestuur als eindverantwoordelijke.

## Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de betrouwbaarheidsaspecten die van belang zijn.

Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ict)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

## Incidenten en datalekken

Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings)incidenten kunnen worden gemeld bij de AVG-functionarissen binnen de school.

Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

## Planning en controle

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door de bestuurder-directeur. Hierbij wordt rekening gehouden met:

* De status van de informatiebeveiliging als geheel (beleid, organisatie, risico’s);
* de actuele geinventariseerde risico’s;
* de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent Stichting jenaplanonderwijs Epe e.o. een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

## Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.

Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de directeur-bestuurder en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door de directeur-bestuurder vast te stellen reglement.

Mocht de naleving van dit beleid ernstig tekort schieten, dan kan Stichting jenaplanonderwijs Epe e.o. de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

## Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt er voor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

# Organisatie - Wie doet wat?

## Rollen en verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij Stichting jenaplanonderwijs Epe e.o.

|  |  |  |  |
| --- | --- | --- | --- |
| **Niveau** | **Wie****Rollen** | **Hoe****Verantwoordelijkheid / taken** | **Wat****Realiseren / vastleggen**  |
| **Richtinggevend****(strategisch)** | Directeur-bestuurderRvT**D-B** schrijft beleid | * Eindverantwoordelijk
* IBP-beleidsvorming, -vastlegging en het uitdragen ervan
* Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens
* Evalueren toepassing en werking IBP-beleid op basis van rapportages
* Organisatie IBP inrichten
 | * Informatiebeveiligings- en privacy beleid
* Baseline / basismaatregelen
* Reglement FG vaststellen
* Privacyreglement vaststellen
 |
| **Sturend****(tactisch)** | Manager IBP, Verantwoordelijke IBP, informatiemanager ofprivacy officer (de persoon die inhoudelijk verantwoordelijk is voor IBP)Manager IBP: JohanOok ouders en kinderen meenemen. Kinderraad erin betrekken. Ouders in de ouderraad**.**Oudergeleding MR.Welke regels moeten we hebben, wat vind jij belangrijk over jouw privacy. | * Inhoudelijk verantwoordelijk voor IBP
* IBP-planning en controle
* Adviseert bestuur/directie over IBP
* Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse
* Hanteren IBP normen en wijze van toetsen
* Evalueren IBP-beleid en maatregelen
* Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze
* Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen
 | Processen, richtlijnen en procedures IBP, waaronder: * Activiteitenkalender
* Protocol beveiligingsincidenten en datalekken ( overkoepelend protocol)
* Security awareness activiteiten
 |
| Functionaris voor Gegevensbescherming en/ofPrivacy officerFG: Carla  | * Toezicht op naleving privacy wetgeving
* Voorlichting privacy en stimuleren bewustwording
* Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens
* Afwikkeling klachten en incidenten
 | * Verwerkersovereenkomsten regelen
* Brief toestemming gebruik beeldmateriaal
* Opstellen informatie documentatie richting leerlingen, ouders / verzorgers
* Sociale media reglement
* Gedragscode ict en internetgebruik
* Gedragscode medewerkers en leerlingen
* Privacyreglement,
* procedure IBP-incident afhandeling
* Inrichten meldpunt datalekken ( functionaris gegevens bescherming)

privacy@jenaplanepe.nl  |
| Domeinverantwoordelijke/ Proceseigenaren Waaronder o.a.:ICT, HRM / P&O, facilitair, onderwijs,financiën, inkoop en administratie | * Classificatie / risicoanalyse in samenwerking met Manager IBP (Informatiemanager / verantwoordelijke IBP / privacy officer)
* Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur/CvB/directie
* Samen met functioneel beheer en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
* Samen met functioneel beheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.
 | * Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister ( Parnassys)
* Classificatie- en risicoanalyse documenten. ( overzicht alle persoonsgegevens die je verwerkt, hoe je dat doet en daar een risico analyse van maken. Zie kennisnet.) dan volgen de risico’s en de stappen die je moet ondernemen.

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder:* Toegangsmatrix diverse informatiesystemen en netwerk
 |
| **Uitvoerend****(operationeel)** | Security officer **(= ICT-coordinator)** Functioneel en/of applicatie beheerder**Wie heeft welke rechten?**MedewerkerDagelijkse leiding / leidinggevende / directie | * Incidentafhandeling (registreren en evalueren).
* Technisch aanspreekpunt voor IBP-incidenten.
* Uitvoeren taken conform gegeven richtlijnen en procedures.
* Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.
* Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan.
* Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers.
* Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid.
* Implementeren IBP-maatregelen.
* periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
* Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur.
 | Communiceren, informeren en toezien op naleving van o.a.:* IBP in het algemeen
* Regels passend onderwijs
* Hoe omgaan met leerling dossiers
* Wie mogen wat zien
* Gedragscode
* Omgaan met sociale media
* Mediawijs maken
 |

De verdere uitwerking van de rollen en taken staat beschreven in bijlage 2.

#

# Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

***Documenten:***  Aandachtspunten:

1. Procedure toestemming gebruik

beeldmateriaal Toestemmingsbrief begin schooljaar;

 Toestemmingsbrief per item

1. Procedure voor verwijderen van gegevens en bewaartermijnen:

***Bewaartermijn***

Leerlingdossier en administratierechten

Scholen moeten zich aan strenge regels houden bij het verwerken van persoonsgegevens. In wet- en regelgeving is ook bepaald hoe lang scholen het leerling dossier, examens en toetsen mogen bewaren.

* *Leerlingdossier*

Het leerlingdossier mag [maximaal 2 jaar worden bewaard](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/scholen-de-avg#hoe-lang-mag-ik-onder-de-avg-een-leerlingdossier-bewaren-6193) nadat de leerling van de school is uitgeschreven. Daarna moeten de gegevens verwijderd worden. Hierop zijn een aantal uitzonderingen:

* Gegevens over verzuim en in- en uitschrijving moeten tot 5 jaar na uitschrijving bewaard worden door de school. Daarna verwijdert de school deze gegevens.
* Gegevens over een leerling die naar een school voor speciaal onderwijs is doorverwezen moeten 3 jaar na uitschrijving bewaard worden door de school. Daarna verwijdert de school deze gegevens.
* Voor het organiseren van reünies mag de school adresgegevens van (oud-)leerlingen bewaren.
* *Personeelsdossier*

Voor sommige gegevens uit het personeelsdossier geldt een fiscale bewaarplicht. De belastingsdienst verplicht de werkgever om die gegevens een bepaalde periode te bewaren.

* Loonbelastingverklaring en kopie identiteitsbewijs ( 5 jaar na uitdiensttreding)
* Voor andere gegevens is 2 jaar een richtlijn na uitdiensttreding.

**Rechten betrokkenen**

* *Recht op dataportabiliteit:*

Onder de Algemene verordening gegevensbescherming (AVG) hebben mensen het recht op dataportabiliteit, oftewel overdraagbaarheid van persoonsgegevens.

In de AVG (artikel 20) heet dit het 'recht om gegevens over te dragen'. Het houdt in dat mensen het recht hebben om de persoonsgegevens te ontvangen die een organisatie van hen heeft.

Zo kunnen zij hun gegevens bijvoorbeeld makkelijk doorgeven aan een andere leverancier van dezelfde soort dienst. Ook kunnen mensen vragen om gegevens rechtstreeks over te dragen aan een andere organisatie.

*Recht op vergetelheid:*

In de volgende situaties moet een organisatie iemand persoonsgegevens wissen:

* De organisatie heeft de persoonsgegevens niet meer nodig voor de doeleinden waarvoor de organisatie ze heeft verzameld of waarvoor de organisatie ze verwerkt.
* De betrokkene heeft eerder (uitdrukkelijke) toestemming gegeven aan de organisatie voor het gebruik van zijn gegevens, maar trekt die toestemming nu in.
* De betrokkene maakt bezwaar tegen de verwerking. Er geldt op grond van artikel 21 van de AVG een absoluut recht van bezwaar tegen direct marketing. En een relatief recht van bezwaar als de rechten van de betrokkene zwaarder wegen dan het belang van de organisatie om de persoonsgegevens te verwerken.
* De organisatie verwerkt de persoonsgegevens onrechtmatig. Bijvoorbeeld omdat er geen wettelijke grondslag is voor de verwerking.
* De organisatie is wettelijk verplicht om de gegevens na bepaalde tijd te wissen.
* De betrokkene is jonger dan 16 jaar en de persoonsgegevens zijn verzameld via een app of website (‘dienst van de informatiemaatschappij’).

*Uitzonderingen recht op vergetelheid*

Het recht op vergetelheid geldt niet in de volgende situaties:

* De verwerking is noodzakelijk om het recht op vrijheid van meningsuiting en informatie uit te oefenen. Daarmee doet de AVG recht aan het principe dat privacy en vrijheid van meningsuiting gelijkwaardige grondrechten zijn.
* De organisatie verwerkt de gegevens omdat er een wettelijke verplichting is om dat te doen.
* De organisatie verwerkt de gegevens om openbaar gezag of een (wettelijk vastgelegde) taak van algemeen belang uit te oefenen.
* De organisatie verwerkt de gegevens voor een taak van algemeen belang op het gebied van de volksgezondheid.
* De organisatie moet de gegevens in het algemeen belang archiveren.
* De gegevens zijn noodzakelijk voor een rechtsvordering.

**Procesbeschrijving rechten betrokkenen**

Ouders en andere betrokkenen kunnen een aanvraag doen om de gegevens te wijzigen of te verwijderen.

De school moet een afweging maken of recht van vergetelheid toegepast moet gaan worden.

Wanneer iemand op grond van recht op vergetelheid vraagt zijn gegevens te wissen, dan moet dat onmiddellijk gebeuren, uiterlijk binnen een maand. Alleen als het om een heel complex verzoek gaat, hebben we twee maanden extra tijd. Wel moet aan betrokkene aangegeven worden dat het langer gaat duren.

Als een betrokkenen het reglement elektronisch indient, moeten we ook elektronisch reageren, tenzij de betrokkene vraagt het anders te doen.

**Privacyreglement :**

Bij persoonsgegevens gaat het om alle informatie over een persoon. Ook gegevens die indirect iets over iemand zeggen, zijn persoonsgegevens. Naam, adres, woonplaats, telefoonnummers, postcodes met huisnummers.

Gevoelige gegevens zoals ras, godsdienst, lidmaatschap van een vakbond, genetische of biometrische gegevens, gezondheid, seksuele leven, strafrechtelijke leven worden bijzondere persoonsgegevens genoemd.

* Verwerkingsverantwoordelijke beslist:

Welke gegevens worden bij ons verwerkt?

Waarom doen we dat?

Hoe doen we dat?

* Betrokkene:

Van wie school persoonsgegevens verwerkt.

* Andere partijen:

Verwerkersovereenkomst afsluiten.

* Verwerker:

Een persoon aan wie de verwerkersverantwoordelijke de gegevens verwerking heeft uitbesteed. Bijvoorbeeld een administratiekantoor.

Een verwerker is niet zelfstandig verantwoordelijk voor de verwerking van de persoonsgegevens, maar heeft wel afgeleide verplichtingen, voor onder meer beveiliging en geheimhouding van de gegevens.

Autorisatiematrix (wie mogen gegevens inzien, bewerken enz.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Parnassys**  |  |  |  |  |  |
| Administratie: | In- uitschrijvingen | Mailen naar allen | Gegevens alle kinderen kunnen inzien en bewerken. Uitdraaien gegevens  | OSO bestanden klaarzetten en binnen halen | Instellingen wijzigen (i.o.v.) |
| Intern begeleider  | Alle niveaus in Parnassys | Mailen naar allen | Gegevens alle kinderen kunnen inzien en bewerken. Uitdraaien gegevens | OSO bestanden binnen halen | Instellingen wijzigen (i.o.v.) |
| Directeur  | Alle niveaus in Parnassys | Mailen naar allen | Gegevens alle kinderen kunnen inzien en bewerken. Uitdraaien gegevens | OSO bestanden klaarzetten en binnen halen | Instellingen wijzigen (i.o.v.) |
| Teamleden  | Inzage in kinderen van hun bouwgroep | Mailen op bouwniveau  | Gegevens kinderen van hun bouw uitdraaien op bouwniveau |  |  |
| Ouders | Inzage in Parnassys op verzoek | Mails ontvangen | Info ParnasSys via teamleden over eigen kind, alleen op verzoek. |  |  |
| **Office 365** |  |  |  |  |  |
| It-medewerker | Alle niveaus van invoering |  | Zicht op de docentenschijf |  |  |
| administratie | Toegang tot eigen mailbox |  | Zicht op eigen documenten |  |  |
| Directeur  | Toegang tot eigen mailbox en van administratie |  | Zicht op docentenschijf, administratie en directieniveau |  |  |
| Team  | Toegang tot eigen mailbox |  |  |  |  |
| **Contacten**  |  |  |  |  |  |
| Administratie  | Contacten intern en extern | Contact loopt via: Gesprekken, telefoon, schriftelijk. Het schriftelijke gedeelte loopt via outlook computer met externe harde schijf | OudersLeveranciersBRON, DUO, BAO-BAO scholen, huurders, Onderwijsbureau Meppel,Schoolleveranciers, Canon, Gemeente Epe, Zwembad de Koekkoek, VO-scholen regio, Rond-communicatie, verhuur, schoonmaak, |  |  |
| Directeur  | Contacten in- en extern  | Contact verloopt via:Gesprekken, telefoon, schriftelijk. Het schriftelijke gedeelte loopt naar binnen via Office 365, naar buiten via outlook computer met externe harde schijf | OudersBestuurders scholen EpeBesturen kinderopvangCJGGemeente EpeDirecteuren jenaplanregioBesturen overleg Fredeshiem MeppelPO-raadInspectieDUOBronARBOLeveranciersAannemersOnderwijs Bureau MeppelLEJABurenBelastingKeuringsorganisaties zoals Janssen-Fritsen, speelmaatje, AJAX, media |  |  |
| Intern begeleider | Contacten met zorg voor kinderen als uitgangspunt | Contact verloopt via:Gesprekken, telefoon, schriftelijk. Het schriftelijke gedeelte loopt via Office 365 | Collega scholenOudersRemedial teachersZeeluweGGZ jeugdCJGOrthopedagoog Corine HuisintveldSpecialisten J Plesman en M Cramer.Zorginstellingen als Intraverte, Kentalis.IEP eimdtoets, Parnassys, aanmeldingen congressen |  |  |
| Teamleden  | Contacten met onderwijs en kind als uitgangspunt | Contact verloopt via:Gesprekken, telefoon, schriftelijk. Het schriftelijke gedeelte loopt via Office 365 | Ouders, VO-scholen, zorgverleners via Intern Begeleider, mensen met expertise die meedoen in de school, activiteiten buiten de school |  |  |
| **Apps**  |  |  |  |  |  |
| Team  | Niveaus per bouw |  | Zicht op kind-ontwikkelingen per stamgroep |  | verwerkersovereenkomst |
| **typetuin** |  |  |  |  |  |
| Team MB |  |  | Inzicht op groepsniveau |  | verwerkersovereenkomst |
| IT-medewerker |  |  | Inzicht op alle niveaus  |  |  |
| **werknemersgegevens**  | Direct functioneren bij directeur |  | Administratieve gegevens Onderwijsbureau:aanstellingsgegevens, financiën, verzuim, salaris, pensioen opbouw, verzekeringen, Arbo, e.d. |  | verwerkersovereenkomst |
| **BRON-DUO** | administratie | Digitaal  | Uitwisseling informatie |  | Verwerkersovereenkomst |
| **OSO** | Administratie  | Digitaal  | Uitwisseling informatie  |  | verwerkersovereenkomst |
| **Basispoort**  | Alle ICT-gebruikers | Digitaal  | Digitale schoolprogramma’s  |  | verwerkersovereenkomst |
| **Po-raad**  | Directeur-bestuurder | Digitaal Mijn inlogContact  | Verstrekken PO-informatie via website.Via eigen inlog gegevens verstrekkenPo-raad bijeenkomsten in het land en met Fredeshiem. Stemrecht.  |  | verwerkersovereenkomst |
|  |  |  |  |  |  |
| **KiVa** | KiVa-team | digitaal | Monitoring kinderen sociaal-emotioneel |  | Verwerkersovereenkomst |

Afspraken gebruik sociale media

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Emailadressen ouders | Met toestemming in informatieboekje voor de andere ouders en teamleden | -schooladministratie-penningmeester ouderraad-parnassys-weekbulletin (BCC) | -Facebook school, alleen met toestemming |  | 2 overeenkomsten met ouders |
| Emailadressen team | Schooladressen met voornaam of gekoppeld aan de functie. | directie@jenaplanepe.nladministratie@jenaplanepe.nlib@jenaplanepe.nl   |  |  | werkgerelateerd |
| Emailadressen RVT | RVT@jenaplanepe.nl  | - |  |  | Komt binnen bij de secretaris |
| Emailadressen ouderraad  | OR@jenaplanepe.nl |  |  |  | Komt binnen bij de secretaris |
| EmailadressenMR | MR@jenaplanepe.nl |  |  |  | Komt binnen bij de secretaris |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Procedure rondom training medewerkers**

De functionarissen AVG gaan een opleiding volgen om op de hoogte te zijn van hun werkzaamheden als waakzaak oog. Tevens hebben zij een taak om bewustzijn te creëren onder het personeel om alert te blijven.

**Cameratoezicht**

Is niet aanwezig in school, wel op initiatief van de gemeente zijn camera’s buiten geplaatst. Doel is tegengaan vandalisme en inbraak. De gemeente heeft hier protocollen voor opgesteld.

**Wachtwoordbeleid**

Coördinatie ligt bij de ICT-medewerker op school. Wachtwoorden worden regelmatig veranderd.

**Responsible disclosure**

Privacy omschrijving in schoolgids en op de website:

Binnen de school worden slechts de volgende persoonlijke gegevens verwerkt:

• persoonsgegevens in relatie tot de wettelijke verplichtingen bij inschrijving van het kind

• gegevens die noodzakelijk zijn et het ook op de gezondheid of het welzijn van het kind

• gegevens over de aard en verloop van de ontwikkeling van het kind

• gegevens met het oog op de organisatie van het onderwijs

• gegevens ten behoeve van de begeleiding van het kind

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

• zoveel mogelijk wordt gekozen voor de uitwisseling van anonieme gegevens

• persoonlijke gegevens slechts worden uitgewisseld met toestemming van de ouders/verzorgers

• bij het ontbreken van toestemming van de ouders/verzorgers gebeurt dit op basis van het verenigbaarheid criterium uit de Wpb. Daarbij gaat het om de belangen van het kind in het kader van begeleiding, gezondheid en welzijn, waarbij slechts die gegevens mogen worden uitgewisseld, die een relatie hebben met het doel van de oorspronkelijke registratie.

Samen zijn we verantwoordelijk voor de privacy van de gegevens van de mensen met wie we werken.

Wanneer er een datalek ( inbreuk in verband met persoonsgegevens) ontstaat, wordt meteen de Autoriteit Persoonsgegevens geïnformeerd.. Tevens wordt melding gemaakt bij de betrokkenen.

*Er zijn drie categorieën datalekken te onderscheiden:*

Inbreuk op de vertrouwelijkheid

Wanneer er sprake is van een onbevoegde of onopzettelijke openbaring van, of toegang tot, persoonsgegevens.

Inbreuk op de integriteit

Wanneer er sprake is van een onbevoegde of onopzettelijke wijziging van persoonsgegevens.

Inbreuk op de beschikbaarheid

Wanneer er sprake is van een onbevoegd of onopzettelijk verlies van toegang tot, of vernietiging van, persoonsgegevens.

*Voorbeelden van datalekken zijn:*

Het verlies van een USB-stick met niet-versleutelde persoonsgegevens;

een cyberaanval waarbij persoonsgegevens zijn buitgemaakt;

een besmetting met ransomware waarbij persoonsgegevens ontoegankelijk zijn gemaakt.

Een datalek moet alleen gemeld worden, als dit leidt tot een risico voor de rechten en vrijheden van betrokkenen.

**Gedragscode ict en internetgebruik**

Er is beleid gemaakt voor ict gedrag en interngebruik.

**Procesbeschrijving melden datalekken**

1.De bewerker meldt een datalek bij de directeur-bestuurder.

De directeur-bestuurder meldt het lek bij AP via het meldloket van de AP met het invullen van een formulier.

2.Een melding bij de AP is alleen verplicht als het datalek ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, of als er een aanzienlijke kans is dat dit gebeurt. Volgens de privacywaakhond speelt de aard van de gelekte persoonsgegevens hierbij een belangrijke rol.

Gaat het over persoonsgegevens van gevoelige aard, dan is een melding over het algemeen noodzakelijk. De AP noemt een aantal voorbeelden:

• Bijzondere persoonsgegevens – zie vraag 2.

• Gebruikersnamen, wachtwoorden en inloggegevens.

• Gegevens die kunnen worden misbruikt voor identiteitsfraude, zoals biometrische gegevens als vingerafdrukken, identiteitsbewijzen en BSN-nummers.

• Gegevens over de financiële en economische situatie van de betrokkene, bijvoorbeeld over schulden, salaris- en betalingsgegevens.

• Gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene, zoals informatie over verslavingen, relatieproblemen en school- of werkprestaties.

De aard van de gegevens is niet de enige factor bij deze afweging. Zo kunnen ook de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen aanleiding zijn om de AP in te lichten.

Bij twijfel, doe voor de zekerheid een melding. De meldplicht voorziet namelijk niet in boetes voor onnodige meldingen, maar wel voor het niet melden van een datalek. Voor informatie: AP via het telefoonnummer 0900-3282535.

3.Betrokkenen op de hoogte stellen

Als het datalek waarschijnlijk ongunstige gevolgen heeft voor hun persoonlijke levenssfeer informeer je betrokkenen. Dit is bijvoorbeeld het geval als het verlies, onrechtmatig gebruik of misbruik van de persoonsgegevens kan leiden tot discriminatie of identiteitsfraude. Als er persoonsgegevens van gevoelige aard gelekt zijn, dan kun je er van uitgaan dat je de betrokkenen moet informeren. De betrokkene moet mogelijk maatregelen nemen om zich te beschermen tegen de gevolgen van het datalek. Bijvoorbeeld door zijn of haar

wachtwoorden te vervangen. Of door een nieuw paspoort aan te vragen.

Er is overigens wel een uitzondering. Als er passende technische maatregelen zijn genomen, waardoor de persoonsgegevens onbegrijpelijk of niet toegankelijk zijn voor onbevoegden, hoeft de betrokkene niet geïnformeerd te worden. Denk hierbij aan versleuteling door middel van encryptie of hashing.

Moet je een datalek melden bij de AP, maar is het onwaarschijnlijk dat het datalek ongunstige gevolgen heeft voor de persoonlijke levenssfeer van de betrokkenen, dan moet deze beslissing onderbouwd worden in de melding bij de AP.

**Registratie beveiligingsincidenten**

Er is een registratieformulier voor de persoon: ouder, kind, teamlid om een melding van een mogelijk datalek te maken.

Voor de functionaris is er een meldformulier om de stap naar de AP te maken.

**Risicoanalyse**

Er is een risicoanalyse formulier om een goed beeld te krijgen van de risico’s en de te nemen stappen.

**Procedure gegevensbeschermingseffectbeoordeling, (DPIA)**

Zie bijlage 3.

**Voorbeeld van informatievoorziening naar personeel.**

Zie bijlage 4.

# Bijlage 2: Organisatie; wie doet wat

Deze bijlage beschrijft hoe IBPop drie niveaus wordt georganiseerd.

* Richtinggevend (strategisch)
* Sturend (tactisch)
* Uitvoerend (operationeel)

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Stichting jenaplanonderwijs Epe e.o. voor elk niveau een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

Beschreven wordt welke rollen, welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

**Richtinggevend**

Stichting jenaplanonderwijs Epe e.o. is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.

De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd.

De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de manager IBP.

**Sturend**

Manager IBP is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau. De manager IBP moet:

* Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
* De uniformiteit bewaken binnen stichting jenaplanonderwijs Epe e.o.
* Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
* De verdere afhandeling van incidenten binnen stichting jenaplanonderwijs Epe e.o. coördineren

**Functionaris voor Gegevensbescherming of Privacy Officer**

De functionaris voor gegevensbescherming (FG) houdt binnen stichting jenaplanonderwijs Epe e.o. toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het verbeteren en stimuleren van bewustwording rondom IBP, het afhandelen van informatiebeveiligingsincidenten, adviseert over het regelen van privacy, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke (het bestuur). De FG heeft regelmatig overleg met manager IBP. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

**Security Officer, is tevens Portefeuillehouder ICT / ICT beheer (intern en extern)**

Adviseert samen met manager IBP de eindverantwoordelijke en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen stichting jenaplanonderwijs Epe e.o.

**Portefeuillehouder informatiebeveiliging**

Het managementlid dat ICT en informatiebeveiliging / privacy in zijn portefeuille heeft is gesprekspartner voor de manager IBP in kader van informatiebeveiliging en privacy binnen de organisatie.

**Domeinverantwoordelijke / proceseigenaar**

Binnen de school zijn er verschillende domeinen/processen, zoals ict, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, onderwijs et cetera. Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Deze proceseigenaar is tevens verantwoordelijk voor de risico’s die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico’s te verkleinen hebben proceseigenaren de volgende specifieke taken:

* Samen met de directeur-bestuurder stellen zij het beleid voor toegang (autorisaties) vast.
* Samen met functioneel beheer en ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
* Samen met functioneel beheer en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

**Uitvoerend**

**Security Officer (SO)**

De Security Officer, bij ons de IT-deskundige, vormt een technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers.

**Functioneel beheerder of Applicatiebeheerder: IT-RSG**

Ieder softwarepakket of (web-)applicatie heeft een beheerder. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden. De functioneel beheerder wordt vanuit de domeinverantwoordelijke / proceseigenaar voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

.

**Medewerker**

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. de gedragshandleiding AVG. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR)

**Leidinggevende**

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

* er voor te zorgen dat zijn medewerkers op de hoogte zijn van het IBP-beleid;
* toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
* periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
* als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de manager IBP. Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

Een IBP-team wordt organisatie breed zowel preventief als curatief benoemd voor informatiebeveiliging en privacy incidenten. De leden van het IBP-team zijn benoemd door de directeur-bestuurder en handelen in diens opdracht.

Het IBP-team van stichting jenaplanonderwijs Epe e.o. heeft de volgende opdracht:

* Het signaleren en registreren van alle privacy verzoeken, beveiligingsincidenten en datalekken. Het coördineren van de maatregelen en het toezien op de oplossing van problemen die tot incidenten hebben geleid of waardoor de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
* Het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers door het verspreiden van informatie;
* Het leveren van managementrapportages en verbetervoorstellen aan de directeur-bestuurder over de beveiligingsincidenten en verzoeken tot uitoefening privacyrechten van de betrokkenen.

Bij een calamiteit kan het IBP-team terstond bij elkaar worden geroepen op initiatief van de manager IBP, in opdracht van het stichting jenaplanonderwijs Epe e.o. Het doel hiervan is om de **continuïteit** van de informatievoorziening en de privacy te waarborgen. Onder calamiteiten worden verstaan:

* Datalek;
* Grote verstoringen van het netwerk (bijvoorbeeld DDoS aanval);
* Natuurrampen (brand, overstroming, storm, etc.).

Het IBP-team bij stichting jenaplanonderwijs Epe e.o. behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.

De werkzaamheden van het IBP-team bij stichting jenaplanonderwijs Epe e.o. is gedocumenteerd en door de directeur-bestuurder bekrachtigd.

Bijlage 3:

Stuk van Functionaris Gegevensverwerking, Carla: beschrijving van wat wij doen.

Onderwijs en AVG. (1e opzet 16-01-2020)

Met betrekking tot de privacywetgeving en voor de verwerking van persoonsgegevens in het leerlingdossier gelden een aantal regels:

1a Beveiliging en toegang tot leerlingdossiers.

Al onze cumputers beschikken over een inlogcode, behalve de laptops in de groepen. Deze worden door kinderen gebruikt die bijvoorbeeld werken met Bouw! (een spellingsprogramma), rekentuin, en typtuin. Voor het werken met deze programma’s is echter wel weer een individuele inlogcode benodigd. Toegang tot de leerlingadministratie benodigd ook een gebruikersnaam en een wachtwoord. Vervolgens zijn aan stamgroepleiders rollen toegekend. Zij hebben beperkt toegang tot b.v. leerlingkaarten en toetsoverzichten. Zij kunnen nergens wijzigingen aanbrengen.

 Tevens is het zo dat onze school beschikt over drie bouwen: een onderbouw (2) een middenbouw (3) en een bovenbouw (3).

 Stamgroepleiders kunnen alleen in hun eigen bouw kindgegevens inzien. Een collega van de onderbouw kan dus niet kindgegevens van de bovenbouw bekijken.

 Slechts de beheerder, directie en IB-er hebben de mogelijkheid alles in te zien.

1b Alleen gegevens verwerken noodzakelijk voor het doel.

 De gegevens van onze kinderen worden uitgewisseld met BRON/DUO; dit is verplicht.

 Ook de ambtenaar van de leerplicht kan beperkt gegevens opvragen. Hij/zij moet immers kunnen controleren of een kind ingeschreven is op een – in dit geval – basisschool. Zij kunnen niet inloggen in het LAS, maar corresponderen met DUO.

 2 x per jaar doen de kinderen van de bovenbouw mee aan een onderzoek genaamd KIVA. Kiva is een antipestprogramma. Tevens onderzoeken zij door middel van een enquête het welbevinden van de kinderen op onze school.

 Door middel van een soort EDEX-bestand worden de voor- en achternamen en geboortedata opgenomen in een enquête bestand van KIVA. Door middel van inloggegevens kan ieder kind individueel deze enquête invullen.

1c De gegevens die in het leerlingdossier worden verwerkt, moeten juist zijn.

Aan de hand van een door de ouders ingevuld inschrijfformulier worden kinderen opgenomen in de leerlingenadministratie.

 Door middel van uitwisseling met BRON wordt geverifieerd of het om het betreffende kind gaat (BSN).

1d Aantonen houden aan regels van AVG.

 Iedereen (m.b.t. Parnassys (LAV)) beschikt over persoonlijke inloggegevens. Welke gegevens toegankelijk zijn hangt af van je toegekende rol (directeur, beheerder, IB-er, stamgroepleider) en van de bouw waarin je werkzaam bent (onder- midden- of bovenbouw).

 Bij zij-instromers (kinderen die van andere basisscholen komen) en bij kinderen die wegens verhuizing of andere reden vertrekken naar een andere basisschool, maken wij gebruik van OSO. OSO is een beveiligd systeem, waarbij kindgegevens van de ene basisschool naar de andere basisschool getransporteerd worden. De vertrekkende school maakt een dossier aan, bericht de ontvangende school en via deze beveiligde omgeving worden gegevens uitgewisseld.

1e Leerlingen (of hun ouders) moeten hun privacyrechten kunnen uitoefenen.

 Binnen het basisonderwijs variëren de leeftijden van onze kinderen tussen 4 en 12-13 jaar. Totdat kinderen 16 jaar zijn, zijn het de ouders die privacyrechten kunnen uitoefenen.

1f De gegevensverwerking in de leerlingdossiers wordt opgenomen in het register van verwerkingsactiviteiten van de school.

 In ons LAS is uitsluitend door de IB-er, de directeur en de beheerder een verandering aan te brengen. De persoonlijke inlogcodes maken dat het systeem automatisch aangeeft wie de wijziging heeft doorgevoerd.

1g Scholen kunnen verplicht zijn om een DPIA (data protection impact assessment) uit te voeren voor het gebruik van het leerlingdossier.

 Lees boven- en onderstaande hoe wij dit gerealiseerd hebben.

 Privacyrechten:

Toestemming van betrokkene voor persoonsgegevensverwerking.

 Voor elk kind wordt specifiek een formulier ingevuld (en ondertekend) waarop de ouders/verzorgers kunnen aangeven of NAW-gegevens geplaatst mogen worden in een zogenaamd informatieboekje wat alleen intern verspreid wordt. Met betrekking tot foto- en/of filmmateriaal vragen wij ouders/verzorgers schriftelijk toestemming voor het gebruiken van foto’s en filmpjes in brochures over onze school, het (Jenaplanschool) blad “Mensenkinderen”, de schoolkalender (papieren vorm), het Bulletin (nieuwsblad) een flyer (voor open week) en de introfilm van school. Facebook is in deze opsomming niet opgenomen, daar wij geen facebookpagina meer hebben.

Foto’s en filmpjes worden onderling door ouders wel gedeeld op “klasbord”, een besloten appgroep. Ouders dienen onderling (mondeling) te overleggen of een foto van een vriendje of vriendinnetje op bijvoorbeeld een eigen facebookpagina geplaatst mag worden.

Wettelijke plicht van organisaties voor persoonsgegevensverwerking.

Als basisschool zijn wij verplicht gegevens uit te wisselen met BRON en DUO.

Autoriteit Persoonsgegevens.

Indien een betrokkene van mening is dat de gegevens van zijn of haar kind op een incorrecte wijze door een organisatie zijn verwerkt, dan kan diegene een klacht indienen bij de autoriteit persoonsgegevens (AP).

Welke gegevens zijn persoonsgegevens.

Tot de persoonsgegevens van betrokkenen, behoren alle gegevens die betrekking hebben op iemand waarvan de identiteit reeds bekend is, of diens identiteit middels de persoonsgegevens afleidbaar is.

AVG-privacyrechten per 25 mei 2018.

De AVG omschrijft 8 privacyrechten:

1. Recht op dataportabiliteit.

Binnen ons basisonderwijs is dit alleen van toepassing wanneer een kind onze school verlaat. Hetzij naar een andere basisschool (b.v. bij verhuizing) of naar het Voortgezet Onderwijs.

Via het voornoemde OSO worden dossiers via een beveiligde weg ontvangen door de vervolgschool. Vooraf wordt aan het dossier fiat van de ouders/verzorgers toegevoegd.

1. Recht op vergetelheid.

In de praktijk komt het er op neer dat een ouder/verzorger kan vragen om verwijdering van alle gegevens van het kind.

Wij zijn echter verplicht een wettelijke bewaartermijn in acht te nemen van 5 jaar. Dit in tegenstelling van de bewaartijd van 2 jaar, omdat gegevens met betrekking tot verzuim en in- en uitschrijving tot 5 jaar na vertrek beschikbaar moeten zijn.

Ontbrekend belang voor persoonsgegevensverwerking.

Dit is binnen het onderwijs minder van toepassing. Gegevens mogen 5 jaar bewaard blijven en zijn middels leerlingdossiers beveiligd verzonden aan vervolgscholen.

1. Recht op inzage.

Binnen onze Jenaplanschool hebben ouders te allen tijde het recht om het dossier van hun kind(eren) in te zien.

Veelal worden de gegevens ook besproken op zogenaamde 10-minuten gesprekken.

Ouders moeten sowieso hun toestemming geven voor het verzenden van het leerlingdossier aan een vervolgschool.

1. Recht op beperking van de gegevensverwerking.

Is binnen onze Jenaplanschool niet van toepassing. Het verzenden van gegevens van kinderen gebeurt uitsluitend aan BRON/DUO en aan de vervolgschool. Dit is rechtmatig.

1. Recht op rectificatie en aanvulling.

Dit is van toepassing indien de persoonsgegevens geheel of gedeeltelijk feitelijk onjuist zijn, onvolledig zijn, irrelevant voor het doel van de verwerking zijn of in strijd zijn met een wettelijke bepaling.

Binnen ons basisonderwijs komt dit sporadisch voor. De laatste mutatie vond 3 jaar geleden plaats na naamsverandering van een van de kinderen.

1. Recht op duidelijke informatie.

Binnen onze Jenaplanschool ontvangt elk (nieuw) gezin een informatieboekje en een schoolgids.

In de schoolgids staat uitvoerig beschreven op welke wijze en visie wij binnen onze school uiting aan geven aan Jenaplanonderwijs.

In het informatieboekje staan alle praktische zaken op onze school waaronder ondersteuningsprofiel, rapportfoliogesprekken, leertijd, ouderbijdrage, klachtenregeling, verlofregeling etc. Ook is er informatie opgenomen hoe wij omgaan met AVG binnen onze Jenaplanschool.

1. Recht met betrekking tot geautomatiseerde besluitvorming en profilering.

Als school maken wij geen besluiten op basis van eerder automatisch verwerkte gegevens. Tevens maken wij geen gebruik van automatische verwerking van persoonsgegevens met het doel om de persoonlijke aspecten van iemand te evalueren met betrekking tot gezondheid, economische situatie, persoonlijke voorkeuren, belangen, betrouwbaarheid, carrière of gedrag (profilering).

1. Recht op bezwaar.

Het maken van bezwaar heeft betrekking op het gebruik maken van persoonsgegevens van kinderen voor marketingdoeleinden.

Het gaat te ver om diensten van derden (psychologisch onderzoek, onderzoek op dyslexie of dyscalculie, logopedie etc.) te bestempelen als marketingdoeleinden. Al deze diensten kunnen alleen maar na overleg en met toestemming van ouders.

###  Datalek melden

Wij zijn er ons van bewust dat datalekken niet helemaal uit te sluiten is. Een verloren USB-stick of gestolen laptop is realiteit. Een datalek zullen wij zo snel mogelijk na ontdekking, zo mogelijk binnen 72 uur, melden bij de Autoriteit Persoonsgegevens. Deze meldingsplicht geldt niet als er geen risico’s voor (natuurlijke) personen uit voortkomen. Wel moeten we ook dan het datalek intern vastleggen en documenteren. Wij beschrijven het datalek, de gevolgen van het datalek en de genomen maatregelen.

De verwerkersovereenkomst.

Als een ander bedrijf de persoonsgegevens voor ons verwerkt en opslaat, dan moeten wij met dat bedrijf een verwerkersovereenkomst afsluiten. Zelfs zonder het wijzigen van gegevens kan er al sprake zijn van verwerken. Bijvoorbeeld als een externe helpdesk voor onze school gegevens inziet.

Wij hebben dan ook verwerkersovereenkomsten met:

Parnassys (LAS)

Basispoort (leverancier online leerprogramma’s)

BRON

….

….

….

N.B. Gezien bovenstaande hebben wij voldaan aan het Data Protection Impact Assesment (DPIA)

Bijlage 4

Stuk van Functionaris Gegevensverwerking, Carla: voorlichting voor het personeel:

De AVG: hoe ga je daar als school mee om? Waar moet je je aan houden en wat kan er allemaal wel en niet rondom de privacywetgeving? En wat is het ook alweer precies: AVG (Algemene Verordening Gegevensbescherming)? Op 25 mei is het een jaar geleden dat de AVG werd ingevoerd. Tijdens de *Regiobijeenkomst Slimmer in onderwijs* van Basisschool Apps op 8 mei 2019 op basisschool ’t Slingertouw in Eindhoven kwam onder meer dit onderwerp aan bod. We hebben de tips en tricks op een rij gezet over de AVG voor leerkrachten.



AVG-specialist Henk van der Pas, directeur van Stichting Scala, vertelt tijdens de bijeenkomst over de AVG, de nieuwe privacywet. ‘Waarom zou je als school aan de AVG willen voldoen?’, dat is één van zijn eerste vragen aan de aanwezigen. De belangrijkste reden is dat het wettelijk verplicht is, dat de persoonsgegevens waarmee je iemand direct en indirect kunt identificeren, beschermd zijn.

Daarnaast zijn er nog vijf vuistregels van de AVG opgesteld:

1. Het doel van het verzamelen van de gegevens moet duidelijk zijn. Het is bijvoorbeeld van belang dat je het telefoonnummer hebt van je leerlingen, want in noodgevallen moet je hen kunnen bereiken
2. Zes grondslagen uit de wet: alleen wanneer het van belang is om de persoonsgegevens vast te leggen, mogen scholen dat doen. Je hebt hier ook toestemming voor nodig van ouders. Dit kan bijvoorbeeld zijn: vitaal belang (bij allergieën is het wenselijk dat leerkrachten dat weten), gerechtvaardigd belang, nakomen van de wettelijke verplichting en uitoefenen van openbaar gezag
3. Dataminimalisatie: als school mag je alleen de informatie vragen die je echt nodig hebt om je werk goed te kunnen uitvoeren. Denk daarbij bijvoorbeeld aan: wat zet je in een leerling dossier? In dit dossier zet je alle informatie die noodzakelijk is om je werk te kunnen doen en die ouders ook in mogen zien
4. Transparantie: de betrokkene moet duidelijk weten wat zijn of haar rechten zijn over het gebruik van de persoonsgegevens
5. Data integriteit: leg goed vast wat de rechten zijn met foto’s maken. Ouders moeten toestemming geven voor het laten fotograferen en filmen van hun kinderen op school. Is er een app-groep van ouders waarin ze foto’s delen? Je bent daar als school niet verantwoordelijk voor, zolang je er niet zelf in zit.

Zorgvuldig omgaan met gegevens

Volgens Henk is het vooral van belang dat je zorgvuldig omgaat met de gegevens van leerlingen (en ouders).

* Vergrendel bijvoorbeeld je scherm als je niet in klas aanwezig bent
* Bedenk goed hoe je informatie deelt (via de mail of via een beveiligde omgeving)
* Beveilig je accounts met een goed wachtwoord en verander dat regelmatig
* Gebruik niet zomaar gratis apps, de persoonsgegevens die je daar in voert, zijn niet meer *AVG-proof*
* Zorg voor een veilige verbinding (https:// voor je website) en gebruik zo weinig mogelijk USB-sticks

N.B. Punt 5 is een behoorlijk punt van aandacht. Met behulp van Klasbord worden immers ook foto’s/filmpjes gedeeld. Het moet bij alle deelnemers van Klasbord heel duidelijk zijn dat deze foto’s/filmpjes dus niet zomaar op een persoonlijke facebookpagina mogen worden gezet. Bijvoorbeeld: je ziet een prachtige foto van je kind waar ook een vriendje/vriendinnetje op staat. Je wilt deze foto op je facebookpagina zetten. Je moet dan eerst toestemming vragen aan de ouder van dat vriendje/vriendinnetje.

We overwegen om dit op te nemen op het formulier waar ouders aan kunnen geven of zij akkoord gaan met bijvoorbeeld plaatsen van foto op website, bulletin etc.

Let in jouw groep ook op het volgende:

Geen privégegevens van kinderen (onderzoeken etc.) in een map in jouw groep. Zorg dat deze bij mij of bij Lorel achter slot en grendel opgeborgen worden.

Wellicht is het noodzakelijk om richting ouders e.e.a. te melden.

Immers, tijdens de weeksluiting zijn er nog steeds voldoende ouders die een filmpje of foto’s maken.

Zijn er op- en/of aanmerkingen? Je bent van harte welkom!

 Carla 22 januari 2020