JONG LEREN
stichting voor confessioneel onderwijs

# Informatiebeveiligings- en privacy beleid

| | |
|---|---|
| Status | Definitief |
| Versie | |
| | |
| Auteur | |
| Datum | 19-01-2018 |
| Evaluatie | |
| Verspreiding | |

# INLEIDING

Per 25 mei 2018 geldt de Algemene verordening gegevensbescherming (AVG). Vanaf die datum geldt dezelfde privacywetgeving in de hele EU. Nu hebben de lidstaten nog hun eigen nationale wetten, gebaseerd op de Europese privacyrichtlijn uit 1995. Op dit moment geldt in Nederland de Wet bescherming persoonsgegevens (Wbp).

De AVG zorgt onder meer voor:

- versterking en uitbreiding van privacyrechten;
- meer verantwoordelijkheden voor organisaties;
- dezelfde, stevige bevoegdheden voor alle Europese privacytoezichthouders.

Het onderwijsveld is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. Ook neemt de hoeveelheid informatie toe door ontwikkelingen als gepersonaliseerd leren met ict. Deze afhankelijkheid van ict en gegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het is van belang om adequate maatregelen te nemen op het gebied van informatiebeveiliging en privacy (IBP) 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.

**Bron**
Autoriteit persoonsgegevens
saMBO-ICT
Kennisnet

# Afkortingen:

IBP: Informatiebeveiliging en privacy
AVG: Algemene Verordening Gegevensbescherming
AP: Autoriteit persoonsgegevens
FG: functionaris voor gegevensbescherming

# INHOUDSOPGAVE

# HOOFDSTUK 1 Informatiebeveiliging en Privacy

## 1.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening te garanderen. Deze aspecten zijn:

- 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 onacceptabele risico's bij de uitvoering van onderwijs en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

## 1.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform huidige wet – en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die direct of indirect herleidbaar zijn tot een bepaald individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. 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.*

## 1.3 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijk onderdeel is van privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar, en zijn van elkaar afhankelijk. Het onderwerp informatiebeveiliging en privacy wordt afgekort tot IBP. Dit beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen stichting Jong Leren.

# HOOFDSTUK 2 DOEL EN REIKWIJDTE

## 2.1 Doel

***Dit beleid heeft als doelen:***

- ***Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.***
- ***Het garanderen van de privacy van leerlingen en medewerkers waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen.***

Dit beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet zijn tussen privacy, functionaliteit en veiligheid. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene, met name van medewerkers en leerlingen, wordt gerespecteerd en stichting Jong Leren voldoet aan relevante wet- en regelgeving.

## 2.2 Reikwijdte

- Het informatiebeveiligings- en het privacy beleid binnen stichting Jong Leren geldt voor alle medewerkers,[1] leerlingen, ouders/verzorgers, bezoekers en externe relaties (inhuur / outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van stichting Jong Leren. Het beleid heeft zowel betrekking op gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites.
- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen stichting Jong Leren waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, bezoekers en externe relaties (inhuur/outsourcing), evenals op andere betrokkenen waarvan stichting Jong Leren persoonsgegevens verwerkt.
- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van stichting Jong Leren evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het 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.

[1] Medewerkers: hieronder vallen ook stagiaires, vrijwilligers en invallers.

- IBP-beleid binnen stichting Jong Leren heeft 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 inzake aanschaf en gebruik van digitale leermiddelen.

# HOOFDSTUK 3 UITGANGSPUNTEN

## 3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij stichting Jong Leren zijn:

- Informatiebeveiliging en het privacy dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming (die 25 mei 2018 in werking treedt). De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen. Waarbij een goede balans tussen het belang van stichting Jong Leren om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is.
- Binnen stichting Jong Leren 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 fysieke documenten.
- De school 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 moeten goed geïnformeerd worden over de regelgeving rond het gebruik van informatie. Medewerkers hebben de plicht om op de hoogte te zijn en te blijven van de regelgeving rondom IBP (AVG).
- Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt bij stichting Jong Leren geclassificeerd via risico analyse document. De classificatie is het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risicoanalyse, waarbij gebruik gemaakt wordt van de classificatie. Er is een balans tussen de risico's (de kans en de impact) van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.
- Stichting Jong Leren sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) bewerkersovereenkomsten af als zij persoonsgegevens ontvangen van de school. Hierbij wordt gebruik gemaakt van de meest recente versie van het convenant 'Digitale leermiddelen privacy' (www.privacyconvenant.nl) en de bijbehorende model bewerkersovereenkomst. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis.
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. In de regel betekent dit dat we respect voor de school en elkaar hebben en iedereen in zijn waarde laten. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. stichting Jong Leren heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

- Binnen Jong Leren wordt geen gebruik gemaakt van digitale diensten waar de leeftijdsgrens boven de 12 jaar is. Indien dit wel het geval is zal toestemming gevraagd worden aan ouders/verzorgers.
- Informatiebeveiliging en privacy is bij stichting Jong Leren een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatiesystemen), wordt bij stichting Jong Leren vanaf de start rekening gehouden met informatiebeveiliging en privacy.

## 3.2 Uitgangspunten privacy

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij stichting Jong Leren zijn:

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 wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van Persoonsgegevens is gebaseerd op één van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
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 staan tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. 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 deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun Persoonsgegevens. Daarnaast 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.

Vanuit de AVG is het verplicht een registratie te hebben van al je verwerkingen. In dat register moet onder andere zijn opgenomen wat de grondslag is, de noodzaak (belangenafweging), welke gegevens, of er een bewerker is, bewaartermijn, etc.
Jong Leren heeft een register van alle verwerkingen van persoonsgegevens waarin bovenstaande uitgangspunten zijn uitgewerkt.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen. Bij alle registraties op basis van toestemming, zal stichting Jong Leren aan de Betrokkene een eenduidige zogenaamde Opt-in procedure worden aangeboden. Dit betekent dat elke betrokkene vooraf toestemming geeft persoonsgegevens te verwerken.

# HOOFDSTUK 4 WET- EN REGELGEVING

Stichting Jong Leren voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet bescherming persoonsgegevens
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van het convenant 'Digitale onderwijsmiddelen en privacy 2.0' leidend bij het maken van afspraken met leveranciers.

# HOOFDSTUK 5 ORGANISATIE

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.
Dit hoofdstuk beschrijft hoe IBP in stichting Jong Leren is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

Voor elk niveau wordt beschreven welke rollen welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen

## 5.1 Rollen (functies) rondom IBP

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken wordt bij stichting Jong Leren een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

## 5.2 Richtinggevend

**Eindverantwoordelijke (CvB)**
Het College van Bestuur 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.

## 5.3 Sturend

**Manager IBP (Bestuurssecretaris)**
Manager IBP is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke 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 Jong Leren
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen stichting Jong Leren coördineren

**Functionaris voor Gegevensbescherming**
Jong Leren heeft een functionaris voor gegevensbescherming (FG) aangesteld. De FG houdt binnen stichting Jong Leren toezicht op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG). De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. De FG heeft regelmatig overleg met manager IBP. De FG is meestal ook de contactpersoon voor klachten en vragen van betrokkenen.

**Stafmedewerker ICT / ICT beheer**
Adviseert samen met manager IBP het College van Bestuur en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen stichting Jong Leren.

**Proceseigenaar op stichtingsniveau en op schoolniveau**
Binnen de stichting zijn er verschillende afdelingen/processen, zoals ict, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, onderwijs et cetera. Op elk van deze domeinen/processen is een stafmedewerker verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies. De domeinverantwoordelijke/ proceseigenaar is verantwoordelijk voor de eigen registratie. Op schoolniveau is de directeur proceseigenaar.
Bij wijzigingen of nieuwe registraties kunnen ze de FG inlichten.

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 het College van Bestuur stellen zij het beleid voor toegang 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.
- Samen met functioneel beheer en ICT-beheer beoordelen zij regelmatig de toegangsrechten van gebruikers.

Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

## 5.4 Uitvoerend

**Veiligheidsbeheerder stichtingsniveau (stafmedewerker ICT via systeembeheerder)**
De veiligheidsbeheerder vormt een technisch aanspreekpunt inzake informatiebeveiliging voor het management en de medewerkers.

**Veiligheidsbeheerder schoolniveau (ICT-er via systeembeheerder)**
De veiligheidsbeheerder 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 in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in een handleiding verantwoord omgaan met databeveiliging. 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 beveiligingsincidenten, 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 beveiligingsbeleid;
- 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.

# HOOFDSTUK 6 CONTROLE EN RAPPORTAGE

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar getoetst en bijgesteld door het College van Bestuur. Hierbij wordt rekening gehouden met:

- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's)
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent stichting Jong Leren 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.

Voor alle overlegmomenten geldt dat deze zoveel mogelijk ingepast worden in bestaande overlegvormen met hetzelfde karakter waarbij op:

- **strategisch** niveau richtinggevend wordt gesproken over organisatie en compliance, alsmede over doelen, scope en ambitie op het gebied van IBP.
- **tactisch** niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering.
- **operationeel** niveau worden de onderwerpen besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm wordt decentraal georganiseerd, en indien nodig in elk organisatieonderdeel van stichting Jong Leren

## 6.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij stichting Jong Leren 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, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de manager IBP / informatie manager/ Security Officer met het College van Bestuur als eindverantwoordelijke.

## 6.2 Classificatie en risicoanalyse

Bij stichting Jong Leren heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de 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 kwaliteitsaspecten die van belang voor de informatievoorziening.

## 6.3 Incidenten en datalekken

Alle incidenten worden binnen 24 uur gemeld bij meldpunt.datalek@jl.nu. Binnen 48 uur wordt nadere informatie opgevraagd om te beoordelen of het incident bij de Autoriteit Persoonsgegevens (AP) gemeld dient te worden. Een incident dient binnen 72 uur gemeld te worden bij het AP. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken.

## 6.4 Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij Jong Leren wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instellingsbrede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het CvB vast te stellen reglement.
Mocht de naleving ernstig tekort schieten, dan kan stichting Jong Leren de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.
Bij stichting Jong Leren is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

# HOOFDSTUK 7 TRANSPARANTIE EN RECHTEN VAN BETROKKENEN

## 7.1 RECHTEN VAN BETROKKENEN

Betrokkenen hebben in de AVG verschillende rechten ten aanzien van persoonsgegevens:

### 7.1.1. Recht op informatie

Ouders en medewerkers moeten vooraf in begrijpelijke taal actief en laagdrempelig geïnformeerd worden over welke gegeven met welk doel worden verwerkt en wat de rechten van leerlingen zijn.

### 7.1.2. Inzage van gegevens

Ouders en medewerkers hebben recht op inzage in hun persoonsgegevens. Dat houdt in dat zij Jong Leren mogen vragen of deze persoonsgegevens van hen heeft vastgelegd en zo ja, welke. Zij hoeven geen reden te geven voor een inzageverzoek.

Vraagt iemand om inzage, dan moet Jong Leren diegene op een duidelijke en begrijpelijke manier laten weten:

- of Jong Leren zijn persoonsgegevens gebruikt, en zo ja:
- om welke gegevens het gaat;
- wat het doel is van het gebruik;
- aan wie Jong Leren de gegevens eventueel heeft verstrekt;
- wat de herkomst is van de gegevens, als deze bekend is.

Er is één uitzondering op het inzage geven: als het in het belang van de betrokkenen is om geen inzage te geven, blijft inzage achterwege. Bijvoorbeeld aan dossiervorming bij verdenking van misbruik of kindermishandeling. Het is in het belang van het kind om de ouders géén inzage te geven in die informatie te geven. Dit is echter een grote uitzondering waar terughoudend mee om moet worden gegaan.

**Reikwijdte inzagerecht**
Het recht op inzage betreft alleen inzage in iemands eigen gegevens. Mensen hebben dus geen recht op informatie over anderen. Gebruikt een organisatie persoonlijke werkaantekeningen als geheugensteuntje? Dan vallen deze aantekeningen niet onder het inzagerecht. Maar slaat de organisatie de aantekeningen vervolgens op in een dossier of verstrekt de organisatie deze aan anderen? Dan heeft degene over wie het gaat ook recht op inzage in deze aantekeningen.

### 7.1.3. Correctie van gegevens

Ouders en medewerkers hebben het recht om correctie van hun persoonsgegevens te vragen. Dat houdt in dat zij Jong Leren mogen vragen hun persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen.

Iemand kan om correctie vragen als zijn persoonsgegevens:

- feitelijk onjuist zijn;
- onvolledig zijn of niet ter zake doen voor het doel waarvoor ze zijn verzameld;
- op een andere manier in strijd met een wet worden gebruikt.

**Reikwijdte correctierecht**

Het correctierecht is niet bedoeld voor het corrigeren van professionele indrukken, meningen en conclusies waarmee iemand het niet eens is, voor zover deze ter zake doen. Wel mag diegene van de organisatie verwachten dat deze in ieder geval zijn schriftelijke mening toevoegt aan het dossier. Dat kan vooral een oplossing bieden bij situaties waarbij het om niet objectief vast te stellen feiten gaat.

### 7.1.4. Vergetelheid en verwijdering van gegevens

Dit houdt in dat Jong Leren in een aantal gevallen persoonsgegevens moet wissen als een betrokkene hierom vraagt. Dit geldt ook voor de back-up bestanden. daarnaast moet een bewerker geïnformeerd worden dat deze gegevens verwijderd moeten worden.
Het recht op vergetelheid geldt niet altijd. Alleen in de volgende situaties is het recht op vergetelheid van toepassing:

- Niet meer nodig: De organisatie heeft de persoonsgegevens niet meer nodig voor de doeleinden waarvoor de organisatie ze heeft verzameld of waarvoor de organisatie ze verwerkt.
- Intrekken toestemming: De betrokkene heeft eerder (uitdrukkelijke) toestemming gegeven aan de organisatie voor het gebruik van zijn gegevens, maar trekt die toestemming nu in.
- Bezwaar: 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.
- Onrechtmatige verwerking:De organisatie verwerkt de persoonsgegevens onrechtmatig. Bijvoorbeeld omdat er geen wettelijke grondslag is voor de verwerking.
- Wettelijk bepaalde bewaartermijn: De organisatie is wettelijk verplicht om de gegevens na bepaalde tijd te wissen.
- Kinderen: De betrokkene is jonger dan 16 jaar en de persoonsgegevens zijn verzameld via een app of website (‘dienst van de informatiemaatschappij’).

### 7.1.5. Recht van toestemming

Ouders en medewerkers hebben het recht om bij toestemming, ook een beperkte toestemming te geven of toestemming te onthouden voor een onderdeel van de verwerking.

### 7.1.6. Dataportabiliteit van gegevens

Dit houdt in dat een persoon het recht heeft om de persoonsgegevens te ontvangen die een organisatie van hen heeft. Zo kunnen zij hun gegevens bijvoorbeeld makkelijk doorgeven aan een andere organisatie van dezelfde soort dienst.

## 7.2 VERZOEK INDIENEN INZAGE PERSOONSGEGEVENS

Ouders, verzorgers en medewerkers kunnen een verzoek indienen ten aanzien van het recht op inzage. De betrokkene heeft het recht om alles in te zien. Dit verzoek moet schriftelijk of per mail ingediend worden bij de directeur van de school of bij de bestuurssecretaris. Voor het in behandeling nemen van het inzageverzoek dient u een kopie van uw identiteitsbewijs mee te sturen.

Jong Leren is verplicht binnen 4 weken schriftelijk of per e-mail te reageren op het inzageverzoek. Jong Leren kan 8 weken uitstel vragen voor het aanleveren van de persoonsgegevens als zij kan aantonen niet binnen 4 weken de gegevens aan te leveren.

Jong Leren kan op drie manieren inzage geven in uw persoonsgegevens:
- Door een volledig overzicht
- kopieën/afdrukken
- Inzage ter plekke.

Voor deze werkzaamheden worden geen kosten in rekening gebracht.

## 7.3 VERZOEK INDIENEN CORRECTIE, VERWIJDERING OF VERGETELHEID

Ouders, verzorgers en medewerkers kunnen een verzoek indienen ten aanzien van het recht op correctie, verwijdering, vergetelheid en dataportabiliteit. Dit verzoek moet schriftelijk of per mail ingediend worden bij de directeur van de school of bij het College van Bestuur. Voor het in behandeling nemen van het inzageverzoek dient u een kopie van uw identiteitsbewijs mee te sturen.
Jong Leren zal uiterlijk binnen 1 maand het verzoek uitvoeren.

Jong Leren voert de aanpassingen ook uit op de back-up van de bestanden en informeert derden partijen waaraan persoonsgegevens zijn verstrekt dat deze gegevens zijn gewist. En legt uit dat ook de ontvangers iedere kopie van of koppeling naar die persoonsgegevens moeten wissen.

Voor deze werkzaamheden worden geen kosten in rekening gebracht.

Jong Leren informeert betrokkenen als aan het verzoek is voldaan.

## 7.3 BEZWAAR INDIENEN

Betrokkenen kunnen bezwaar indienen. Hiervoor wordt verwezen naar de klachtenregeling van Jong Leren.

# BIJLAGE 1 TABEL ROLLEN EN TAKEN

| Niveau | Wie<br>Rollen | Hoe<br>Verantwoordelijkheid / taken | Wat<br>Realiseren / vastleggen |
|---|---|---|---|
| **Richting-gevend (strategisch)** | CvB<br>Directeur | • Eindverantwoordelijk<br>• IBP-beleidsvorming, -vastlegging en het uitdragen ervan<br>• Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens<br>• Evalueren toepassing en werking IBP-beleid op basis van rapportages<br>• Organisatie IBP inrichten | • Informatiebeveiligings- en privacy beleid<br>• Baseline / basismaatregelen<br>• Reglement FG vaststellen<br>• Privacyreglement vaststellen |
| **Sturend (tactisch)** | Manager IBP = bestuurs secretaris | • Inhoudelijk verantwoordelijk voor IBP<br>• IBP-planning en controle<br>• Adviseert CvB/directie over IBP<br>• Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse<br>• Hanteren IBP normen en wijze van toetsen<br>• Evalueren IBP-beleid en maatregelen<br>• Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze<br>• Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen | Processen, richtlijnen en procedures IBP, waaronder:<br>• activiteitenkalender<br>• Protocol beveiligingsincidenten en datalekken<br>• Bewerkersovereenkomsten regelen<br>• Brief toestemming gebruik foto's en video<br>• Opstellen informatie documentatie richting leerlingen, ouders / verzorgers<br>• Security awareness activiteiten<br>• Sociale media reglement<br>• Gedragscode ict en internetgebruik<br>• Gedragscode medewerkers en leerlingen |

| | | | |
|---|---|---|---|
| | Functionaris voor Gegevensbescherming | • Toezicht op naleving privacy wetgeving<br>• Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens\<br>• Afwikkeling klachten en incidenten | • Privacyreglement,<br>• procedure IBP-incident afhandeling<br>• Inrichten meldpunt datalekken |
| | Proceseigenaren waaronder:<br>ict, personeel (HRM / P&O), Facilitair, onderwijs, financiën, inkoop en administratie | • **Classificatie / risicoanalyse** *in samenwerking met Manager IBP (Informatiemanager / verantwoordelijke IBP / veiligheidsbeheerder)*<br>• Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door *CvB/directie*<br>• *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.<br>• *Samen met functioneel beheer en ICT* beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren. | • Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst)<br>• Classificatie- en risicoanalyse documenten.<br><br>Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder:<br><br>• Toegangsmatrix diverse informatiesystemen en netwerk |

| Niveau | Wie<br>Rollen | Hoe<br>Verantwoordelijkheid / taken | Wat<br>Realiseren / vastleggen<br>Vanuit de Wiki |
|---|---|---|---|
| **Uitvoerend (operationeel)** | veiligheidsbeheerder = stafmedewerker ICT en netwerkbeheerder<br><br>Functioneel beheerder = ICT-er<br><br>Medewerker<br><br>Dagelijkse leiding / leidinggevende / directie | • Incidentafhandeling (registreren en evalueren).<br>• Technisch aanspreekpunt voor IBP-incidenten.<br>• Uitvoeren taken conform gegeven richtlijnen en procedures.<br>• Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.<br>• Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan.<br>• Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers.<br>• Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid.<br>• Implementeren IBP-maatregelen.<br>• periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;<br>• Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur. | Communiceren, informeren en toezien op naleving van o.a.:<br><br>• IBP in het algemeen<br>• Regels passend onderwijs<br>• Hoe omgaan met leerling dossiers<br>• Wie mogen wat zien<br>• Gedragscode<br>• Omgaan met sociale media<br>• Mediawijs maken |

# BIJLAGE 2 VOORBEELDBRIEF INZAGE PERSOONSGEGEVENS

Naam
T.a.v.
Adres
Postcode en woonplaats

Datum

Geachte heer/mevrouw,

Met verwijzing naar artikel 15 van de AVG wil ik graag binnen vier weken schriftelijk van u weten:

- of u mijn persoonsgegevens gebruikt, en zo ja:
- om welke gegevens het gaat;
- wat het doel is van het gebruik;
- aan wie u de gegevens eventueel heeft verstrekt;
- wat de herkomst is van de gegevens, als deze bekend is.

Indien u mijn persoonsgegevens gebruikt, verzoek ik u mij kopieën van alle mijn persoon betreffende stukken, een papieren overzicht of een uitdraai van het digitale dossier te geven.

Hoogachtend,

Naam
geboortedatum
adres
postcode en woonplaats