

Informatieveiligheids- en privacybeleid



**ÓSCAR
ROMERO
SCHOLEN**

samen bouwen aan je toekomst

IVP-BELEID

VZW Óscar Romeroscholen

voor:

- 22962: Harduynschool Oudegem
- 116947: Óscar Romerocollege 1
- 36285: Óscar Romerocollege 2
- 36301: Óscar Romerocollege 3
- 36335: Óscar Romerocollege 4
- 36343: Óscar Romerocollege 5
- 107821: Vrije Basisschool De Bellewij Denderbelle
- 128496: Vrije Basisschool De Margriet Baardgem
- 22962: Vrije Basisschool De Oogappel Appels
- 23119: Vrije Basisschool De Schatkist Wieze
- 22988: Vrije Basisschool HEHASchool
- 27037: Vrije Basisschool voor Buitengewoon Onderwijs - Het Laar
- 23093: Vrije Basisschool Lebbeke
- 128652: Vrije Basisschool Meldert
- 23085: Vrije Basisschool Minnestraal Lebbeke
- 22954: Vrije Basisschool Óscar Romerocollege
- 23011: Vrije Basisschool - Visitatie
- 22996: Vrije Lagere School – Óscar Romerocollege

Deze nota maakt deel uit van het informatieveiligheid- en privacybeleid (IVPB).

| Versie | Datum | Status | Auteur(s) | Opmerking |
|--------|------------|--------|---|-----------|
| 1.0 | 2018-02-22 | GELDIG | Isabelle Putteman + Cel informatieveiligheid | |
| 1.1 | 2019-01-14 | GELDIG | Jan Luyten | |
| | | | | |
| | | | | |

Inhoud

| | | |
|-----|--|----|
| 1 | Inleiding | 4 |
| 1.1 | Toelichting informatieveiligheid | 4 |
| 1.2 | Toelichting privacy | 4 |
| 1.3 | Vervlechting informatieveiligheid en privacy | 4 |
| 2 | Doel en reikwijdte | 5 |
| 2.1 | Doel | 5 |
| 2.2 | Reikwijdte | 5 |
| 3 | Uitgangspunten | 6 |
| 3.1 | Algemene beleidsuitgangspunten | 6 |
| 3.2 | Uitgangspunten privacy | 7 |
| 4 | Wet- en regelgeving | 7 |
| 5 | Organisatie | 7 |
| 5.1 | Rollen (functies) rondom IVP | 8 |
| 5.2 | Richtinggevend | 8 |
| 5.3 | Sturend..... | 8 |
| 5.4 | Uitvoerend | 9 |
| 6 | Controle en rapportage | 9 |
| 6.1 | Voorlichting en bewustzijn | 10 |
| 6.2 | Classificatie en risicoanalyse | 10 |
| 6.3 | Incidenten en datalekken | 10 |
| 6.4 | Controle, naleving en sancties | 10 |
| | Bijlage 1: Tabel IVP rollen en taken | 11 |
| | Bijlage 2: Aanvullende nota's | 13 |

1 Inleiding

Informatie en ict zijn noodzakelijk in de ondersteuning van het onderwijs. Denken we maar aan de leerlingadministratie- en leerlingvolgsystemen, agenda- en rapportprogramma's, oefen- en toetssystemen.... Vaak verwerken deze geautomatiseerde systemen persoonsgegevens (van leerlingen, ouders, lesgevers...) en is de privacywetgeving (AVG) hierop van toepassing.

Deze informatieverwerking en het gebruik van ict brengen risico's met zich mee. Denken we bijvoorbeeld maar aan een cyberaanval waarbij de gegevens versleuteld worden, een vergissing waardoor gegevens onherroepelijk gewist zijn, de natuur (bijv. overstroming of brand), et cetera. Het niet beschikbaar zijn van ict, incorrecte administraties en het uitlekken van gegevens kan leiden tot inbreuken op het geven van onderwijs en het vertrouwen in onze bovengenoemde instellingen (zie pagina 2).

Deze bedreigingen maken het noodzakelijk om adequate maatregelen te nemen op het gebied van informatieveiligheid en privacy (IVP) om de risico's die gepaard gaan met deze bedreigingen tot een aanvaardbaar niveau te reduceren. Om dit structureel aan te pakken is het noodzakelijk dat we een duidelijk beeld schetsen waarover het gaat, een doel stellen en de manier bepalen waarop we dit doel willen bereiken.

1.1 Toelichting informatieveiligheid

Onder informatieveiligheid wordt verstaan: het nemen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatie en ict zo maximaal mogelijk te garanderen.

Deze kwaliteitsaspecten zijn:

- **Beschikbaarheid:** de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- **Integriteit:** de mate waarin gegevens en/of functionaliteiten juist, volledig en actueel zijn.
- **Vertrouwelijkheid:** de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.
- **Controleerbaarheid:** de mate waarin het mogelijk is om achteraf parameters die van belang zijn voor beschikbaarheid, integriteit of vertrouwelijkheid te verifiëren.

Onvoldoende informatieveiligheid kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en bij de dagdagelijkse werking van de onderwijsinstelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en imagooverlies.

1.2 Toelichting privacy

Privacy gaat over de verwerking van persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform de huidige wet- en regelgeving. De bescherming van de privacy regelt onder andere de voorwaarden waaronder persoonsgegevens gebruikt mogen worden.

Persoonsgegevens zijn hierbij alle gegevens van een geïdentificeerd of identificeerbaar individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. Denken we maar aan het verzamelen, raadplegen, bijwerken, verspreiden tot en met het wissen van deze gegevens.

1.3 Vervlechting informatieveiligheid en privacy

Informatieveiligheid is noodzakelijk om privacy te waarborgen. Beide begrippen zijn met elkaar verbonden. Het onderwerp informatieveiligheid en privacy wordt afgekort tot IVP. Deze beleidstekst ligt ten grondslag aan de aanpak van informatieveiligheid en privacy binnen de bovengenoemde instellingen (zie pagina 2).

2 Doel en reikwijdte

2.1 Doel

Dit beleid heeft als doelen:

- Het waarborgen van de continuïteit van het onderwijs en de dagdagelijkse werking van de bovengenoemde instellingen (zie pagina 2).
- Het garanderen van de privacy van leerlingen en medewerkers waardoor beveiligings- en privacy-incidenten zoveel mogelijk worden voorkomen.

Dit beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een goede balans moet zijn tussen privacy, functionaliteit, veiligheid en middelen. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene, met name van medewerkers, leerlingen en ouders wordt gerespecteerd en dat de bovengenoemde instellingen (zie pagina 2) voldoen aan relevante wet- en regelgeving.

2.2 Reikwijdte

- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen de bovengenoemde instellingen (zie pagina 2) waaronder in ieder geval: alle medewerkers, vrijwilligers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties, evenals op andere betrokkenen waarvan de bovengenoemde instellingen (zie pagina 2) persoonsgegevens verwerkt.
- Dit beleid is van toepassing op zowel de digitale als geschreven verwerking van persoonsgegevens.
- Het IVP-beleid geldt voor alle medewerkers, vrijwilligers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties die uit hoofde van hun taak, op school of thuis persoonsgegevens verwerken.
- Het beleid heeft betrekking op gecontroleerde informatie die door onszelf 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 en sociale media. Hiervoor werken de bovengenoemde instellingen (zie pagina 2) met **gedragscodes**.
- Het IVP-beleid binnen de bovengenoemde instellingen (zie pagina 2) heeft raakvlakken met:
 - Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen;(IDPB of CPBW)
 - Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties;
 - IT-beleid; met als aandachtspunten de aanschaf, het beheer, het gebruik en/of het uit dienst stellen van hardware, software, services en (digitale) leermiddelen;
 - Participatie van leerlingen, hun ouders/verzorgers en medewerkers.

3 Uitgangspunten

3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij de bovengenoemde instellingen (zie pagina 2) zijn:

- IVP dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de **Algemene Verordening Gegevensbescherming (AVG)**.
De verwerking van persoonsgegevens is steeds gebaseerd op één van de in deze verordening vastgelegde rechtmatigheden. Hierbij willen we een goede balans zoeken tussen het belang van de bovengenoemde instellingen (zie pagina 2) om persoonsgegevens te verwerken en het belang van de betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn/haar persoonsgegevens.
- Het schoolbestuur, VZW Óscar Romeroscholen, is als rechtspersoon de **verwerkingsverantwoordelijke** voor alle persoonsgegevens die in opdracht van de bovengenoemde instellingen (zie pagina 2) verwerkt worden.
- De bovengenoemde instellingen (zie pagina 2) beheren ook informatie waarvan de intellectuele eigendom (het **auteursrecht**) toebehoort aan derden. Medewerkers en leerlingen moeten dus goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.
- Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt daarom bij de bovengenoemde instellingen (zie pagina 2) geclassificeerd. Deze **classificatie** vormt het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risico-analyse, waarbij gebruik gemaakt wordt van de classificatie. Het beleid maakt een balans tussen de risico's van hetgeen we willen beschermen en de benodigde maatregelen.
- De bovengenoemde instellingen (zie pagina 2) sluiten met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) **verwerkersovereenkomsten** af indien deze persoonsgegevens ontvangen van de school.
- Binnen de bovengenoemde instellingen (zie pagina 2) 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.
- Er wordt van alle medewerkers, vrijwilligers, leerlingen, ouders, (geregistreerde) bezoekers en externe relaties verwacht 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 imagooverlies. In het *algemeen reglement van het personeel van het katholiek onderwijs* (artikel 7 § 7) wordt hiernaar verwezen.
- Bij wijzigingen in de infrastructuur, de aanschaf en de uit dienst name van (informatie)systemen, worden bij de bovengenoemde instellingen (zie pagina 2) steeds rekening gehouden met IVP.
- IVP is bij de bovengenoemde instellingen (zie pagina 2) een continu proces, waarbij regelmatig (minimaal trimestrieel) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

3.2 Uitgangspunten privacy

De zes vuistregels met betrekking tot de omgang van persoonsgegevens bij de bovengenoemde instellingen (zie pagina 2) 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 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 rechtmatigheden: toestemming, overeenkomst, wettelijke verplichting, openbaar belang, 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 tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt.
4. **Transparantie:** de school legt aan betrokkenen (leerlingen, hun ouders, vrijwilligers en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IVP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op inzage, verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Opslagbeperking:** data wordt niet langer bewaard dan noodzakelijk. De verwerking wordt door het IVP-beleid beperkt in de tijd.
6. **Data-integriteit:** er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn, en dat zij voldoende beschikbaar zijn om de werking van de bovengenoemde instellingen (zie pagina 2) te waarborgen. Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van **toestemming**, zal bij de bovengenoemde instellingen (zie pagina 2) een eenduidige procedure hanteren die een actieve en aantoonbare handeling vereist.

4 Wet- en regelgeving

De bovengenoemde instellingen (zie pagina 2) voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Algemene Verordening Gegevensbescherming (AVG)
- Camerawet
- Auteurswet

5 Organisatie

De organisatie van IVP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Dit hoofdstuk beschrijft hoe IVP in de bovengenoemde instellingen (zie pagina 2) is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

Voor elk niveau wordt beschreven welke verantwoordelijkheden en taken de verschillende rollen met zich meebrengen.

5.1 Rollen (functies) rondom IVP

Om IVP gestructureerd en gecoördineerd aan te pakken worden bij de bovengenoemde instellingen (zie pagina 2) een aantal rollen aan medewerkers in de bestaande organisatie toegewezen.

5.2 Richtinggevend

Verwerkingsverantwoordelijke

Het schoolbestuur is eindverantwoordelijk voor IVP en stelt het beleid en de basismaatregelen op het gebied van IVP vast.

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

Zie bijlage 1 voor een schematische weergave van de rol- en taakverdelingen aangaande IVP op de bovengenoemde instellingen (zie pagina 2) en binnen VZW Óscar Romeroscholen.

5.3 Sturend

Data Protection Officer (DPO) van de koepelorganisatie

Vanuit de koepelorganisatie Katholiek Onderwijs Vlaanderen wordt er een Data Protection Officer aangesteld. Deze zal binnen het schoolbestuur of instelling het Aanspreekpunt Informatieveiligheid (AIV) aansturen. De taak bestaat uit:

- schoolbesturen informeren en adviseren over hun verplichtingen vanuit de AVG en vanuit andere gegevensbeschermingsbepalingen;
- AIV's opleiden en hulpmiddelen verstrekken zodanig dat ze binnen hun instelling(en) het IVP-beleid kunnen ondersteunen;
- desgevraagd advies verstrekken over de gegevensbeschermingseffectbeoordeling;
- met de toezichthoudende autoriteit samenwerken en optreden als aanspreekpunt voor deze autoriteit.

Aanspreekpunt Informatieveiligheid

Het AIV is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (directie van de instelling, raad van bestuur van het schoolbestuur) en staat de mensen op uitvoerend niveau bij. Het AIV moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele vzw.
- De uniformiteit bewaken binnen de VZW Óscar Romeroscholen
- Meewerken aan de bewustmaking en opleiding van het personeel
- Het aanspreekpunt zijn voor incidenten op het gebied van IVP
- De verdere afhandeling van incidenten binnen de vzw coördineren

Domeinverantwoordelijke / proceseigenaar

Binnen elke instelling zijn er verschillende domeinen/processen, zoals bv. ict, personeel, administratie, facilitaire en financiële zaken, onderwijs et cetera. Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze IVP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

De proceseigenaar is 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 raad van bestuur / de directie stellen zij het beleid voor toegang vast.*
- *Samen met het functioneel beheer en ict zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.*
- *Samen met het functioneel beheer en ict beoordelen zij regelmatig de toegangsrechten van gebruikers.*

Leidinggevendens hebben een voorbeeldrol ten opzichte van hun medewerkers.

5.4 Uitvoerend

Leidinggevende

Naleving van het Informatieveiligheidsbeleid 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 IVP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp IVP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IVP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door het AIV.

Ict-coördinator

De ict-coördinator vormt een technisch aanspreekpunt inzake informatieveiligheid voor het management en de medewerkers, en zorgt in de praktijk voor de implementatie van toegangsrechten en de rapportage aangaande digitale informatieveiligheid.

Functioneel beheerder

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 een verantwoordelijkheid met betrekking tot informatieveiligheid in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het privacyreglement en eraan toegevoegde nota's en visieteksten aangaande IVP op de bovengenoemde instellingen (zie pagina 2). Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists, formulieren en praktische tools.

Medewerkers wordt gevraagd om actief betrokken te zijn bij informatieveiligheid. Dit kan door meldingen te maken van veiligheidsincidenten, het doen van voorstellen ter verbetering van IVP en het uitoefenen van invloed op het beleid (individueel of via de ervoor voorziene overlegorganen en/of via het aanspreekpunt). Zelf hebben zij ook een voorbeeldfunctie naar andere medewerkers, vrijwilligers, ouders, externen en vooral leerlingen toe.

Van ambtswege uit, of eventueel contractueel, worden alle medewerkers (ook extern) van de bovengenoemde instellingen (zie pagina 2) die toegang kunnen hebben tot persoonsgegevens, gebonden aan een discretieplicht. Welbepaalde (externe) medewerkers zijn wettelijk gebonden aan een beroepsgeheim.

6 Controle en rapportage

Dit IVP-beleid en alle bijhorende richtlijnen, nota's en tools, worden minimaal elke twee jaar getoetst en bijgesteld door het schoolbestuur. Hierbij wordt rekening gehouden met:

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

Daarnaast kennen de bovengenoemde instellingen (zie pagina 2) een jaarlijkse planning en controlecyclus voor IVP. Dit is een vast evaluatieproces waarmee de inhoud en effectiviteit van het IVP-beleid wordt getoetst.

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

- **strategisch** niveau (richtinggevend) wordt gesproken over organisatie, alsmede over doelen, bereik en ambitie op het gebied van IVP.
- **tactisch** niveau (sturend) de strategie wordt vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering.
- **operationeel** niveau (uitvoerend) de onderwerpen worden besproken die de dagelijkse uitvoering aangaan. Deze overlevorm wordt niet centraal georganiseerd, en indien nodig in elk organisatieonderdeel van de bovengenoemde instellingen (zie pagina 2) afzonderlijk.

6.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatieveiligheid en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij de bovengenoemde instellingen (zie pagina 2) 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 onder andere de regelmatig terugkerende bewustwordingscampagnes voor iedereen binnen de school. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van het AIV en leidinggevende(n), met de raad van bestuur van VZW Óscar Romeroscholen als eindverantwoordelijke.

6.2 Classificatie en risicoanalyse

Bij de bovengenoemde instellingen (zie pagina 2) heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. De risicoanalyse zal het niveau van de beveiligingsmaatregelen bepalen rekening houdend met de classificatie van de gegevens. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang zijn voor de informatievoorziening.

6.3 Incidenten en datalekken

Bij de bovengenoemde instellingen (zie pagina 2) is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

Alle incidenten kunnen worden gemeld bij de cel informatieveiligheid via het mailadres: privacy@romerocollege.be. De afhandeling van deze incidenten volgt een gestructureerd proces, waarbij men 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 IVP proces. Van belang hierbij is dat leidinggevend en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij de bovengenoemde instellingen (zie pagina 2) wordt actief aandacht besteed aan IVP bij de aanstelling, tijdens functioneringsgesprekken, met een gedragscode, met periodieke bewustwordingscampagnes, et cetera.

Mocht de naleving ernstig tekort schieten, dan kunnen de bovengenoemde instellingen (zie pagina 2) de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden. Voor de bevordering van de naleving van de AVG heeft het AIV een belangrijke rol.

Bijlage 1: Tabel IVP rollen en taken

| Wie Rollen | Hoe Verantwoordelijkheid / taken | Wat Realiseren / vastleggen |
|-----------------------------------|--|--|
| School- of centrumbestuur | <ul style="list-style-type: none"> • Eindverantwoordelijke • IVP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IVP-beleid op basis van rapportages en bijsturen van dit beleid indien nodig • Organisatie IVP inrichten | <ul style="list-style-type: none"> • Informatieveiligheids- en privacy beleid opstellen en goedkeuren en communiceren • Aanspreekpunt informatieveiligheid aanstellen • Oprichten veiligheidscel |
| Leidinggevende (directie) | <ul style="list-style-type: none"> • Toezien op de naleving van het IVP-beleid en privacywetgeving en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Communicatie naar alle betrokkenen; er voor zorgen dat alle medewerkers op de hoogte zijn van het IVP-beleid en de consequenties ervan. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IVP-beleid. • Rapporteren voortgang m.b.t. doelstellingen IVP-beleid aan bestuur • Periodiek het onderwerp informatieveiligheid onder de aandacht brengen in werkoverleg, beoordelingen,... • Implementeren IVP-maatregelen. | <p>Communiceren, informeren en toezien op naleving van o.a.:</p> <ul style="list-style-type: none"> • IVP in het algemeen • Hoe omgaan met leerlingendossiers • Wie mag wat zien • Gedragscode • Beveiliging van ruimtes • Preventieve maatregelen (o.a. brand en waterschade aan servers...) • ... |
| Data protection officer koepel | <ul style="list-style-type: none"> • Schoolbesturen informeren en adviseren over hun verplichtingen krachtens de AVG en regelgeving; • Richtlijnen, kaders, procedures opstellen en aanbevelingen doen m.b.t. informatieveiligheid en privacy • Aanspreekpunten IVP opleiden en hen de nodige tools en hulpmiddelen verstrekken • desgevraagd advies verstrekken over de gegevensbeschermingseffectbeoordeling • samenwerken met de toezichhoudende autoriteit en optreden als aanspreekpunt voor deze autoriteit • Brugfiguur naar de externe partijen toe • Lerend netwerk ontwikkelen en aansturen | <ul style="list-style-type: none"> • Opstellen van algemene processen, richtlijnen en sjablonen IVP • Nascholingstraject organiseren • Overleg met informatieveiligheidsconsulenten onderwijsnetten en GO! • Overleg met externe partijen: leveranciers van leerlingadministratie en -volgsystemen en leveranciers van didactische software • Tools aanpassen/ontwikkelen |

| Wie Rollen | Hoe Verantwoordelijkheid / taken | Wat Realiseren / vastleggen |
|---|---|---|
| Aanspreekpunt informatieveiligheid | <ul style="list-style-type: none"> • Informeert en adviseert directie/bestuur en personeel over IVP • Rapporteert naar directie/bestuur • Informeert de data protection officer van de koepel • Meewerken aan de uitwerking van een specifiek IVP-beleid op basis van het algemeen IVP-beleid • Voorstellen doen tot aanpassingen van centraal aangeboden processen, richtlijnen en procedures om de uitvoering van het IVP-beleid te ondersteunen binnen de school • Meewerken aan: <ul style="list-style-type: none"> ○ classificatie van middelen ○ risicoanalyse ○ het opstellen van een veiligheidsplan • Aanspreekpunt voor IVP-incidenten • Incidentafhandeling (registreren en evalueren). • Invullen register verwerkingsactiviteiten | <p>Voorstellen van aanpassingen aan de uitgewerkte formulieren van processen, richtlijnen en procedures rond IVP, bijvoorbeeld:</p> <ul style="list-style-type: none"> • Security awareness activiteiten • Authenticatie en autorisatie-beleid • Gedragscodes (ICT en internetgebruik, sociale media, privacybeleid...) naar medewerkers en leerlingen toe • Verwerkersovereenkomsten regelen • Toestemming opstellen gebruik foto's en video • Communicatieplan naar medewerkers, leerlingen, ouders en cursisten • Procedure IVP-incident afhandeling • Inrichten meldpunt datalekken • Melden datalekken naar de overheid toe • ... <p>Invullen van register verwerkingsactiviteiten voor schooleigen situatie</p> |
| Informatieveiligheids cel (CIV) van de school of het schoolbestuur ¹ | <ul style="list-style-type: none"> • Classificatie van informatie • IVP risicoanalyse uitvoeren • Prioriteiten voorstellen • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten bekrachtigen door bestuur • De toegangsrechten van gebruikers regelmatig beoordelen en controleren. • Evalueren IVP-beleid en voorstellen van verbetermaatregelen • Bespreking veiligheidsincidenten en voorstellen formuleren voor te nemen maatregelen • Aanpassen gegevensbeschermings-effectbeoordeling aan eigen situatie | <ul style="list-style-type: none"> • Inventariseren waar persoonsgegevens van de school terecht komen (leveranciers lijst) • Classificatie van informatiebronnen en persoonsgegevens • Risicoanalyse uitvoeren en documenteren <p>Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder:</p> <ul style="list-style-type: none"> • Toegangsmatrix diverse informatiesystemen en netwerk |
| Iedereen | <ul style="list-style-type: none"> • Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IVP bij de dagelijkse werkzaamheden | <p>Richtlijnen en procedures volgen</p> <p>Melden incidenten aan aanspreekpunt informatieveiligheid</p> |

¹ bestaande uit domeinverantwoordelijke/ proceseigenaren waaronder: ICT, personeelsdienst, preventieadviseur, financiën, leerlingenadministratie, facilitair management, leidinggevende en het aanspreekpunt informatieveiligheid

Bijlage 2: Aanvullende nota's

Bij dit algemene deel van het IVP-beleid horen nog enkele specifieke nota's :

- Classificatie van persoonsgegevens
- Toegangsmatrices
- Wachtwoordbeleid
- Communicatiebeleid
- Toestelbeleid
- Backupbeleid

Tevens is er een bijkomend document voorzien, dat de nodige achtergrondinformatie bij deze nota's.