INFORMATIEVEILIGHEIDS- EN PRIVACYBELEID

vzw Katholiek Onderwijs Gent-Zuid

Lange Violettestraat 29 9000 Gent

KBOnr. 0409.855.088 RPR Gent T(09)2254744

voor:

Vrije Basisschool Nieuwen Bosch, Tweebruggenstraat 34, Gent

Humaniora Nieuwen Bosch, Lange Violettestraat 65, Gent

Internaat Nieuwen Bosch, Lange Violettestraat 65, Gent

Vrije Basisschool Onze-Lieve-Vrouwcollege, Langestraat 70, Gent

Internaat Onze-Lieve-Vrouw-Presentatie 1, Langestraat 66, Gent

Internaat Onze-Lieve-Vrouw-Presentatie 2, Zuidstraat 3, Gent

Onze-Lieve-Vrouwe-instituut, Tweebruggenstraat 55, Gent

Internaat Onze-Lieve-Vrouw Julie Billiart, Tweebruggenstraat 36, Gent

Vrije Basisschool Crombeen, Tentoonstellingslaan 4, Gent

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-06-26	GELDIG		

Inhoud

1 Inleiding

Informatieverwerking en het gebruik van ict zijn noodzakelijk in de ondersteuning van het onderwijs maar brengen risico's met zich mee.

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.

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 imagoverlies.

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 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 vzw Ka.O.G-Z en haar scholen en internaten.

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 het schoolbestuur, de scholen en de internaten van vzw Ka.O.G-Z (= gerechtvaardigheidsbelang).

- 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 vzw Ka.O.G-Z voldoet aan relevante wet- en regelgeving.

2.2 Reikwijdte

- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen vzw Ka.O.G-Z waaronder in ieder geval: alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties, evenals op andere betrokkenen waarvan vzw Ka.O.G-Z of zijn instellingen persoonsgegevens verwerkt.

- Dit beleid is van toepassing op zowel de digitale als geschreven verwerking van persoonsgegevens.

- Het IVP-beleid geldt voor alle medewerkers, 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 de scholen of onszelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de scholengemeenschap kunnen worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en sociale media. Hiervoor werkt het schoolbestuur met haar scholen en internaten gedragscodes uit.

- Het IVP-beleid binnen vzw Ka.O.G-Z heeft raakvlakken met:
  - Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtpunten: 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 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 vzw Ka.O.G-Z zijn:

- IVP dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de **Algemene Verordening Gegevensbescherming** (AVG) (=GDPR).
  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 vzw Ka.O.G-Z en haar instellingen 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 Ka.O.G-Z, is de **verwerkingsverantwoordelijke** voor alle persoonsgegevens die in opdracht van de scholen en internaten van de vzw verwerkt worden.

- Scholen en internaten van vzw Ka.O.G-Z beheren ook informatie waarvan de intellectuele eigendom (het **auteursrecht**) toebehoort aan derden. Medewerkers en leerlingen/internen van de scholen/internaten 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 geclassificeerd. Deze **classificatie** vormt het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risicoanalyse, 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 school of het internaat of het schoolbestuur zelf sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) en alle leveranciers van digitale bedrijfseconomische middelen (bank, sociaal secretariaat, juridische dienst, …) **verwerkersovereenkomsten** af indien deze persoonsgegevens ontvangen van de school of het internaat of het schoolbestuur zelf.

- Binnen vzw Ka.O.G-Z 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 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 imagoverlies. 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, wordt bij vzw Ka.O.G-Z steeds rekening gehouden met IVP.

- IVP is bij vzw Ka.O.G-Z een continu proces, waarbij regelmatig (minimaal eens om de twee schooljaren) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

3.2 Uitgangspunten privacy

De zes vuistregels met betrekking tot de omgang van persoonsgegevens bij vzw Ka.O.G-Z 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 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 scholen, internaten en schoolbestuur te waarborgen. Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van **toestemming**, zal vzw Ka.O.G-Z een eenduidige procedure hanteren die een actieve en aantoonbare handeling vereist.

4 Wet- en regelgeving

Vzw Ka.O.G-Z 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 vzw Ka.O.G-Z 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 vzw Ka.O.G-Z een aantal rollen aan medewerkers in de scholen, internaten en schoolbestuur toegewezen.

5.2 Richtinggevend

Verwerkingsverantwoordelijke

Het schoolbestuur (de inrichtende macht) is eindverantwoordelijk voor IVP en stelt het beleid en de basis-maatregelen op het gebied van IVP vast.

Zie bijlage 1 voor een schematische weergave van de rol- en taakverdelingen aangaande IVP in het schoolbestuur en de scholen en internaten van vzw Ka.O.G-Z.

5.3 Sturend

Data Protection Officer (DPO) van de koepelorganisatie

Vanuit de koepelorganisatie Katholiek Onderwijs Vlaanderen wordt er een Data Protection Officer aangesteld, die het (de) Aanspreekpunt(en) Informatieveiligheid (AIV) zal 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 (het schoolbestuur; de directie van de school / het internaat) en staat de mensen op uitvoerend niveau bij. Het AIV moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen vzw Ka.O.G-Z
- 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 vzw Ka.O.G-Z coördineren

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-coördinatoren

De ict-coördinatoren van de scholen vormen een technisch aanspreekpunt inzake informatieveiligheid voor het management en de medewerkers, en zorgen in de praktijk voor de implementatie van toegangsrechten en de rapportage aangaande digitale informatieveiligheid.

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 binnen vzw Ka.O.G-Z.

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, externen en vooral leerlingen/internen toe.

Van ambtswege uit, of eventueel contractueel, worden alle medewerkers (ook extern) van vzw Ka.O.G-Z 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 stellen de scholen en internaten een tweejaarlijkse planning en controlecyclus voor IVP op. 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 overlegvormen 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. Dit overleg wordt in elk organisatieonderdeel van vzw Ka.O.G-Z afzonderlijk georganiseerd.

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 scholen en internaten van vzw Ka.O.G-Z 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/het internaat. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van het AIV en leidinggevende(n), met de raad van bestuur van vzw Ka.O.G-Z als eindverantwoordelijke.

6.2 Classificatie en risicoanalyse

Bij vzw Ka.O.G-Z 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 vzw Ka.O.G-Z is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

Alle incidenten kunnen worden gemeld bij privacy@kaogentzuid.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 leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij vzw Ka.O.G-Z 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 kan het schoolbestuur 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**
schoolbestuur vzw Ka.O.G-Z	• 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	• Informatieveiligheids- en privacy beleid opstellen en goedkeuren en communiceren • Aanspreekpunt informatieveiligheid aanstellen • Oprichten veiligheidscel
directeur	• 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 informatiebeveiliging onder de aandacht brengen in werkoverleg, beoordelingen,… • Implementeren IVP-maatregelen.	Communiceren, informeren en toezien op naleving van o.a.: • IVP in het algemeen • Hoe omgaan met leerlingdossiers • Wie mag wat zien • Gedragscode • Beveiliging van ruimtes • Preventieve maatregelen (o.a. brand en waterschade aan servers…) • …
Data protection officer (koepel) Gino De Meester	• 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 toezichthoudende autoriteit en optreden als aanspreekpunt voor deze autoriteit • Brugfiguur naar de externe partijen toe • Lerend netwerk ontwikkelen en aansturen	• 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	• 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 scholengemeenschap.
	• Meewerken aan:
	  ○ classificatie van middelen
	  ○ risicoanalyse
	  ○ het opstellen van een veiligheidsplan
	• Aanspreekpunt voor IVP-incidenten
	• Incidentafhandeling (registreren en evalueren).
	• Invullen register verwerkingsactiviteiten
		Voorstellen van aanpassingen aan de uitgewerkte formulieren van processen, richtlijnen en procedures rond IVP, bijvoorbeeld:
		
		• Security awareness activiteiten
		• Authenticatie en autorisatie-beleid
		• Gedragscodes (ICT en internetgebruik, sociale media, privacybeleid…) naar medewerkers en leerlingen/internen 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
		• …
		Invullen van register verwerkingsactiviteiten voor school/internaat-eigen situatie

Informatieveiligheidscel (CIV) van de school/het internaat (AIV + directie + ICT)	• 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	• Inventariseren waar persoonsgegevens van de school/het internaat terechtkomen (leveranciers lijst) • Classificatie van informatiebronnen en persoonsgegevens • Risicoanalyse uitvoeren en documenteren Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk
Iedereen	• Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IVP bij de dagelijkse werkzaamheden	Richtlijnen en procedures volgen Melden incidenten aan aanspreekpunt informatieveiligheid

Bijlage 2: Aanvullende nota's

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

- Toegangsmatrices
- Wachtwoordbeleid
- Communicatiebeleid
- Toestelbeleid
- Backupbeleid