DONBOSCOHalle
SCHOOL VOOR WETENSCHAP & TECHNOLOGIE
CENTRUM LEREN & WERKEN
STEM / DUAAL

INFORMATIEVEILIGHEIDS- EN PRIVACYBELEID

Don Bosco Onderwijscentrum VZW

voor:

Don Bosco Halle Technisch Instituut / Centrum Leren & Werken

Versie	Datum	Status	Auteur(s)	Opmerking
1.0	2018-09-01	GELDIG		

DONBOSCOHalle
SCHOOL VOOR WETENSCHAP & TECHNOLOGIE
CENTRUM LEREN & WERKEN
STEM / DUAAL

Inhoud

DONBOSCOHalle
SCHOOL VOOR WETENSCHAP & TECHNOLOGIE
CENTRUM LEREN & WERKEN
STEM / DUAAL

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.

Om dit structureel op te pakken is het noodzakelijk dat we duidelijk maken waar het om gaat, een doel stellen en de manier 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.

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 Don Bosco Halle Technisch Instituut / Centrum Leren & Werken.

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 Don Bosco Halle Technisch Instituut / Centrum Leren & Werken.
- Het realiseren van het opvoedingsproject van Don Bosco en in het bijzonder het daaraan gekoppelde zorgbeleid.
- 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 Don Bosco Halle Technisch Instituut / Centrum Leren & Werken voldoet aan relevante wet- en regelgeving.

2.2 Reikwijdte

- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle relevante (intern en extern) betrokkenen van Don Bosco Halle Technisch Instituut / Centrum Leren & Werken.
- Dit beleid is van toepassing op zowel de digitale als analoge 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 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 werkt Don Bosco Halle Technisch Instituut / Centrum Leren & Werken met **gedragscodes**.
- Het IVP-beleid binnen Don Bosco Halle Technisch Instituut / Centrum Leren & Werken heeft impact op verschillende domeinen zoals:
  - algemeen veiligheids- en toegangsbeveiligingsbeleid;
  - personeels- en organisatiebeleid;
  - IT-beleid;
  - participatie van leerlingen, hun ouders/verzorgers en medewerkers;
  - zorgbeleid;
  - …

3 Uitgangspunten

3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij Don Bosco Halle Technisch Instituut / Centrum Leren & Werken 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 Don Bosco Halle Technisch Instituut / Centrum Leren & Werken 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, Don Bosco Onderwijscentrum VZW, is als rechtspersoon de **verwerkingsverantwoordelijke** voor alle persoonsgegevens die in opdracht van en door Don Bosco Halle Technisch Instituut / Centrum Leren & Werken verwerkt worden.

- Don Bosco Halle Technisch Instituut / Centrum Leren & Werken beheert 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 Don Bosco Halle Technisch Instituut / Centrum Leren & Werken geclassificeerd. Deze **classificatie** vormt het uitgangspunt voor de te nemen maatregelen.

- Don Bosco Onderwijscentrum VZW sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) **verwerkersovereenkomsten** af indien deze persoonsgegevens ontvangen van de school.

- Binnen Don Bosco Halle Technisch Instituut / Centrum Leren & Werken 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, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich ‘fatsoenlijk’ gedragen met een eigen verantwoordelijkheid. 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 Don Bosco Halle Technisch Instituut / Centrum Leren & Werken steeds rekening gehouden met IVP.

- IVP is bij Don Bosco Halle Technisch Instituut / Centrum Leren & Werken een continu proces dat regelmatig wordt geëvalueerd en indien nodig aangepast.

3.2 Uitgangspunten privacy

De zes vuistregels met betrekking tot de omgang van persoonsgegevens bij Don Bosco Halle Technisch Instituut / Centrum Leren & Werken 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 Don Bosco Halle Technisch Instituut / Centrum Leren & Werken te waarborgen. Persoonsgegevens worden adequaat beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van **toestemming**, zal Don Bosco Halle Technisch Instituut / Centrum Leren & Werken een eenduidige procedure hanteren die een actieve en aantoonbare handeling vereist.

4 Wet- en regelgeving

Don Bosco Halle Technisch Instituut / Centrum Leren & Werken 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, 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 Don Bosco Halle Technisch Instituut / Centrum Leren & Werken is georganiseerd.

5.1 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 Don Bosco Halle Technisch Instituut / Centrum Leren & Werken en binnen Don Bosco Onderwijscentrum VZW.

5.2 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.

5.3 Aanspreekpunt informatieveiligheid (AIV)

Het AIV geeft terugkoppeling en advies aan de eindverantwoordelijke (schoolbestuur of gemandateerde) en staat de mensen die gegevens verwerken bij. Het AIV moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen Don Bosco Halle Technisch Instituut / Centrum Leren & Werken
- 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 Don Bosco Halle Technisch Instituut / Centrum Leren & Werken coördineren

5.4 Cel informatieveiligheid (CIV)

De Cel Informatie Veiligheid ondersteunt het realiseren van het Informatie Veiligheid en Privacybeleid. Dit gebeurt op twee niveaus:

- overkoepelend op niveau schoolbestuur;
- schoolspecifiek.

De CIV komen op regelmatige basis samen.

5.5 Leidinggevende

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.

5.6 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.

5.7 Medewerker

Elke medewerker heeft een verantwoordelijkheid met betrekking tot informatieveiligheid in de dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in dit document en eraan toegevoegde nota's en visieteksten aangaande IVP op Don Bosco Halle Technisch Instituut / Centrum Leren & Werken. 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 toe.

Van ambtswege uit, of eventueel contractueel, worden alle medewerkers (ook extern) van Don Bosco Halle Technisch Instituut / Centrum Leren & Werken 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 regelmatig getoetst en bijgesteld door het schoolbestuur. De overkoepelende CIV adviseert hierbij het schoolbestuur. Er 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

6.1 Voorlichting en bewustzijn

Beleid en maatregelen alleen 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 Don Bosco Halle Technisch Instituut / Centrum Leren & Werken het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

6.2 Classificatie en risicoanalyse

Bij Don Bosco Halle Technisch Instituut / Centrum Leren & Werken 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 Don Bosco Halle Technisch Instituut / Centrum Leren & Werken is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol. Alle incidenten kunnen worden gemeld bij privacy@donboscohalle.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.

Mocht de naleving ernstig tekort schieten, dan kan Don Bosco Onderwijscentrum VZW 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	• 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
Leidinggevende (directie)	• 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 leerlingendossiers • Wie mag wat zien • Gedragscode • Beveiliging van ruimtes • Preventieve maatregelen (o.a. brand en waterschade aan servers…) • …
Data protection officer koepel	• 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 -volgsysytemen en leveranciers van didactische software • Tools aanpassen/ontwikkelen

Wie **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**

Aanspreekpunt informatieveiligheid schoolbestuur	• 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:
	  ○ classificatie van middelen
	  ○ risicoanalyse
	  ○ het opstellen van een veiligheidsplan
	• Aanspreekpunt voor IVP-incidenten
	• Incidentafhandeling (registreren en evalueren).
		Voorstellen van aanpassingen aan de uitgewerkte formulieren van processen, richtlijnen en procedures rond IVP, bijvoorbeeld:
		
		• Security awareness activiteiten
		• Authenticatie- en autorisatiebeleid
		• 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
		• …

Aanspreekpunt informatieveiligheid school	• Aanspreekpunt voor IVP-incidenten • Incidentafhandeling (registreren en evalueren). • Invullen register verwerkingsactiviteiten	• Security awareness activiteiten • Implementatie authenticatie- en autorisatiebeleid • Verwerkersovereenkomsten regelen • Invullen van register- en verwerkingsactiviteiten voor schooleigen situatie • Inrichten meldpunt datalekken • Melden datalekken naar AIV schoolbestuur toe
Informatieveiligheids cel (CIV) van de school en van het schoolbestuur	• Informeren en ondersteunen van het AIV	• Ieder lid van de CIV ondersteunt het AIV vanuit de eigen specifieke functie • Bespreking en evaluatie van het IVP
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

DONBOSCOHalle
SCHOOL VOOR WETENSCHAP & TECHNOLOGIE
CENTRUM LEREN & WERKEN
STEM / DUAAL

Bijlage 2: Aanvullende nota's

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

- Wachtwoordbeleid
- Communicatiebeleid
- Toestelbeleid
- Backupbeleid