



ZoWe
VERPLEEGKUNDE

INFORMATIEVEILIGHEIDS- EN PRIVACYBELEID

vzw ZoWe verpleegkunde

voor:

opleidingscentrum ZoWe verpleegkunde

campus Brugge, Barrièrestraat 2D, 8200 Brugge

campus Oostende, Frère Orbanstraat 145A, 8400 Oostende

Inhoud

Inhoud	2
Deel 1 Algemeen	4
1.1. Inleiding	4
1.2. Doel en reikwijdte	5
1.3. Uitgangspunten	6
1.4. Organisatie	7
1.5. Controle en rapportage	9
Bijlagen bij deel 1:	11
Bijlage 1: Tabel IVP-rollen en -taken	11
Deel 2 IVP-communicatiebeleid	13
2.1. Inleiding	13
2.2. Gedragscodes	13
2.3. Privacyverklaringen	15
Bijlagen bij deel 2:	18
Bijlage 1: Privacyverklaring voor de student	18
Bijlage 2: Privacyverklaring voor personeelsleden	21
Deel 3 Wachtwoordbeleid	24
3.1. Inleiding	24
3.2. Toegangsbeheer	24
3.3. Wachtwoorden	24
3.4. Gebruik van two-factor authenticatie	25
Deel 4 Toestellenbeleid	26
4.1. Inleiding	26
4.2. Netwerkbeveiliging en -controle	26
4.3. Beveiliging en controle op internetverkeer	27
4.4. Beveiliging en controle op toestellen van het opleidingscentrum	27
4.5. Beveiliging en controle op toestellen van eindgebruikers zelf	28

Deel 5 Backupbeleid	30
5.1. Inleiding	30
5.2. Stroomvoorziening	30
5.3. Internetverbinding	31
5.4. Backups	31
5.5. Brandveiligheid	31
Deel 6 Toegangsmatrices	32
6.1. Inleiding	32
6.2. Toegangsmatrices	33

Deel 1 Algemeen

1.1. Inleiding

Ons opleidingscentrum wil persoonsgegevens verwerken conform de wetgeving rond privacy en informatieveiligheid zoals gestipuleerd in de Algemene Verordening Gegevensbescherming of General Data Protection Regulation van 25 mei 2018. In deze tekst verwoordt ZoWe verpleegkunde hoe zij daar beleidsmatig mee omgaat.

1.1.1 Toelichting informatieveiligheid

Onder informatieveiligheid wordt verstaan: het nemen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de verwerking van persoonsgegevens 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 zij 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 het opleidingscentrum. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schade en imagooverlies.

1.1.2 Toelichting privacy

Privacy gaat over de manier waarop persoonsgegevens beschermd worden conform de huidige wet- en regelgeving. De bescherming van de privacy regelt onder andere de voorwaarden waaronder persoonsgegevens gebruikt mogen worden, maar is ook gelinkt aan de camerawet.

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.

1.1.3 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 ZoWe verpleegkunde.

1.2. Doel en reikwijdte

1.2.1. Doel

Dit beleid heeft als doel:

- Het waarborgen van de continuïteit van de onderwijsorganisatie en de dagdagelijkse werking van ZoWe verpleegkunde.
- Het garanderen van de privacy van studenten, personeelsleden, onderwijspartners en derden waardoor beveiligings- en privacy-incidenten zoveel mogelijk worden voorkomen.
- De kwaliteit van de verwerking van persoonsgegevens te optimaliseren.

1.2.2. Reikwijdte

- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen ZoWe verpleegkunde.
- Dit beleid is van toepassing op zowel de digitale als geschreven verwerking van persoonsgegevens.
- Het IVP-beleid geldt voor alle personeelsleden, studenten, onderwijspartners en derden die binnen een professionele context 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 het opleidingscentrum kan worden aangesproken, zoals uitspraken van medewerkers en studenten in discussies, op (persoonlijke pagina's van) websites en sociale media. Hiervoor werkt ZoWe verpleegkunde met gedragscodes zoals uitgewerkt binnen het communicatiebeleid (zie onderdeel 'IVP-communicatiebeleid').
- Het IVP-beleid binnen ZoWe verpleegkunde heeft raakvlakken met:
 - het personeels- en organisatiebeleid, met als voorbeelden de in- en uitstroom van personeelsleden, functiewisselingen, functiescheiding en vertrouwensfuncties;
 - het IT-beleid, met als voorbeelden de aanschaf, het beheer, het gebruik en/of het uit dienst stellen van hardware, software, services en (digitale) leermiddelen;
 - Het participatiebeleid van studenten en personeelsleden.
 - het algemeen preventie- en welzijnsbeleid en toegangsbeveiligingsbeleid, met als voorbeelden fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen, EHBO-verlening;

1.3. Uitgangspunten

1.3.1. Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij ZoWe verpleegkunde 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 (zie verder) waarbij het uitgangspunt is dat de persoonlijke levenssfeer van alle betrokkenen wordt gerespecteerd.
- Het schoolbestuur, vzw ZoWe verpleegkunde, is als rechtspersoon de **verwerkingsverantwoordelijke** voor alle persoonsgegevens die in opdracht van ZoWe verpleegkunde verwerkt worden.
- De waarde van deze informatie kan door ZoWe verpleegkunde geclassificeerd worden waarbij het beleid een balans maakt tussen de risico's van hetgeen we willen beschermen en de benodigde maatregelen.
- ZoWe verpleegkunde sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) **verwerkersovereenkomsten** af indien deze persoonsgegevens ontvangen van het opleidingscentrum .
- Binnen ZoWe verpleegkunde 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 personeelsleden, studenten, onderwijspartners en derden verwacht dat zij zich verantwoordelijk gedragen.
- Bij wijzigingen in de infrastructuur, de aanschaf en de uit dienst name van (informatie)systemen, wordt bij ZoWe verpleegkunde steeds rekening gehouden met IVP.
- IVP is bij ZoWe verpleegkunde een continu proces, waarbij regelmatig (minimaal tweejaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

1.3.2. Uitgangspunten privacy

De zes vuistregels met betrekking tot het omgaan met persoonsgegevens bij ZoWe verpleegkunde 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:** ZoWe verpleegkunde legt aan alle betrokkenen 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 ZoWe verpleegkunde te waarborgen. Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van **toestemming**, zal ZoWe verpleegkunde een eenduidige procedure hanteren die een actieve en aantoonbare handeling vereist.

1.4. 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 ZoWe verpleegkunde 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.

1.4.1. 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 ZoWe verpleegkunde en binnen het schoolbestuur vzw ZoWe verpleegkunde.

1.4.2. 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 het opleidingscentrum 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 scholen 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 het opleidingscentrum, 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 het hele opleidingscentrum;
- de uniformiteit bewaken binnen ZoWe verpleegkunde;
- 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 ZoWe verpleegkunde coördineren.

1.4.3. 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 personeelgerelateerde 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.

Personeelslid

Alle personeelsleden hebben een verantwoordelijkheid met betrekking tot informatieveiligheid in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in alle IVP-teksten.

Personeelsleden zijn actief betrokken bij informatieveiligheid. Dit gebeurt 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 personeelsleden, externen en vooral studenten toe.

Van ambtswege uit, of eventueel contractueel, worden alle personeelsleden en derden van ZoWe verpleegkunde die toegang kunnen hebben tot persoonsgegevens, gebonden aan een discretieplicht. Welbepaalde (externe) medewerkers zijn wettelijk gebonden aan een beroepsgeheim.

1.5. 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 kent ZoWe verpleegkunde minimaal tweejaarlijks een planning en controlecyclus voor IVP. Dit is een vast evaluatieproces waarmee de inhoud en effectiviteit van het IVP-beleid wordt getoetst.

Het resultaat van deze rapportage en controle wordt best opgenomen in bestaande overlegvormen:

- **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 overlegvorm wordt niet centraal georganiseerd, en indien nodig in elk organisatieonderdeel van ZoWe verpleegkunde afzonderlijk.

1.5.1. 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 ZoWe verpleegkunde 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 het opleidingscentrum. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van het AIV en leidinggevenden, met het schoolbestuur van ZoWe verpleegkunde als eindverantwoordelijke.

1.5.2. Incidenten en datalekken

Bij ZoWe verpleegkunde is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

Alle incidenten kunnen worden gemeld bij privacy@zowe.be. De afhandeling van deze incidenten volgt een gestructureerd proces, waarbij men ook voorziet in de juiste stappen rondom de meldplicht datalekken.

1.5.3. 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 ZoWe verpleegkunde wordt actief aandacht besteed aan IVP bij de inschrijving van studenten, de indiensttreding van personeelsleden, tijdens periodieke bewustwordingscampagnes, enzovoort.

Mocht de naleving ernstig tekort schieten, dan kan ZoWe verpleegkunde 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.

Bijlagen bij deel 1:

Bijlage 1: Tabel IVP-rollen en -taken

Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
School- of centrum-bes tuur	<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 informatiebeveiliging 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 studentendossiers • 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 informatieveiligheidsconsulent en onderwijsnetten en GO! • Overleg met externe partijen: leveranciers van studentenadministratie 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 het opleidingscentrum • 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 studenten toe • Verwerkersovereenkomsten regelen • Toestemming opstellen gebruik foto's en video • Communicatieplan naar medewerkers en studenten • Procedure IVP-incident afhandeling • Inrichten meldpunt datalekken • Melden datalekken naar de overheid toe • ... <p>Invullen van register verwerkingsactiviteiten voor schooleigen situatie</p>
=werkgroep informatieveiligheid en privacybeleid 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 het opleidingscentrum terechtkomen (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, studentenadministratie, facilitair management, leidinggevende en het aanspreekpunt informatieveiligheid

Deel 2 IVP-communicatiebeleid

2.1. Inleiding

De manier waarop alle betrokkenen communiceren maakt ook deel uit van het IVP-beleid. In dit document worden enkele principes vastgelegd inzake interne én externe communicatie, om er samen voor te zorgen dat de privacy, de informatieveiligheid op en het imago van ZoWe verpleegkunde bewaakt wordt.

Deze nota valt onder de eindverantwoordelijkheid van het schoolbestuur ZoWe verpleegkunde.

2.2. Gedragscodes

2.2.1. Gedragscode voor personeelsleden

Discretieplicht

Alle personeelsleden van ZoWe verpleegkunde zijn gebonden aan een discretieplicht, ten aanzien van de persoonsgegevens van andere personeelsleden en van alle studenten, onderwijspartners en derden, conform artikel 23 van het *Algemeen reglement van het personeel van het katholiek onderwijs*.

Dit betekent dat personeelsleden van ambtswege uit, geen persoonsinformatie mogen vermelden of publiceren, buiten de daarvoor voorziene kanalen binnen ZoWe verpleegkunde. Onderling informatie delen is enkel toegestaan via de hieronder vastgelegde kanalen en procedures, en steeds als dit in het belang is van de student of een collega in kwestie.

Personeelsleden worden van ambtswege uit geacht om de geldende IVP-procedures en IVP-afspraken steeds te volgen, teneinde het accidenteel verspreiden van persoonsgegevens te vermijden.

Als men vermoedt dat, door toedoen van uzelf of van anderen, er mogelijks persoonsgegevens buiten de context van deze discretieplicht verspreid werden, dan dient men het aanspreekpunt informatieveiligheid en/of het meldpunt datalekken hierover te contacteren. Voor ZoWe verpleegkunde is het meldpunt datalekken: privacy@zowe.be.

E-mail- en berichtenbeleid

Voor alle personeelsleden gelden de gedragscodes conform bijlage 3, punt 3.5 van het *Algemeen model van arbeidsreglement, opgesteld door Katholiek Onderwijs Vlaanderen*. Daarnaast leggen we richtlijnen vast inzake het doel, het gebruik en de beveiliging van de accounts. We maken een onderscheid tussen:

- (Algemeen-) Functionele mailaccounts van het opleidingscentrum
Het e-mailbeheer van functionele schoolaccounts van het type info@zowe.be, ICT@zowe.be, communicatie@zowe.be, ... is toegewezen aan één of meerdere personeelsleden. Deze adressen worden vrij verspreid en gepubliceerd.
- Privémailadressen
Privéaccounts van het type voornaam.familienaam@hotmail.com, voornaam.familienaam@gmail.com, ... worden niet gebruikt voor schoolgerelateerde communicatie met collega's, studenten, oud-studenten of externen.

Let op bij het gebruik van prive-accounts op toestellen waarop zich ook persoonsgegevens van ZoWe verpleegkunde bevinden: dit kan risico's inhouden (virussen, ransomware, ...).

- **Individuele schoolaccounts**

Deze accounts van het type voornaam.familienaam@zowe.be worden toegewezen aan individuele personeelsleden voor professioneel gebruik. Het gebruik is dus verbonden met de taken die voortvloeien uit de functie. Deze adressen kunnen verspreid en gepubliceerd worden.

Gebruik deze accounts voor schoolgerelateerde externe communicatie met derden (b.v. stageplaatsen, de scholengemeenschap, ...). Communicatie met collega's en studenten kan best gebeuren via het intern berichtensysteem (*Smartschool*).

- **Berichtensystemen**

Personeelsleden die gebruik maken van een berichtensysteem via communicatie-apps zorgen voor een maximale beveiliging (zie toestelbeleid).

Het interne berichtensysteem (*Smartschool*) is een gesloten communicatieplatform waarin wel persoonsgegevens gecommuniceerd kunnen worden.

Via externe berichtensystemen (*instant messaging, video conferencing, ...*) worden geen persoonsgegevens gecommuniceerd.

Social media-protocol

Sociale media bieden een mogelijkheid om te laten zien dat men trots is op het opleidingscentrum en kunnen een bijdrage leveren aan een positief imago van het opleidingscentrum. Personeelsleden houden zich eraan om de goede naam van het opleidingscentrum via sociale media niet te schaden en er verantwoord mee om te gaan, volgens de reguliere fatsoensnormen en in het verlengde van de missie en visie van het opleidingscentrum.

Docenten kunnen verantwoord gebruik maken van sociale media in de lespraktijk zolang dit past binnen een pedagogisch-didactische context.

Personeelsleden kunnen informatie en kennis delen, zolang deze niet vertrouwelijk of schadelijk is ten aanzien van anderen en zijn zelf verantwoordelijk voor de gepubliceerde inhoud.

Personeelsleden zijn er zich van bewust dat gepubliceerde informatie voor onbepaalde tijd openbaar blijft, ook na verwijdering van het bericht; en dat het publiceren van foto-, film- of geluidsopnames van schoolgerelateerde situaties op sociale media afhankelijk is van uitdrukkelijk toestemming.

2.2.2. Gedragscode voor studenten

Leefregels

Zie onderwijs- en evaluatiereglement / ICT-protocol

E-mail- en berichtenbeleid

Studenten die gebruik maken van berichtensystemen via communicatie-apps (het schoolcommunicatieplatform, *instant messaging* via telefonie of *online, video conferencing, enz.*), doen dit conform de afspraken van het onderwijsreglement.

Social media-protocol

Studenten die gebruik maken van sociale media, gebruiken deze kanalen conform de afspraken van het onderwijsreglement.

2.2.3. Gedragscode voor derden

Discretieplicht

Derden die via hun dienst, levering of werk persoonsgegevens verwerken van personeelsleden, studenten of onderwijspartners sluiten een verwerkersovereenkomst af met het opleidingscentrum .

Social media-protocol

Derden mogen binnen de schoolinfrastructuur geen foto-, film- of geluidsopnames maken van opleidingsgerelateerde situaties zonder uitdrukkelijke toestemming van het opleidingscentrum. Het is niet toegelaten sociale media in het opleidingscentrum te gebruiken die een goed en veilig opleidingsklimaat in het gedrang brengen.

2.3. Privacyverklaringen

2.3.1. Privacyverklaring voor personeelsleden

Zie bijlage 2

De wettelijke grondslag

Personeelsgegevens worden verwerkt door ZoWe verpleegkunde / het schoolbestuur van ZoWe verpleegkunde volgens regels vastgelegd in de *Algemene Verordening Gegevensbescherming* (AVG). Deze regelgeving beschermt personeelsleden bij de verwerking van gegevens, *in concreto* door de toepassing ervan door de personeelsadministratie van het opleidingscentrum of het schoolbestuur van het opleidingscentrum, en door passende beveiligingsmaatregelen tegen ongeoorloofde verwerkingen.

Uw persoonsgegevens

De personeelsadministratie van het schoolbestuur vzw ZoWe verpleegkunde houdt zich eraan de persoonsgegevens op een bewuste, discrete, veilige en verantwoorde manier te verwerken. Het schoolbestuur vzw ZoWe verpleegkunde houdt een register bij van de manier waarop de persoonsgegevens verwerkt worden. Dit register brengt in kaart van wie en welke persoonsgegevens verwerkt worden, waarom dit gebeurt, door wie ze worden gedeeld, en voor welke termijn ze bewaard worden.

Recht op toegang

Personeelsleden kunnen persoonsgegevens die voor hem/haar van toepassing zijn in een gestructureerde elektronische vorm verkrijgen via de personeelsadministratie.

Recht op correctie en uitwissing

Personeelsleden kunnen de personeelsadministratie contacteren en hebben het recht op correctie als gegevens niet meer juist zijn, of uitwissing in het geval van toestemming. Personeelsleden hebben tevens meldingsplicht als administratieve gegevens gewijzigd moeten worden.

Datalek

Als personeelsleden vermoeden dat persoonsgegevens buiten de context van deze discretieplicht verspreid werden, dan dient men het aanspreekpunt informatieveiligheid en/of het meldpunt datalekken hierover te contacteren. Voor ZoWe verpleegkunde is het meldpunt datalekken: privacy@zowe.be.

2.3.2. Privacy-verklaring voor studenten

Zie bijlage 1

De wettelijke grondslag

Studentengegevens worden verwerkt door ZoWe verpleegkunde volgens regels vastgelegd in de *Algemene Verordening Gegevensbescherming (AVG)*. Deze regelgeving beschermt studenten bij de verwerking van hun gegevens, *in concreto* door de toepassing ervan door de studentenadministratie van het opleidingscentrum en door passende beveiligingsmaatregelen tegen ongeoorloofde verwerkingen.

Uw persoonsgegevens

De studentenadministratie van het opleidingscentrum houdt zich eraan persoonsgegevens op een bewuste, discrete, veilige en verantwoorde manier te verwerken. ZoWe verpleegkunde houdt een register bij van de manier waarop de persoonsgegevens verwerkt worden. Dit register brengt in kaart van wie en welke persoonsgegevens verwerkt worden, waarom dit gebeurt en door wie ze worden gedeeld, en hoe lang ze bewaard worden.

Recht op toegang

Studenten kunnen persoonsgegevens die voor hem/haar van toepassing zijn in een gestructureerde elektronische vorm verkrijgen.

Recht op correctie en uitwissing

Studenten kunnen de studentenadministratie contacteren en hebben het recht op correctie als gegevens niet meer juist zijn, of uitwissing in het geval van toestemming. Studenten hebben ook de plicht om relevante wijzigingen te melden aan de studentenadministratie.

2.3.3. Privacy-verklaring voor derden

De wettelijke grondslag

Gegevens van derden worden verwerkt door ZoWe verpleegkunde volgens regels vastgelegd in de *Algemene Verordening Gegevensbescherming (AVG)*. Deze regelgeving beschermt derden bij de verwerking van hun gegevens, *in concreto* door de toepassing ervan door de administratieve diensten en door passende beveiligingsmaatregelen tegen ongeoorloofde verwerkingen.

Uw persoonsgegevens

De administratie houdt zich eraan persoonsgegevens op een bewuste, discrete, veilige en verantwoorde manier te verwerken. ZoWe verpleegkunde houdt een register bij van de manier waarop de persoonsgegevens verwerkt worden. Het register brengt in kaart van wie en welke persoonsgegevens verwerkt worden, waarom dit gebeurt en door wie ze worden gedeeld, en hoe lang ze bewaard worden.

Recht op toegang

Derden kunnen persoonsgegevens die voor hem/haar van toepassing zijn in een gestructureerde elektronische vorm verkrijgen.

Recht op correctie en uitwissing

Derden kunnen de administratie contacteren en hebben het recht op correctie als gegevens niet meer juist zijn, of uitwissing in het geval van toestemming.

Bijlagen bij deel 2:

Bijlage 1: Privacyverklaring voor de student

Privacyverklaring (student) – ZoWe verpleegkunde

Wegens de wetgeving inzake informatieveiligheid en privacy, willen wij jou informeren over de verwerkingen die wij met jouw persoonsgegevens uitvoeren, en de beleidsmaatregelen die wij nemen om deze te beschermen.

1 Verantwoordelijken

Het schoolbestuur, vzw ZoWe verpleegkunde (104141), is de verwerkingsverantwoordelijke voor alle studentengegevens. Op ZoWe verpleegkunde is er een aanspreekpunt informatieveiligheid aangeduid, dat gemakkelijk te contacteren is via privacy@zowe.be. Het aanspreekpunt informatieveiligheid en/of de directie van ZoWe verpleegkunde kan voor advies en ondersteuning terecht bij de 'data protection officer' (DPO) van de onderwijskoepel Katholiek Onderwijs Vlaanderen.

2 Verwerkingen

2.1 Verwerkingsdoeleinden

Op ZoWe verpleegkunde verwerken wij studentengegevens omwille van de volgende doelen:

- studentenadministratie;
- stageplanning
- studentenbegeleiding;
- studentenevaluatie;
- public relations;
- studentenrekrutering;
- toezicht op telecommunicatie;
- camerabewaking.

2.2 Verwerkte studentengegevens

Om jou in te schrijven, te begeleiden en op te volgen in ZoWe verpleegkunde is het noodzakelijk dat wij de volgende gegevens verwerken:

- identificatiegegevens (met in het bijzonder *voornaam en naam, roepnaam, een pasfoto, het rijksregisternummer, gezinssamenstelling, voorrang- en indicatorfactoren*);
- persoonlijke kenmerken (nl: *geboortedatum, geboorteplaats, geslacht, nationaliteit*);
- privé contactgegevens (met in het bijzonder *telefoonnummer(s), adresgegevens, e-mail*);
- evaluatiegegevens (met in het bijzonder *remediëring, competentielijsten, rapporten ...*);
- gezondheidsgegevens: *lichamelijk, psychisch, risicosituaties en -gedragingen (met het oog op begeleiding)*;
- opleiding en vorming (met in het bijzonder *vorige scholen, gevolgde richtingen, attesten, deliberatiebeslissingen, -motivaties en -verslagen, getuigschriften en diploma's*);
- aanwezigheid en discipline (met in het bijzonder *afwezigheidsbewijzen, sancties, tucht*);
- afbeeldingen (*die niet administratief gebruikt worden*);
- bewakingsbeelden.

Deze gegevens kunnen, mits wettelijke grondslag, eventueel bekomen worden van de vorige school waar de student ingeschreven was.

2.3 Ontvangers

- Het departement onderwijs is, via het *Discimus*-systeem van AgODi, een ontvanger van een deel van jouw studentengegevens;
- de scholengemeenschap Sint-Donaas Brugge ontvangt jouw administratieve gegevens omwille van hun bevoegdheden om onderwijssubsidies en -werkingsmiddelen te beheren;
- het CLB is, indien het jou begeleidt, bevoegd om alle in § 2.2 opgesomde gegevens op te vragen;
- het ondersteuningsnetwerk is, indien van toepassing, bevoegd om een deel van de in § 2.2 opgesomde gegevens op te vragen;
- iedereen die deel uitmaakt van het multidisciplinair team dat jou begeleidt, is bevoegd om alle in § 2.2 opgesomde gegevens op te vragen;
- bij verificatie krijgt de onderwijsverificateur toegang tot administratieve gegevens, aanwezigheden, afwezigheidsbewijzen, ... in het kader van zijn wettelijk bepaalde taak;
- bij inspectie is het mogelijk dat een onderwijsinspecteur ook toegang vraagt tot bepaalde studentengegevens in het kader van zijn wettelijk bepaalde taak.

2.4 Verwerkers

Op ZoWe verpleegkunde worden onderstaande platformen gebruikt bij de verwerking van studentengegevens:

- Informat
- portaal
- Smartschool
- Count-e
- Papercut (Ricoh)

2.5 Voorwaarden

Jouw gegevens zullen verwerkt worden zolang je bij ons ingeschreven bent, of zolang ze nodig zijn om je te begeleiden. Daarna worden ze verwijderd, geanonimiseerd of gearchiveerd conform de geldende regelgevingen.

Indien we bepaalde gegevens langer zouden willen bewaren, dan zullen we dat melden en de expliciete toestemming ervoor vragen.

Meer informatie over de beleidsmatige aanpak inzake privacy en informatieveiligheid op ZoWe verpleegkunde kan je raadplegen op www.zowe.be of opvragen via: privacy@zowe.be

3 Rechten inzake privacy

3.1 Rechten uitoefenen

Je kan je steeds op onderstaande rechten beroepen:

- recht op informatie: je mag vragen welke gegevens van jou er verwerkt worden en wie er toegang toe heeft (zie ook verwijzing in § 2.6), waarom het opleidingscentrum die persoonsgegevens nodig heeft of gebruikt en hoe lang ze bewaard worden;
- recht op inzage: je mag steeds de gegevens die het opleidingscentrum van jou heeft, inkijken a.d.h.v. een kopie;
- recht op verbetering: als je fouten in jouw gegevens vindt, mag je vragen om dit aan te passen. Je kan ook aanvullingen toevoegen aan jouw gegevens;
- recht op gegevenswissing: je kan vragen dat gegevens, die niet (meer) strikt noodzakelijk zijn voor het opleidingscentrum, permanent en volledig verwijderd worden;
- recht op beperking van de verwerking: als je bezwaar hebt (zie verder) tegen de verwerking van bepaalde gegevens, kan je vragen om deze verwerking te stoppen;
- recht op overdraagbaarheid van gegevens: als je bepaalde gegevens wenst over te dragen naar een nieuwe school of andere werkgever, dan faciliteert het opleidingscentrum dit (in de mate van het mogelijke);
- recht van bezwaar: als je niet akkoord gaat met de grondslag van een verwerking of met de manier waarop bepaalde gegevens van jou verwerkt worden, kan je je hiertegen verzetten;
- recht om niet te worden onderworpen aan geautomatiseerde besluitvorming: wanneer het opleidingscentrum algoritmes gebruikt om, zonder tussenkomst van mensen, bepaalde gevolgen te trekken uit (een deel van) jouw gegevens (zie § 3.3), dan kan je je hiertegen verzetten;
- recht om intrekken van toestemming: als men jou voor bepaalde verwerkingen de toestemming gevraagd heeft, kan je ten allen tijde kiezen om deze niet meer te verstrekken.

Voor meer uitleg over of om je op een van deze rechten te beroepen, gelieve je intern te richten tot privacy@zowe.be. Bij eventuele disputen of twijfel, kan je je ook wenden tot de toezichthoudende autoriteit inzake privacy en de verwerking van persoonsgegevens: <https://www.gegevensbeschermingsautoriteit.be>

3.2 Gerechtvaardigd belang

Een aantal verwerkingen hebben een 'gerechtvaardigd belang' als grondslag:

- toezicht op telecommunicatie;
- de in § 2.4 vermelde doorgifte van jouw gegevens aan onderwijsinspectie.

3.3 Geautomatiseerde besluitvorming

Op ZoWe verpleegkunde worden studenten niet onderworpen aan eender welke vorm van geautomatiseerde besluitvorming.

3.4 Al dan niet verstrekken van gegevens

De in § 2.2 en § 2.3 vermelde gegevens moeten, indien van toepassing, verstrekt worden om de inschrijving op ZoWe verpleegkunde te kunnen afronden. Met uitzondering van die gegevens waar expliciet toestemming voor nodig is.

Bijlage 2: Privacyverklaring voor personeelsleden

Privacyverklaring (personeel) – ZoWe verpleegkunde

Wegens de wetgeving inzake informatieveiligheid en privacy, willen wij je informeren over de verwerkingen die wij met jouw persoonsgegevens uitvoeren, en de beleidsmaatregelen die wij nemen om deze te beschermen.

1 Verantwoordelijken

Het schoolbestuur, vzw ZoWe verpleegkunde (104141), is de verwerkingsverantwoordelijke voor alle personeelsgegevens. Op ZoWe verpleegkunde is er een aanspreekpunt informatieveiligheid aangeduid, dat gemakkelijk te contacteren is via privacy@zowe.be. Het aanspreekpunt informatieveiligheid en/of de directie van ZoWe verpleegkunde kan voor advies en ondersteuning terecht bij de 'data protection officer' (DPO) van de onderwijskoepel Katholiek Onderwijs Vlaanderen.

2 Verwerkingen

2.1 Verwerkingsdoeleinden

Op ZoWe verpleegkunde verwerken wij personeelsgegevens omwille van de volgende doelen:

- personeelsadministratie;
- personeelsbeheer (o.m. evaluatie);
- loonadministratie;
- public relations;
- personeelsrekrutering;
- toezicht op telecommunicatie;
- camerabewaking.

2.2 Verwerkte personeelsgegevens

Om je te werk te stellen, te begeleiden en op te volgen in ZoWe verpleegkunde is het noodzakelijk dat wij de volgende gegevens verwerken:

- identificatiegegevens (*met in het bijzonder een pasfoto, het rijksregisternummer, gezinssamenstelling*);
- persoonlijke kenmerken (*met in het bijzonder geboortedatum, geboorteplaats, geslacht, nationaliteit*);
- privé contactgegevens (*met in het bijzonder telefoonnummer(s), adresgegevens, email*);
- loongegevens (*met in het bijzonder werkstation, opdracht(en), barema, salaris*);
- loopbaangegevens (*met in het bijzonder uittreksel strafregister, getuigschriften, diploma's en bekwaamheidsbewijzen, voorgaande werkgevers (in het onderwijs), dienstanciënniteit, TADD, statutaire benoeming, verlofstelsels*);
- loopbaanbegeleiding (*met in het bijzonder lesobservaties, functionerings- en evaluatiegesprekken, gevolgde bijscholingen, verslagen pedagogische begeleiding*);
- aanwezigheid en discipline (*met in het bijzonder afwezigheidsbewijzen, berispingen, blamen, tucht*);
- afbeeldingen (*die niet administratief gebruikt worden*);
- bewakingsbeelden.

2.3 Ontvangers

- Het departement onderwijs is, via het werkstation bij AgoDi, een ontvanger van een deel van jouw personeelsgegevens;
- De scholengemeenschap Sint-Donaas ontvangt jouw loopbaan- en loongegevens omwille van hun bevoegdheden inzake TADD, statutaire benoemingen, mutaties en reffectaties.
- bij verificatie krijgt de onderwijsverificateur mogelijk toegang tot bepaalde loopbaan- en loongegevens;
- bij inspectie is het mogelijk dat een onderwijsinspecteur ook toegang vraagt tot bepaalde personeelsgegevens.

2.4 Verwerkers

Op ZoWe verpleegkunde worden onderstaande platformen gebruikt bij de verwerking van personeelsgegevens:

- informat
- Smartschool
- portaal
- Count-e
- Papercut (Ricoh)

2.5 Voorwaarden

Jouw gegevens zullen verwerkt worden zolang je bij ons te werk gesteld bent. Daarna worden ze verwijderd, geanonimiseerd of gearchiveerd conform de geldende regelgevingen.

Indien we bepaalde gegevens langer zouden willen bewaren, dan zullen we je dat melden en jouw expliciete toestemming ervoor vragen.

Meer informatie over de beleidsmatige aanpak inzake privacy en informatieveiligheid op ZoWe verpleegkunde kan je raadplegen op www.zowe.be of opvragen via:

privacy@zowe.be

3 Rechten inzake privacy

3.1 Rechten uitoefenen

Je kan je steeds op onderstaande rechten beroepen:

- recht op informatie: je mag vragen welke gegevens van jou er verwerkt worden en wie er toegang toe heeft (zie ook verwijzing in § 2.5), waarom het opleidingscentrum die persoonsgegevens nodig heeft of gebruikt en hoe lang ze bewaard worden;
- recht op inzage: je mag steeds de gegevens die het opleidingscentrum van jou heeft, inkijken a.d.h.v. een kopie;
- recht op verbetering: als je fouten in jouw gegevens vindt, mag je vragen om dit aan te passen. Je kan ook aanvullingen toevoegen aan jouw gegevens;
- recht op gegevenswissing: je kan vragen dat gegevens, die niet (meer) strikt noodzakelijk zijn voor het opleidingscentrum, permanent en volledig verwijderd worden;
- recht op beperking van de verwerking: als je bezwaar hebt (zie verder) tegen de verwerking van bepaalde gegevens, kan je vragen om deze verwerking te stoppen;
- recht op overdraagbaarheid van gegevens: als je bepaalde gegevens wenst over te dragen naar een nieuwe school of andere werkgever, dan faciliteert het opleidingscentrum dit (in de mate van het mogelijke);
- recht van bezwaar: als je niet akkoord gaat met de grondslag van een verwerking of met de manier waarop bepaalde gegevens van jou verwerkt worden, kan je zich hiertegen verzetten;

- recht om niet te worden onderworpen aan geautomatiseerde besluitvorming: wanneer het opleidingscentrum algoritmes gebruikt om, zonder tussenkomst van mensen, bepaalde gevolgen te trekken uit (een deel van) jouw gegevens (zie § 3.3), dan kan je je hiertegen verzetten;
- recht om zijn/haar toestemming in te trekken: indien men je voor bepaalde verwerkingen de toestemming gevraagd heeft, kan je ten allen tijde kiezen om deze niet meer te verstrekken.

Voor meer uitleg over of om je op een van deze rechten te beroepen, gelieve je intern te richten tot privacy@zowe.be. Bij eventuele disputen of twijfel, kan je je ook wenden tot de toezichthoudende autoriteit inzake privacy en de verwerking van persoonsgegevens: <https://www.gegevensbeschermingsautoriteit.be>

3.2 Gerechtvaardigd belang

Een aantal verwerkingen hebben een 'gerechtvaardigd belang' als grondslag, namelijk:

- toezicht op telecommunicatie;
- de in § 2.3 vermelde doorgifte van jouw gegevens aan onderwijsinspectie.

3.3 Geautomatiseerde besluitvorming

Op ZoWe verpleegkunde worden personeelsleden niet onderworpen aan eender welke vorm van geautomatiseerde besluitvorming.

3.4 Al dan niet verstrekken van gegevens

De in § 2.2 vermelde gegevens moeten, indien van toepassing, verstrekt worden om het arbeidscontract op ZoWe verpleegkunde te kunnen aangaan. Met uitzondering van:

- afbeeldingen (voor public relations).

Deel 3 Wachtwoordbeleid

3.1. Inleiding

Een goed beveiligingsbeleid dient zich aan omdat steeds meer privacygevoelige gegevens gedigitaliseerd worden, vanuit verschillende locaties toegankelijk zijn en online worden gedeeld. Een wachtwoordbeleid en extra beveiliging om toegang te hebben tot jouw toestel voorkomt identiteitsdiefstal, *phishing* en *hacking*. Als uitgangspunt stellen we dat elke gebruiker toegang heeft tot alle informatie die ze nodig hebben om hun taak naar behoren uit te oefenen, maar hen ook alle toegang ontzegt tot informatie die een gebruiker niet nodig heeft.

Deze nota valt onder de eindverantwoordelijkheid van het schoolbestuur vzw ZoWe verpleegkunde.

3.2. Toegangsbeheer

De directeur van het opleidingscentrum is verantwoordelijk voor het gebruikersbeheer van de organisatie. Gebruikersbeheer houdt het aanmaken van gebruikers, toekennen van rechten en stopzetten van rechten in.

Het opleidingscentrum houdt een toegangsmatrixprocedure bij die een inventaris bevat van alle rollen en rechten gekoppeld aan personeelsleden en studenten in het opleidingscentrum. Aan de hand van dit overzicht kan men een beveiligingsbeleid verder uitwerken rond volgende pijlers:

3.2.1. Authenticatie

Authenticatie is het proces waarbij je je identiteit gaat bewijzen (ben je wel diegene die je beweert te zijn). Het opleidingscentrum sensibiliseert en maakt afspraken om het inlogproces en

-procedures en dus de toegang tot gevoelige data optimaal te beveiligen.

- Betrokkenen wordt informatie aangereikt hoe ze wachtwoorden veilig aanmaken en correct gebruiken.
- Het opleidingscentrum bepaalt waar een dubbele authenticatiemethode van toepassing is.

3.2.2. Autorisatie

Autorisatie is een proces waarbij onderzocht wordt of je voldoende rechten hebt of toestemming hebt voor hetgeen je wilt doen.

3.2.3. Auditing (controleerbaarheid)

Auditing (controleerbaarheid) is het proces waarmee je kan nagaan wie wat waar, wanneer en waarmee doet.

3.3. Wachtwoorden

Wachtwoorden zorgen er mee voor dat de toegang tot applicaties goed beveiligd is. Het is dus van belang om een sterk beleid op te zetten om het inlogproces en -procedures te beheren. Op ZoWe verpleegkunde werken we er continu aan om personeel en studenten het belang van sterke wachtwoorden bij te brengen.

Een wachtwoordbeleid heeft als doel enkele bepalingen op te leggen rond het correct gebruik van wachtwoorden om de toegang tot gevoelige data (waaronder privacy gevoelige persoonsgegevens) te beveiligen middels een wachtwoord.

3.3.1. Wachtwoordbepalingen

- Hoe langer een wachtwoord hoe beter. Het wachtwoord moet minstens 8 karakters hebben. Beter nog is om te werken met een wachtwoordzin (bijvoorbeeld: IkGaSinds2015NaarDeSchool)
- Mix hoofdletters, kleine letters en tekens door elkaar: gebruik volgende tekens in het wachtwoord:
 - Hoofdletters
 - Kleine letters
 - Cijfers
 - Niet-alfanumerieke karakters
- Verander minstens 1 per schooljaar je wachtwoord
- Gebruik verschillende wachtwoorden voor verschillende applicaties
- Geef het wachtwoord niet door, op geen enkele wijze aan niemand.
- Schrijf het wachtwoord niet op: niet op papier, niet elektronisch in jouw GSM of PC.
- Verzend nooit een wachtwoord via email of een ander communicatiesysteem. (Niemand van ZoWe verpleegkunde zal ooit je wachtwoord, om eender welke reden, op deze manier opvragen.)
- Gebruik andere wachtwoorden dan privé-wachtwoorden.
- Bewaar je wachtwoord niet in de browser.

3.3.2. Wachtwoordbeheer

- Na 3 pogingen om in te loggen in een digitaal schoolplatform wordt het account vergrendeld.
- Laat de computer nooit onbeheerd achter maar vergrendel het scherm of log uit.
- Na maximum 30 minuten inactiviteit valt de computer automatisch in slaapmodus en wordt het scherm vergrendeld.

3.3.3. Wat doen bij vermoeden van misbruik?

Misbruik kan ontvreemding of onrechtmatig gebruik van een wachtwoord zijn.

- Verander het wachtwoord onmiddellijk
- Neem direct contact op met het aanspreekpunt informatieveiligheid, de dienst ICT en/of de systeembeheerder. Meldpunt datalekken: privacy@zowe.be

Deze personen gaan na of er sprake is van een misbruik en proberen zo nodig de schade te herstellen.

3.4. Gebruik van two-factor authenticatie

Als je echt met veel privacygevoelige persoonsgegevens werkt, is vaak een combinatie van gebruikersnaam en wachtwoord niet voldoende veilig. Daarom bestaan er two-factor authenticatiemethodes.

Deze systemen zijn veel veiliger en worden binnen ZoWe verpleegkunde dan ook toegepast voor iedereen die aan de meest privacygevoelige gegevens binnen het opleidingscentrum kan.

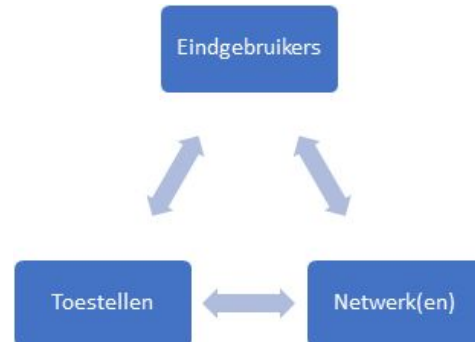
Deel 4 Toestellenbeleid

4.1. Inleiding

4.1.1 Algemeen

In een eenvoudige interpretatie zijn er drie aspecten van een modern ICT-netwerk om rekening mee te houden inzake beschikbaarheid, integriteit en vertrouwelijkheid:

- **(Eind)gebruikers** = *personen*
- **Toestellen** = *desktops, laptops, maar ook tablets, smart-phones, ... en ook: servers*
- **Netwerk(en)** = *de verbinding(en) tussen de toestellen onderling en toestellen en gebruikers.*



Deze beleidsnota omschrijft de manier waarop ZoWe verpleegkunde elk van deze drie aspecten in het IVP-beleid enerzijds maximaliseert en anderzijds controle op elk van deze aspecten uitvoert.

Deze nota valt onder de eindverantwoordelijkheid van het schoolbestuur vzw ZoWe verpleegkunde.

4.1.2 Algemene bepalingen

Ongeacht het "type" toestel of netwerk, kan ZoWe verpleegkunde een aantal maatregelen nemen om:

- te herkennen wanneer het "gewone" verkeer gemonitord, onderschept, nagebootst of gewijzigd wordt.
- het geheel te monitoren of via logboeken handelingen bij te houden voor analyse of eventueel naar bewijslast toe.
- in deze logboeken een aantal **identificatieparameters** te registreren. Er vinden geen ongeoorloofde inzages of systematische analyses plaats op deze gegevens. Enkel bij gegronde vermoedens van inbreuken kunnen hierop gerichte en/of willekeurige controles uitgevoerd worden. Alle informatie hier aangaande wordt strikt vertrouwelijk behandeld.

4.2. Netwerkbeveiliging en -controle

4.2.1. Bekabeld netwerk en servers

Met het "bekabelde netwerk" bedoelen we het geheel van componenten die de netwerkverbindingen maken en beheren, zoals: routers, switchen, hubs, kabels, servers, modems, ...

De algemene maatregelen (zie hierboven) worden toegepast.

Wachtwoorden op de netwerkcomponenten worden systematisch gewijzigd t.o.v. de "default" waarden, of te gemakkelijke combinaties. De gekozen wachtwoorden voldoen aan alle afspraken uit het **wachtwoordbeleid**.

4.2.2. Wifi-netwerk

Voor personeel, studenten en gasten is wifi voorzien op ZoWe verpleegkunde.

De algemene maatregelen (zie hierboven) worden toegepast.

Het netwerkverkeer dat via het draadloze netwerk verloopt, wordt *niet* versleuteld. Het raadplegen, bewerken enz. van persoonsgegevens wordt dan ook ten stelligste afgeraden, tenzij er een andere vorm van versleuteling gehanteerd wordt (bv. *https i.p.v. http*).

4.3. Beveiliging en controle op internetverkeer

Op ZoWe verpleegkunde is er, zowel voor de toestellen die eigendom zijn van het opleidingscentrum als op bepaalde andere toestellen, een internetverbinding mogelijk. Als organisatie is ZoWe verpleegkunde verantwoordelijk voor het algehele dataverbruik, en voor alles dat er met / via deze internetverbinding gebeurt. Daarom hanteert men ook hier een aantal regels en controles daarop.

De algemene maatregelen (zie hierboven) worden toegepast.

De beheerders, noch de elektronische controlesystemen en de logboeken, hebben op geen enkele manier toegang tot de inhoud van persoonlijke berichten (zoals messaging, email, intern communicatiesysteem, ...).

4.4. Beveiliging en controle op toestellen van het opleidingscentrum

Onder "toestellen" van het opleidingscentrum rekenen we zowel *desktop computers, laptops, tablets* als (eventuele) *werkgsm's* die eigendom zijn van het opleidingscentrum .

4.4.1. Algemeen

De volgende beveiligingsregels resp. -controles kunnen hierop (tegelijkertijd) toegepast worden:

- Het internetverkeer en gebruikte toepassingen worden, op verscheidene niveaus, gecontroleerd inzake bv. bezochte doelsites, uitgaand verkeer, capaciteit maar ook veiligheid van de toepassing, het al dan niet veranderen van systeeminstellingen (gerelateerd aan beveiliging resp. prestaties, enz.).
- De beheerders steken veel energie in de efficiënte en effectieve werking van alle hardware en het netwerk. Dit is onmogelijk als gebruikers de systeem- of beveiligingsinstellingen veranderen. Er worden op ZoWe verpleegkunde dan ook verschillende maatregelen genomen om dit te verhinderen. Het doelbewust veranderen van systeem- of beveiligingsinstellingen is verboden.

Dit beleid wordt gecombineerd met een aantal monitoring tools en/of (lokale) logboeken, d.w.z. manieren om de handelingen bij te houden voor analyse of eventueel naar bewijslast toe.

Op ZoWe verpleegkunde worden er bepaalde *tools* gebruikt die de actieve vensters en/of het *realtime* beeldscherm van de toestellen eigendom van het opleidingscentrum kunnen monitoren. De doeleinden hiervan zijn pedagogisch en voor technische ondersteuning. Het is *niet* toegestaan om schermafdrucken te bewaren, een scherm op te nemen of een scherm over te nemen zonder toestemming van de betrokkene.

- Personeel kan, in het kader van de uit te oefenen taak, de actieve vensters, geopende websites en/of het beeldscherm zien. Het is niet uitgesloten dat de inhoud van **persoonlijke berichten** (ontvangen en/of verzonden) leesbaar is, alhoewel dit nooit het doel op zich zal zijn. Al deze medewerkers behandelen de informatie strikt vertrouwelijk, en bewaren deze niet.
- Het is, met dezelfde tools, wel toegestaan dat de beheerders, directie en eventueel andere personeelsleden die hiervoor bevoegd geacht worden, de schermen bewaren (als een schermafdruck of als een opname). Zij doen dit enkel bij een concreet vermoeden van doelbewuste en ernstige inbreuken op de deontologische code van het opleidingscentrum en alle informatie wordt strikt vertrouwelijk behandeld. Onbevoegde medewerkers hebben geen toegang tot de schermafdrucken of opnames.

4.4.2. Vergrendeling, encryptie en wissen van op afstand

De mobiele toestellen (d.w.z. *laptops, pda's, tablets, smartphones*) die bepaalde personeelsleden gebruiken maar die eigendom zijn van ZoWe verpleegkunde, dienen extra beveiligd te worden indien er persoonsgegevens op bewaard, bekeken of verwerkt worden. In het bijzonder wordt er een vergrendeling aan de hand van wachtwoord, pincode, swipe code, vingerafdruk of andere authenticatie toegepast.

Voor personeelsleden en derden (CLB) die toegang hebben tot gevoelige persoonsgegevens op het toestel in kwestie geldt bovendien:

- Encryptie van opslagmedia (indien mogelijk);
- Optie om te lokaliseren of te wissen van op afstand, in geval van diefstal of verlies (indien mogelijk).

4.5. Beveiliging en controle op toestellen van eindgebruikers zelf

Op ZoWe verpleegkunde is het mogelijk om, via het netwerk of wifi van het opleidingscentrum (zie ook

§ 2), gebruik te maken van eigen toestellen. Het is de bedoeling dat deze maximaal gebruikt worden om taken uit te voeren gerelateerd aan het opleidingscentrum .

Ook thuis kan men gebruik maken een persoonlijk toestel waarbij er toch enkele aandachtspunten zijn:

4.5.1. Algemeen

Inzake het meebrengen van een eigen toestel op school worden dezelfde maatregelen genomen zoals de toestellen van het opleidingscentrum .

4.5.2. Vergrendeling, encryptie, antivirusbeveiliging, backups en wissen van op afstand

De mobiele toestellen (d.w.z. *laptops, pda's, tablets, smartphones*) van medewerkers, waarop persoonsgegevens van ZoWe verpleegkunde bewaard, bekeken of verwerkt

worden, dienen extra beveiligd te worden. Dit beleid vraagt die medewerkers dan ook om de volgende maatregelen op deze toestellen in acht te nemen:

- Er wordt een vergrendeling aan de hand van wachtwoord, pincode, swipe code, vingerafdruk of andere authenticatie gevraagd.
- Er wordt gevraagd om een ten allen tijde up-to-date antivirusprogramma te gebruiken.
- Het is belangrijk dat de persoonlijke toestellen steeds geüpdatet zijn met de laatste patches en updates van het besturingssysteem.
- Backups dienen genomen, bewaard en beheerd te worden zoals in het respectievelijke beleid vastgelegd.

Voor personeelsleden en derden (vb VDAB, ...) die toegang hebben tot gevoelige persoonsgegevens op het toestel in kwestie wordt daarenboven het volgende gevraagd:

- Encryptie van opslagmedia (indien mogelijk);
- Optie om te lokaliseren of te wissen van op afstand, in geval van diefstal of verlies (indien mogelijk)

4.5.3. Verwisselbare media (o.a. usb-stick)

Het opleidingscentrum maakt afspraken om personeelsleden veiliger te laten omgaan met verwisselbare media.

- We adviseren om bij verwisselbare media gegevens te versleutelen als er lesvoorbereidingen, toetsen, proefwerken, studentengegevens en/of personeelsgegevens op staan.
- Gevoelige (student- of personeels-)gegevens worden niet op verwisselbare media getransporteerd.
- Verwisselbare media met privégegevens worden best niet op school gebruikt.

4.5.4. Aandachtspunten voor het gebruik van thuiscomputer voor schoolgerelateerd werk.

Het betreft toestellen in eigen bezit zoals:

- de thuiscomputer
 - *desktop of laptop*
 - *Windows, Mac, Linux, ...*
- persoonlijke *laptop* (dus geen eigendom of onder beheer van het opleidingscentrum, b.v. *leasing*)
 - thuisgebruik en/of op school
- persoonlijke tablet
- persoonlijke smartphone, gsm, ...

Richtlijnen: personeelsleden bewaken:

- een afzonderlijke account (tegenover andere gezinsleden, thuisbewoners)
- een voldoende toegangsbeveiliging
- backups en het *up-to-date* houden (besturingssysteem, antivirus en malware).

Deel 5 Backupbeleid

5.1. Inleiding

5.1.1 Situering

Voor de gegevens die een bepaald niveau van beschikbaarheid en/of integriteit vereisen, is een goed uitgestippeld backupbeleid noodzakelijk. Deze principes gelden zowel voor gegevens die zich op NAS-en¹, servers, clients, eigen toestellen, andere locaties, in de cloud, ... bevinden

Deze nota valt onder de eindverantwoordelijkheid van het schoolbestuur vzw ZoWe verpleegkunde.

5.1.2 Enkele begrippen

UPS (<i>uninterrupted power supply</i>) Noodstroomvoorziening	<i>Aangesloten systemen en opslagmedia worden gedurende enkele minuten van stroom voorzien bij pannes of spanningsfluctuaties. Dit zorgt ervoor dat gegevens in het werkgeheugen en/of cache nog kan weggeschreven worden voordat het system afgesloten moet worden.</i>
Redundantie	<i>Het algemene principe waarbij een systeem, opslag of netwerkverbinding zo opgebouwd wordt, dat indien nodig een ander systeem overneemt. In principe mogen eindgebruikers hier niets van merken. Het "eerste" systeem dient zo snel mogelijk terug hersteld te worden.</i>
Backups	<i>Het nemen van geregelde kopieën, op een andere locatie en medium, zodat bij eventueel verlies of diefstal de gegevens in kwestie hersteld kunnen worden. De aard, frequentie, enz. van de backups wordt bepaald door de classificatie van de gegevens in kwestie. Dit proces kan volledig geautomatiseerd gebeuren.</i>
Synchronisatie	<i>Gegevens bevinden zich op verschillende locaties en media, maar een onderlinge netwerkverbinding zorgt ervoor dat beide kopieën hetzelfde zijn. Aanpassingen gebeuren m.a.w. steeds in beide kopieën tegelijk. Het systeem zorgt ervoor dat aanpassingen bijgehouden worden in het geval dat de verbinding (even) weg valt, om deze bij het herstellen van de verbinding zo snel mogelijk samen te voegen.</i>

5.2. Stroomvoorziening

De ZoWe verpleegkunde zorgt in de mate van haalbaarheid voor een redundante opstelling van stroomvoorziening.

¹ NAS: Networked Attached Storage (opslagruimte die verbonden is met je netwerk.)
informatieveiligheid- en privacybeleid ZoWe verpleegkunde

5.3. Internetverbinding

De ZoWe verpleegkunde streeft er naar om een continue internetverbinding te voorzien.

5.4. Backups

ZoWe verpleegkunde streeft er naar om een performant *backup*-plan uit te werken, rekening houdend met de *'best practices'*:

- een dagelijkse *backup* van data
- een *backup* op een andere plaats
- een *'offsite'* *backup*.

5.5. Brandveiligheid

ZoWe verpleegkunde zorgt voor afdoende brandbeveiligingsmaatregelen.

Deel 6 Toegangsmatrices

6.1. Inleiding

6.1.1 Situering

In deze nota bepalen we het gebruikersrechtenbeleid op ZoWe verpleegkunde. Hiermee bedoelen we welke gebruikers(groepen) welke toegangen hebben tot bepaalde gegevens.

Deze nota valt onder de eindverantwoordelijkheid van het schoolbestuur vzw ZoWe verpleegkunde.

6.1.2 Gebruikersgroepen

Alle dragers, platformen, systemen en het netwerk die binnen ZoWe verpleegkunde gebruikt worden, vallen onder het IVP-beleid. Dit houdt in dat elk van deze dragers, platformen, systemen en het netwerk voorzien zijn van **beveiligingsgroepen**, waartoe de respectievelijke gebruikers behoren na authenticatie (zie het **toestelbeleid** en **wachtwoordbeleid**).

De volgende gebruikersgroepen worden hierbij gehanteerd:

- Administrators
- ICT-coördinatoren
- Directieleden
- Studiebegeleiders
- docenten
 - Die les geven aan betrokken student
 - Die geen les geven aan betrokken student
- Administratief medewerkers
 - Die bevoegd zijn om (in welbepaalde zin) studentgegevens te verwerken
 - Die bevoegd zijn om (in welbepaalde zin) personeelsgegevens te verwerken
 - Die niet bevoegd zijn om studenten- en/of personeelsgegevens te verwerken
- studenten
- Derden (bv. onderhoudspersoneel, externe betrokkenen, gasten)

Deze groepen worden globaal gehanteerd binnen het IVP-beleid van ZoWe verpleegkunde. Mogelijks bestaan er, voor welbepaalde gevallen of toepassingen, hiernaast nog specifiekere beveiligingsgroepen.

6.1.3 Gebruikersrechten

De algemeen gehanteerde gebruikersrechten zijn:

- Blanco: geen toegang (*men kan de gegevens niet opvragen of zien. Ze worden ook niet in overzichten of dergelijke vermeld*);
- L: leestoegang (*men kan alles zien, maar niets verwijderen, toevoegen of aanpassen*);
- W: wijzig- of schrijftoegang (*men kan alles zien, items toevoegen en aanpassen*);
- VB: volledig beheer (*dit wil zeggen dat men de toegangsrechten, van zichzelf en van anderen, kan aanpassen*).

6.2. Toegangsmatrices

De ZoWe verpleegkunde heeft een toegangsmatrixprocedure waarin alle gebruiksrechten gedefinieerd worden voor elke gebruikersgroep. Deze toegangsmatrixprocedure wordt jaarlijks opnieuw bekeken en geëvalueerd.

Volgende onderdelen worden in opgenomen:

- Gegevens van studenten
- Gegevens van personeelsleden
- Gegevens van oud-studenten
- Gegevens van oud-personeelsleden
- Gegevens van derden

goedgekeurd door Raad van Bestuur 24 oktober 2018