Informatiebeveiliging en privacybeleid

Steeds wijzer

wijzer in opvang

Colofon
Burgemeester van Lierplein 77
3134 ZB Vlaardingen
T 010 59 10 581
E info@wijzer.nu
W www.wijzer.nu

Voorgenomen besluit CvB-MT	
Overleg directeurenberaad	
Overleg medezeggenschap WIOP - COC	
Overleg medezeggenschap WIOP - OR	
Overleg Raad van Toezicht	
Definitieve vaststelling CvB	

Versie 01.1 | 1 april 2021
Deze versie verloopt op 1 januari 2025

Inhoud

1. Inleiding

Informatie en ict zijn noodzakelijk in de ondersteuning van de opvang. Omdat we met persoonsgegevens (van onszelf, kinderen en anderen) werken, is privacywetgeving daarop van toepassing.

De informatie en ict van Stichting Wijzer in Opvang worden blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Alle informatie die we bewaren en verwerken kan worden bedreigd door een aanval, een vergissing, de natuur (bijv. overstroming of brand), et cetera.

Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's die gepaard gaan met deze bedreigingen tot een aanvaardbaar niveau te reduceren. 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.

Dit beleid is van toepassing op Stichting Wijzer in Opvang en onder de Stichting Wij-zer in Opvang ressorterende opvanglocaties.

1.1.1 Informatiebeveiliging en privacy

Informatiebeveiliging is een proces voor het beschermen van Stichting Wijzer in Opvang tegen risico's en bedreigingen met betrekking tot informatie en ict. Het richt zicht op drie aspecten:

- Beschikbaarheid; informatie en aanverwante bedrijfsmiddelen zijn toegankelijk wanneer nodig;
- Integriteit; informatie en verwerkingsmethoden bevatten zo min mogelijk fouten;
- Vertrouwelijkheid; informatie is alleen toegankelijk voor diegenen die daartoe bevoegd zijn.

Privacy gaat om de bescherming van persoonsgegevens conform de huidige wet- en regelgeving. Door het goed toepassen van informatiebeveiliging kan aan deze wetgeving worden voldaan. Vooral het aspect vertrouwelijkheid is hiervoor van belang. Informatiebeveiliging is daarom integraal onderdeel van privacy.

Om privacy goed te regelen is informatiebeveiliging nodig. Daarom zien we het als één onderwerp: informatiebeveiliging en privacy (IBP).Aanhef Dit reglement is voor Stichting Wijzer in Opvang en onder de Stichting Wijzer in Opvang ressorterende opvanglocaties, gevestigd te Burgemeester van Lierplein 77 3134 ZB Vlaardingen.

2. Doel en reikwijdte

Dit beleid heeft als doelen:

- Het waarborgen van de continuïteit van de opvang en de bedrijfsvoering.
- Het garanderen van de privacy van kinderen en medewerkers waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen.

Dit beleid is een leidraad voor iedereen die betrokken is bij IBP binnen Stichting Wijzer in Opvang. Het is van toepassing op onze eigen medewerkers, tijdelijk personeel en andere personen die een rol spelen binnen Stichting Wijzer in Opvang. Het is van toepassing op

de hele organisatie van Stichting Wijzer in Opvang, waaronder de fysieke locaties, systemen op interne en externe locaties en gegevensverzamelingen die gebruikt worden.

Het informatiebeveiligings- en privacybeleid heeft raakvlak met andere beleidsgebieden, te weten:

- Algemeen veiligheids- en beveiligingsbeleid; met als aandachtsgebieden bedrijfshulpverlening, fysieke toegang en –beveiliging, crisismanagement, huisvesting en ongevallen;
- IT-beleid; met als aandachtsgebieden de aanschaf en het beheer van ict;
- Personeels- en organisatiebeleid; met als aandachtsgebieden in- en uitstroom van medewerkers, functiescheiding en vertrouwensfuncties;

Dit beleid maakt duidelijk waar de verantwoordelijkheden rondom informatiebeveiliging en privacy zijn belegd.

3. Uitgangspunten

De belangrijkste beleidsuitgangspunten bij Stichting Wijzer in Opvang zijn:

- Informatiebeveiliging en het privacy dient te voldoen aan alle relevante wet- en regelgeving
- Veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen
- Er wordt van alle medewerkers, kinderen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich ‘fatsoenlijk’ gedragen met een eigen verantwoordelijkheid
- Stichting Wijzer in Opvang is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt
- Stichting Wijzer in Opvang maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy
- IBP is een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is
- Er is een balans tussen de risico’s van hetgeen we willen beschermen en de benodigde investeringen en maatregelen
  IBP beleid Stichting Wijzer in Opvang 6
- Er is een balans tussen privacy, functionaliteit/werkbaarheid en veiligheid

3.1.1 Privacy

Stichting Wijzer in Opvang hanteert de vijf vuistregels voor privacy:

1. **Doelbepaling en doelbinding**
   Persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**
   Verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie**
   Bij de verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding staan tot het doel (= proportioneel). Het doel kan

niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. **Transparantie**
   De school/Stichting legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun Persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun Persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit**
   Er zijn maatregelen getroffen om te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn. Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen. Bij alle registraties is het privacyreglement van toepassing.

4. Wet- en regelgeving

Stichting Wijzer in Opvang voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet IKK
- Wet Harmonisatie
- Wet bescherming persoonsgegevens
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Auteurswet
- Wetboek van Strafrecht

5. Organisatie

Dit hoofdstuk beschrijft hoe IBP binnen Stichting Wijzer in Opvang is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

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

5.1.1 Richtinggevend

Eindverantwoordelijke
Het bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de maatregelen vast op het gebied van informatiebeveiliging en privacy. De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages door hen geëvalueerd. Binnen het bestuur is de directeur-bestuurder verantwoordelijk voor IBP.

5.1.2 Sturend

Manager IBP

Manager IBP is een rol op sturend niveau. Deze geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen aan op de uitvoerende laag. De manager IBP moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen Stichting Wijzer in Opvang
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen Stichting Wijzer in Opvang coördineren

Functionaris voor Gegevensbescherming
De functionaris voor gegevensbescherming (FG) houdt binnen Stichting Wijzer in Opvang toezicht op de toepassing en naleving van de privacy-wetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. FG heeft regelmatig overleg met manager IBP.

Domeinverantwoordelijkheid/proceseigenaar
Binnen de Opvang/Stichting zijn er verschillende domeinen/processen, zoals ict, personeel, administratie et cetera. Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Leidinggevenden hebben een voorbeeldrol ten opzichte van hun medewerkers.

5.1.3 Uitvoerend

Security Officer/functioneel beheerder
De Security Officer vormt een technisch aanspreekpunt voor incidenten en informatiebeveiliging. Op basis van de domeinverantwoordelijke/proceseigenaar heeft de functioneel beheerder een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in het IBP handboek.

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de (G)MR/OR)

Leidinggevende
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfs-voering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligings-beleid;
- toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;

- periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de manager IBP.

6. Controle en rapportage

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

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

Daarnaast kent Stichting Wijzer in Opvang een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst.

6.1.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij Stichting Wijzer in Opvang het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de manager IBP en Security Officer met het Bestuur als eindverantwoordelijke.

6.1.2 Classificatie en risicoanalyse

Bij Stichting Wijzer in Opvang heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang voor de informatievoorziening.

6.1.3 Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij info@wijzer.nu. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken.

6.1.4 Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid

nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij Stichting Wijzer in Opvang wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de Functionaris Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement.
Mocht de naleving ernstig tekort schieten, dan kan Stichting Wijzer in Opvang de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.
Bij Stichting Wijzer in Opvang is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

Bijlage 1: Tabel IBP rollen en taken

Niveau	Wie	Hoe	Wat
	Rollen	Verantwoordelijkheid/taken	Realiseren/vastleggen
Richtinggevend (strategisch)	Bestuur	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacy beleid • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
Sturend (tactisch)	Manager IBP	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert bestuur/CvB/directie over IBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	Processen, richtlijnen en procedures IBP, waaronder: • activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Bewerkersovereenkomsten regelen • Brief toestemming gebruik foto's en video • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers en medewerkers • Security awareness activiteiten • Sociale media reglement • Gedragscode ict en internetgebruik • Gedragscode medewerkers en leerlingen
	Functionaris voor Gegevensbe-scherming / Privacy officer	• Toezicht op naleving privacy wetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement, • procedure IBP-incident afhandeling • Inrichten meldpunt datalekken

Sturend (tactisch) (vervolg)	Domeinverantwoordelijke/ Proceseigenaren waaronder: ict, personeel (HRM / P&O), Facilitair, onderwijs, financiën, inkoop en administratie	• Classificatie / risicoanalyse in samenwerking met Manager IBP (Informatiemanager / verantwoordelijke IBP / Security officer) • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur • Samen met functioneel beheer en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • Samen met functioneel beheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leverancierslijst) • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk
Uitvoerend (operationeel)	Security officer Functioneel beheerder Medewerker Leidinggevende / directie	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • Communicatie naar alle betrok-kenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers en voortgang rapporteren aan bestuur. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken

		werkoverleggen, beoordelingen etc.;	

Blijf nieuwsgierig.
Durf te doen.
Samen steeds
wijzer.