wijzer

opvang &
onderwijs

Beleidsplan 2024-2028

Informatiebeveiliging & privacy

Colofon

Burgemeester van Lierplein 77

3134 ZB Vlaardingen

010 59 10 581

info@wijzer.nu

www.wijzer.nu

Voorgenomen besluit CvB:	27-02-2024
Overleg directeurenberaad:	19-03-2024
Overleg medezeggenschap WION:	27-03-2024
Overleg medezeggenschap WIOP:	20-03-2024
Definitieve vaststelling CvB:	09-04-2024

Versie 1.4 | 9 april 2024
Deze versie verloopt op 1 april 2028

Inhoud

1 Het belang van informatiebeveiliging en privacy

Opvang en onderwijs zijn in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van informatiebeveiliging en privacy (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van opvang, onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

2 Toelichting informatiebeveiliging en privacy

2.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden. Informatiebeveiliging richt zich op de volgende aspecten:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het opvang- en onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

2.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:

Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

2.3 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis op informatiebeveiliging en privacy binnen Wijzer te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3 Doel en reikwijdte

3.1 Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van opvang, onderwijs en bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan Wijzer persoonsgegevens verwerkt, waaronder kinderen, hun ouders/verzorgers en medewerkers.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (IBP-beleid) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, kinderen en hun ouders/verzorgers, sollicitanten, vrijwilligers en stagiaires) wordt gerespecteerd en Wijzer voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

Het IBP-beleid van Wijzer geldt voor alle medewerkers, kinderen, ouders/verzorgers, (geregistreerde) bezoekers, stagiaires, vrijwilligers (met overeenkomst) en externe relaties (inhuur/outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het netwerk verkregen kan worden.

Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Wijzer waaronder in ieder geval alle medewerkers, kinderen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Wijzer persoonsgegevens verwerkt.

Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Wijzer**.** Hieronder valt ook de gecontroleerde informatie, die door de locatie zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de locatie kan worden aangesproken. (Bijvoorbeeld uitspraken van medewerkers en kinderen in discussies, op (persoonlijke pagina's van) websites en of sociale media.)

Het beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Wijzer evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Het IBP-beleid heeft binnen Wijzer raakvlakken met:

- Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen

- Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
- IT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen
- Medezeggenschap van kinderen, hun ouders/verzorgers en medewerkers

4 Beleid – Hoe doen we dat?

Wijzer hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Wijzer neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
2. Wijzer voldoet aan alle relevante wet- en regelgeving.
3. Bij Wijzer is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van Wijzer om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen te allen tijde hun toestemming herzien.
4. Wijzer zal alle betrokkenen helder en actief informeren over de verwerkingen van de persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.
5. Wijzer legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Wijzer voldoet hiermee aan de documentatieplicht.
6. Binnen Wijzer 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 papieren documenten.
7. Wijzer is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de locatie informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en kinderen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
8. Wijzer classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.
9. Wijzer sluit met alle leveranciers van digitale leermiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de locatie, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van kinderen of medewerkers worden verstrekt.
10. Wijzer verwacht van alle medewerkers, kinderen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Wijzer heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
11. Informatiebeveiliging en privacy is bij Wijzer een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
12. Wijzer kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen

vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

13. Wijzer neemt passende technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van opvang en onderwijs, de privacy en de bedrijfsvoering kunnen verstoren. Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt Wijzer aanvullende afspraken vast over de technische maatregelen.
14. Wijzer zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

5 Uitwerking van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

5.1 Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet goed onderwijs en goed bestuur PO/VO
- Wet op het primair onderwijs, Wet voortgezet onderwijs en Wet op de expertisecentra
- Wet Onderwijstoezicht
- Wet Kinderopvang
- Wet Innovatie Kwaliteit Kinderopvang
- Besluit Basisvoorwaarden Voorschoolse Educatie
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.

De bepalingen van de meest recente versie van het convenant ‘Digitale onderwijsmiddelen en privacy’ zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

5.2 Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen over verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de **vijf vuistregels** met betrekking tot de omgang met persoonsgegevens te weten:

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 manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.
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 (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. **Transparantie**: de locatie legt aan betrokkenen (kinderen, 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 betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens 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.

5.3 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Bij dit beleidsplan IBP hoort een notitie waarin de rollen en verantwoordelijkheden worden beschreven.

5.4 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt 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, kinderen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de IBP-verantwoordelijke, de FG, en de Privacy Officer met het bestuur als eindverantwoordelijke.

5.5 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen 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 betrouwbaarheidsaspecten die van belang zijn.

Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ICT)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

5.6 Incidenten en datalekken

Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle

(beveiligings)incidenten kunnen worden gemeld via www.wijzer.nu/privacy.

Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.7 Planning en controle

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door het bestuur. Hierbij wordt rekening gehouden met:

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

Daarnaast kent Wijzer 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. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

5.8 Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.

Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG is 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 van dit beleid ernstig tekortschieten, dan kan Wijzer de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.9 Logging en monitoring

Logging en monitoring door de externe infrastructuurbeheerder zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (poging tot) ongeautoriseerde toegang tot het netwerk.

Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage beschrijft een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht en met een * aangegeven.

Documenten	**Toelichting**
Procesbeschrijving rechten betrokkenen	*Proces rondom aanvragen van betrokkenen*
Privacyreglement	
Autorisatiematrix	*Wie mogen gegevens inzien, bewerken enz.*
Afspraken gebruik sociale media	
Procedure rondom training medewerkers	*Bewustzijn creëren*
Cameratoezicht	
Wachtwoordbeleid	
Responsible disclosure	*De vinder van een kwetsbaarheid stelt eerst de eigenaar van het kwetsbare systeem op een verantwoorde manier op de hoogte voordat deze publiekelijk wordt gedeeld.*
Gedragscode ICT en internetgebruik	
Acceptable use policy	*Verantwoord gebruik bedrijfsmiddelen*
Procedure rondom uitwisselen gegevens	*Passend onderwijs, kinddossiers, leerplicht enz.*
Procesbeschrijving melden datalekken*	
Registratie beveiligingsincidenten*	
Dataregister om te voldoen aan de registratieplicht*	
Verwerkersovereenkomsten*	*Privacy bijlage beschikbaar stellen*
Procedure gegevensbeschermingseffectbeoordeling*	*DPIA*
Risicoanalyse*	
Functionaris voor Gegevensbescherming*	*Communicatie hierover aan medewerkers*

“Ik draag bij aan de toekomst van mijn omgeving, neem verantwoordelijkheid voor mijn eigen ontwikkeling en ben nieuwsgierig.”