Informatiebeveiligings- en privacybeleid

Beleid IBP

swv Zeeluwe Harderwijk

vastgesteld 5 oktober 2020

1. Inleiding

Informatie en ICT zijn noodzakelijk in de ondersteuning van het onderwijs. Omdat we vaak met kwetsbare persoonsgegevens (van onszelf, leerlingen en anderen) werken, is privacywetgeving daarop van toepassing.

De informatie en ICT van swv Zeeluwe is naar zijn aard privacygevoelig en kan worden bedreigd. Het niet beschikbaar zijn van ICT, incorrecte administraties en het uitlekken van gegevens leidt tot een onjuiste administratie. Dit kan het verttrouwen in onze organisatie schaden.

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.

Bij de ontwikkeling van dit beleid hebben we gebruik gemaakt van de ondersteuning door:
- Kennisnet
- G-flex, gecertificeerd bureau voor ICT.

1.1 Informatiebeveiliging en privacy

Informatiebeveiliging is een proces voor het beschermen van swv Zeeluwe 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).

2. Doel en reikwijdte

Dit beleid heeft als doelen:
- Het waarborgen van de continuïteit van de administratie en de bedrijfsvoering.
- Het garanderen van de privacy van leerlingen 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 swv Zeeluwe. Het is van toepassing op onze eigen medewerkers, tijdelijk personeel en andere personen die een rol spelen in swv Zeeluwe. Voor zover van toepassing zijn hierover met de aangesloten

schoolbesturen afspraken vastgelegd in diverse protocollen (voorbeeld: proces van afgifte TLV).

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

- Algemeen veiligheids- en beveiligingsbeleid; met als aandachtsgebieden bedrijfshulpverlening, 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

3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij swv Zeeluwe zijn:

- Informatiebeveiliging en privacy dient te voldoen aan alle relevante wet- en regelgeving.
- Veilig en betrouwbaar omgaan met informatie is de verantwoordelijkheid van iedereen.
- Er wordt van alle medewerkers, bezoekers en externe relaties verwacht dat zij zich ‘fatsoenlijk’ gedragen met een eigen verantwoordelijkheid; zij worden daarop aangesproken.
- swv Zeeluwe is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt.
- swv Zeeluwe maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy.
- IBP is een continu proces, waarbij periodiek wordt geëvalueerd vanuit het principe dat het altijd beter kan 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.
- Er is een balans tussen privacy, functionaliteit/werkbaarheid en veiligheid.

3.2 Beleidsuitgangspunten Privacy

swv Zeeluwe 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 organisatie 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 op basis van toestemming, zal door swv Zeeluwe de eenduidige zogenaamde Opt-out procedure worden toegepast. Dit betekent dat alle betrokkenen niets hoeven te doen om mee te doen met de regeling, maar de mogelijkheid hebben om ervan af te zien.

4. Wet- en regelgeving; protocollen

swv Zeeluwe voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet bescherming persoonsgegevens
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van het convenant ‘Digitale onderwijsmiddelen en privacy 2.0’ (zie bijlage 2) leidend bij het maken van afspraken met leveranciers.
Verder hebben we in dit kader te maken met het Protocol ‘Veilig thuis’. Voor een nadere info is bijgevoegd het ‘vng model handelingsprotocol veilig thuis’. (zie bijlage 6)
We leven de Gedragscode van Zeeluwe na.

5. Organisatie

Dit hoofdstuk beschrijft hoe IBP in swv Zeeluwe 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 Richtinggevend

Eindverantwoordelijke
De directeur-bestuurder 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 jaarlijkse rapportages door haar geëvalueerd.

5.2 Sturend

Kwaliteitsmedewerker, w.o. voor IBP
De kwaliteitsmedewerker IBP is een rol op sturend niveau. Deze geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen binnen het kantoor (de uitvoerende laag) aan. De kwaliteitsmedewerker IBP moet:

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

Naast deze sturende rol houdt de kwaliteitsmedewerker IBP binnen swv Zeeluwe toezicht op de toepassing en naleving van de privacy-wetgeving. Hij/zij zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten en is meestal ook contactpersoon voor klachten en vragen van betrokkenen met een vertrouwelijk karakter.

Domeinverantwoordelijkheid/proceseigenaar
Binnen de organisatie zijn er verschillende domeinen/processen, zoals ICT, personeel, administratie, etcetera. Gezien de kleine organisatie zijn de verantwoordelijkheden voor elk van deze domeinen/processen belegt bij enkele personen. Zij zijn verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Gezien de kleine organisatie spreekt men elkaar aan op de afspraken in dit beleid.

5.3 Uitvoerend

Ook de uitvoerende rol is belegt bij de kwaliteitsmedewerker IBP. Hij vormt een technisch aanspreekpunt voor incidenten en informatiebeveiliging.

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden en worden gevraagd om actief betrokken te zijn bij de informatiebeveiliging. Deze verantwoordelijkheden zijn beschreven in de functiebeschrijving. Ook zijn ze vastgelegd in de richtlijn 'gebruik bedrijfsmiddelen' (zie bijlage 3). Daarmee is deze richtlijn onderdeel van dit beleid.

Waar nodig worden medewerkers in hun dagelijkse werkzaamheden ondersteund met aanwezige checklists en formulieren en wordt hen gevraagd om invloed uit te oefenen op dit beleid. Dit houdt dus in dat je je verantwoordelijkheid neemt door onderzoek te doen hoe je het kan voorkomen en vervolgens elkaar weet aan te spreken.

5.4 Directeur-bestuurder

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. De directeur-bestuurder 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 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 directeur-bestuurder wordt in haar taak ondersteund door de kwaliteitsmedewerker IBP.

6. Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt periodiek getoetst en bijgesteld door de directeur-bestuurder. 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 swv Zeeluwe een risico inventarisatie en een continuiteitsparagraaf. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst.

Ook heeft swv Zeeluwe een zgn. Memorandum van overeenstemming afgesloten met het ICT bedrijf G-flex. (zie bijlage 4). Hiermee heeft G-flex toestemming om penetratie proeven uit te voeren op het IP adres van swv Zeeluwe. Hiermee wordt een back-up gemaakt en tevens gescand op kwetsbaarheden. Het systeem genereert vervolgens een gedetailleerd rapport met een lijst van kwetsbaarheden en mogelijke oplossing van het beveiligingslek.

6.1 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 swv Zeeluwe het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Binnen swv Zeeluwe is verhoging van het beveiligingsbewustzijn een verantwoordelijkheid van kwaliteitsmedewerker IBP met de directeur-bestuurder als eindverantwoordelijke.

6.2 Incidenten en datalekken

T.a.v. het swv Zeeluwe worden alle incidenten gemeld bij info@zeeluwe.nl. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken (zie bijlage 4).

6.3 Controle en naleving *en sancties*

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat de medewerkers hun verantwoordelijkheid nemen en elkaar aanspreken in geval van tekortkomingen. Dit houdt ook in dat swv Zeeluwe geen nadere afspraken op privacy-gebied maakt met andere zorginstellingen. Via de scholen heeft Zeeluwe de expliciete toestemming van ouders goed geregeld; voor zover nodig houdt ze zich aan het landelijk meldingsprotocol kindermishandeling en huiselijk geweld.

Bij swv Zeeluwe wordt actief aandacht besteed aan IBP bij de aanstelling en tijdens functioneringsgesprekken.

Voor de bevordering van de naleving van de Algemene Verordening Gegevensbescherming (AVG) vervult de kwaliteitsmedewerker IBP een belangrijke rol. Hij wordt aangesteld door de directeur-bestuurder en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

Mocht de naleving ernstig tekort schieten, dan kan swv Zeeluwe de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Bij swv Zeeluwe is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol (zie bijlage 5).

7 Overzicht bijlagen:

Bijlage 1: Tabel IBP rollen en taken

Bijlage 2: Convenant 'Digitale Onderwijsmiddelen en privacy 2.0'

Bijlage 3: Richtlijn 'Gebruik van bedrijfsmiddelen'

Bijlage 4: Pentest contract G-flex

Bijlage 5: Protocol 'Melding datalekken'

Bijlage 6: VNG Model Handelingsprotocol Veilig Thuis protocol 'Melding datalekken'

Bijlage 7: Overwegingen mbt optimalisering van TLV proces Zeeluwe