Stichting Samenwerkingsverband Passend Primair Onderwijs Hoeksche Waard

Informatiebeveiligings- en privacybeleid (IBP) **voor het SWV PPO Hoeksche Waard**

Vastgesteld door het dagelijks bestuur d.d. 18 december 2018

na goedkeuring van het toezichthoudend bestuur d.d. 18 december 2018

en instemming van de Ondersteuningsplanraad d.d. 6 december 2018

Voorwoord

Stichting SWV PPO Hoeksche Waard Passend Primair Onderwijs Hoeksche Waard (hierna: “SWV PPO Hoeksche Waard”) ondersteunt scholen bij het aanbieden van passend onderwijs. Omdat we daarbij met gevoelige persoonsgegevens omgaan, moet informatiebeveiliging en privacy voor ons natuurlijk op orde zijn. In dit document laten wij zien aan iedereen met wie wij samenwerken, intern en extern, hoe wij dat georganiseerd hebben.

Voor het SWV PPO Hoeksche Waard zijn Informatiebeveiliging en privacy onlosmakelijk met elkaar verbonden en integraal onderdeel van beleid, processen en uitvoering. Beveiliging is bij ons een continue proces van risicoafweging en het (waar nodig) vorm geven van mitigerende maatregelen. Verder gelden security en privacy by design. Dit zorgt er ook voor dat IBP geen papieren tijger is of wordt maar een onderdeel van onze dagelijkse werkwijze.

Puttershoek, juli 2018

1. Het belang van informatiebeveiliging en privacy

1.1. Inleiding

Uitwisselen van (bijzondere) persoonsgegevens is onderdeel van het dagelijks werk in het SWV PPO Hoeksche Waard. Hierbij hebben we te maken met een groot aantal mogelijke bedreigingen. Alle systemen die we gebruiken en gegevens die we bewaren en verwerken, kunnen worden bedreigd door bijvoorbeeld een aanval, een vergissing of de natuur (zoals een overstroming of brand).

Datalekken, incorrecte gegevens of diensten die niet beschikbaar zijn - in het ergste geval schaden deze incidenten onze bedrijfsvoering en daarmee het vertrouwen. Daarom zijn de continuïteit van onze dienstverlening en privacybescherming van groot belang. Ook treffen we gericht maatregelen om mogelijke risico's tot een aanvaardbaar niveau te reduceren.

Het bestuur doet daarom een beroep op iedereen die betrokken is bij de activiteiten van het SWV PPO Hoeksche Waard, vanuit een gemeenschappelijke visie en wil, de verwerking van (persoons)gegevens correct te laten verlopen.

Dit beleid gaat dieper in op de bescherming van ict en in het bijzonder persoonsgegevens. Het dient als norm en leidraad voor alle informatieverwerking en biedt een uitgangspunt voor controle.

Naast het Privacyreglement en de Privacyverklaring biedt dit beleid elke belanghebbende – het ingezette personeel, (ouders / verzorgers van) kinderen of leverancier –inzage in de manier waarop we omgaan met persoonsgegevens.

1.2. De scope van het informatiebeveiligings- en privacybeleid

Het informatiebeveiligings- en privacybeleid is van toepassing op alle informatieverwerking binnen en namens het SWV PPO Hoeksche Waard.

Het beleid is van toepassing op personeel dat door derden wordt ingezet om diensten te verlenen aan of namens onze organisatie. SWV PPO Hoeksche Waard heeft geen eigen (tijdelijk) personeel.

1.3. Het doel van informatiebeveiliging en privacy

Het Informatiebeveiligings- en privacybeleid heeft de volgende doelen:

- het waarborgen van de continuïteit van de dienstverlening;
- het beschermen van de privacy van eenieder van wie het SWV PPO Hoeksche Waard persoonsgegevens verwerkt;
- het voorkomen en zo goed mogelijk afhandelen van incidenten;
- het minimaliseren van de eventuele gevolgen van incidenten.

Bij het realiseren van deze doelen bewaakt het SWV PPO Hoeksche Waard de balans tussen werkbaarheid – in de meest brede zin van het woord – en informatiebeveiliging en privacy.

2. Het beleid

Het beleid bestaat uit keuzes die het SWV PPO Hoeksche Waard maakt om de doelen rond informatiebeveiliging en privacy te bereiken.

2.1. Communicatie

Het SWV PPO Hoeksche Waard communiceert zowel intern als extern helder en actief over informatiebeveiliging en privacy. Zo beschikt het SWV PPO Hoeksche Waard over een Privacyreglement en Privacyverklaring. Al het ingezette personeel en diensten van het SWV PPO Hoeksche Waard dienen voorbeeldig te zijn wat betreft informatiebeveiliging en privacy.

2.2. Wet- en regelgeving

Het SWV PPO Hoeksche Waard houdt zich aan alle relevante wet- en regelgeving. Twee regels vormen daarbij de basis:

- het bestuur van het SWV PPO Hoeksche Waard is eindverantwoordelijk voor de bescherming van persoonsgegevens;
- het SWV PPO Hoeksche Waard hanteert passende technische en organisatorische maatregelen voor het beschermen van diensten en in het bijzonder persoonsgegevens.

2.3. IBP is overal in verweven

Het SWV PPO Hoeksche Waard beschouwt informatiebeveiliging en privacy als onlosmakelijk met elkaar verbonden en als belangrijk onderdeel van het beleid, de processen en de uitvoering van diensten. Daar waar mogelijk wordt informatiebeveiliging en privacy opgenomen in bestaande processen.

2.4. IBP is de verantwoordelijkheid van iedereen

Omdat iedereen binnen en rondom het SWV PPO Hoeksche Waard bijdraagt aan informatie-beveiliging en privacy, zijn de rollen en verantwoordelijkheden rondom informatiebeveiliging en privacy duidelijk vastgelegd.

2.5. Beveiliging

Ons proces voor informatiebeveiliging is doorlopend en cyclisch. Dat betekent dat het SWV PPO Hoeksche Waard jaarlijks de organisatie als geheel evalueert, controleert en waar nodig verbetert. Nieuwe ontwikkelingen, incidenten binnen en buiten het SWV PPO Hoeksche Waard, aanschaf van diensten of bedrijfsmiddelen en grote wijzigingen in de dienstverlening zijn aanleiding tot extra evaluatie, controle en eventuele bijstelling.

Het SWV PPO Hoeksche Waard past waar nodig classificatie, privacy by design, security by design en privacy by default toe om passende maatregelen te kunnen treffen.

3. Uitvoering

Om het informatiebeveiligings- en privacybeleid te realiseren, besteedt het SWV PPO Hoeksche Waard aandacht aan een aantal zaken.

3.1. Bewustzijn

Het bevorderen van bewustzijn rondom informatiebeveiliging en privacy is de verantwoordelijkheid van al het ingezette personeel. Het beveiligingsbewustzijn wordt vergroot door:

- voorlichting;
- opstellen en uitdragen van werkinstructies (o.a. handleiding aanvaardbaar gebruik bedrijfsmiddelen, geheimhouding, werkinstructie met betrekking bewaren en vernietigen).

Deze middelen dragen het volgende uit:

- het belang van informatiebeveiliging en privacy voor het SWV PPO Hoeksche Waard;
- nieuwe ontwikkelingen op het gebied van informatiebeveiliging en privacy (bijvoorbeeld actuele incidenten);
- de belangrijkste veiligheidsmaatregelen rond dagelijkse werkzaamheden;
- waar belanghebbende terecht kunnen bij incidenten of met ideeën en vragen.

3.2. Incidenten en datalekken

Ingezet personeel die een incident of inbreuk rond informatiebeveiliging en/of privacy vermoeden, dienen dit te melden. Een vraag of suggestie over informatiebeveiliging en privacy kan ook gemeld worden. Alle meldingen worden volgens een vast proces behandeld. Het SWV PPO Hoeksche Waard heeft daartoe een Beveiligingsincident en Datalek protocol opgesteld.

3.3. Naleving

Schending van de wetgeving, instructies of regels rond informatiebeveiliging en privacy kan leiden tot corrigerende maatregelen.

3.4. Actualiteit

Het SWV PPO Hoeksche Waard houdt rekening met actuele ontwikkelingen. Daarom wordt dit beleid minimaal elke twee jaar getoetst en bijgesteld door de Directie aan de hand van het volgende:

- de behoeften en verwachtingen van belanghebbenden in de onderwijsketen;
- de status van de informatiebeveiliging als geheel (beleid, organisatie, risico's);
- de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan;
- wet- en regelgeving.

3.5. Wet- en regelgeving

Het SWV PPO Hoeksche Waard voldoet aan alle wet- en regelgeving die relevant is in dit verband.

Ter uitvoering van de privacyregels heeft het SWV PPO Hoeksche Waard – zoals gezegd- een Privacyreglement, Privacyverklaring en interne werkinstructies vastgesteld.

3.6. De vijf vuistregels van privacy

Het SWV PPO Hoeksche Waard houdt zich bij het verwerken van persoonsgegevens aan de beginselen rond de verwerking persoonsgegevens (art.5 AVG). De vijf vuistregels van privacy 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 verder verwerkt voor andere doeleinden.

2. Grondslag: verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen.

3. Dataminimalisatie: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt. Het type persoonsgegevens staat in verhouding tot het doel – het doel kan niet met minder of alternatieve gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. Transparantie: het SWV PPO Hoeksche Waard legt aan betrokkenen (zoals leerlingen, hun ouders/verzorgers en ingezette personeel) op transparante manier en ongevraagd verantwoording af over het gebruik van hun persoonsgegevens en het beleid daarover. Daarnaast hebben de betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Ook kunnen betrokkenen zich geheel verzetten tegen het gebruik van hun persoonsgegevens.

5. Data-integriteit: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

3.7. Dataregister

Alle verwerkingen binnen en namens het SWV PPO Hoeksche Waard worden vastgelegd en up-to-date gehouden in een dataregister.

3.8. Planning & controle

Het SWV PPO Hoeksche Waard doorloopt een jaarlijkse planning- en controlecyclus voor informatiebeveiliging en privacy, deze bestaat minimaal uit de volgende activiteiten:

- Risico-inventarisatie en selectie van maatregelen.

  Ieder jaar vindt een risico-inventarisatie plaats om de grootste risico's te identificeren. De resultaten hiervan bepalen welke informatiebeveiligingsmaatregelen geïmplementeerd of verbeterd dienen te worden in dat jaar.

- Controle en rapportage

  Operationele controle op de naleving van beleid en instructies wordt verricht door de Directie. De Directie rapporteert elk half jaar aan het bestuur over de informatiebeveiliging binnen het SWV PPO Hoeksche Waard, de vorderingen rond implementatie en verbetering van maatregelen. Incidenten worden zo spoedig mogelijk gemeld aan het dagelijks bestuur. Aan het einde van het jaar rapporteert de Directie over de implementatie van informatiebeveiligingsmaatregelen die uit de risico-inventarisatie zijn gekomen.

- Overleg FG

  Er vindt maandelijks overleg plaats met de FG.

4. Organisatie

Het SWV PPO Hoeksche Waard verdeelt de rollen en verantwoordelijkheden voor informatiebeveiliging en privacy als volgt:

4.1. Ingezet personeel

Al het ingezette personeel heeft verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Daartoe heeft het SWV PPO Hoeksche Waard specifieke werkinstructies opgesteld en met het ingezette personeel gedeeld.

Het SWV PPO Hoeksche Waard vraagt het ingezette personeel zich actief bezig te houden met informatiebeveiliging. Bijvoorbeeld door meldingen te maken van beveiligingsincidenten, verbetervoorstellen te doen en invloed uit te oefenen op het beleid binnen het SWV PPO Hoeksche Waard.

4.2. Bestuurder en Directie

De bestuurder is de eindverantwoordelijke voor informatiebeveiliging en privacy.

Het bestuur is verantwoordelijk voor:

- het vaststellen van het informatiebeveiligingsbeleid en de daaruit volgende instructie voor het SWV PPO Hoeksche Waard;
- het evalueren van de toepassing en werking van het informatiebeveiligingsbeleid op basis van rapportages.

Binnen het dagelijks bestuur is de voorzitter portefeuillehouder voor informatiebeveiliging en privacy.

De Directie:

- ziet toe op de naleving van het informatiebeveiligings- en privacybeleid door het ingezette personeel;
- heeft een positieve en actieve houding ten aanzien van informatiebeveiliging en privacy;
- fungeert als voorbeeldfunctie.
- behandelt informatiebeveiliging in bijvoorbeeld werkoverleg;
- handelt samen met de FG (vertrouwelijke) informatiebeveiligingsincidenten af.

4.3. Specifieke verantwoordelijkheden

Voor de uitvoering van het informatiebeveiligings- en privacybeleid zijn onder meer nodig: beleidsvoorbereiding, beheer van de processen, richtlijnen en procedures en controle op de naleving daarvan. Het SWV PPO Hoeksche Waard verdeelt deze verantwoordelijkheden als volgt:

- de Directie houdt de centrale geautomatiseerde informatievoorziening en de beveiliging daarvan in stand;
- de Directie is het technische aanspreekpunt rond informatiebeveiliging binnen het SWV PPO Hoeksche Waard;
- de Directie beheert de personele bezetting van het SWV PPO Hoeksche Waard. Dit raakt de informatiebeveiliging en privacy wat betreft de selectie, de voorlichting en de beëindiging de inhuur van het ingezette personeel en het gebruik en delen van personeelsgegevens;

- het Bestuur is verantwoordelijk voor de huisvesting. Binnen informatiebeveiliging is vooral de fysieke beveiliging van het kantoorpand een belangrijk thema;
- de Directie is verantwoordelijk voor de informatiebeveiliging rond administratieve procedures;
- De FG houdt toezicht op de naleving van de Algemene Verordening Gegevensbescherming binnen het SWV PPO Hoeksche Waard. Hij of zij doet waar nodig aanbevelingen voor een betere bescherming van persoonsgegevens. De FG meldt incidenten, indien nodig, aan de toezichthouder.
- de Directie (in samenspraak met de FG en met ondersteuning van het secretariaat) beheert het loket voor inzageverzoeken en meldingen van externe partijen.