Passend Onderwijs IJmond

Voorwoord

Digitalisering in de maatschappij leidt tot toenemende beschikbaarheid van data en potentieel dus tot nieuwe of rijkere informatie. Digitalisering speelt ook een grote rol binnen het onderwijs, datasturing en informatisering maken het mogelijk om steeds beter samen te werken.

Digitalisering brengt ook risico's met zich mee. Het leidt tot vraagstukken rondom het verzamelen van data en de verschillende vormen van classificatie daarbinnen.
Denk daarbij in het bijzonder aan persoonsgegevens. Met welk doel worden ze verzameld, wie beslist hierover, wie heeft ervoor getekend? En indien je met de juiste doelbinding beschikt over data hoe ga je er dan qua beveiliging mee om, zodat je voorkomt dat ze in verkeerde handen kunnen vallen.

Het Samenwerkingsverband Passend Onderwijs IJmond ondersteunt scholen bij het realiseren van goed (passend) onderwijs. Omdat we daarbij met gevoelige persoonsgegevens omgaan, moet informatiebeveiliging en privacy voor ons natuurlijk op orde zijn. In dit document laten wij aan iedereen met wie wij samenwerken (zowel intern als extern) zien, hoe wij dat georganiseerd hebben.

Voor het Samenwerkingsverband Passend Onderwijs IJmond zijn Informatiebeveiliging en privacy onlosmakelijk met elkaar verbonden en integraal onderdeel van beleid, processen en uitvoering. We hebben gekozen voor ISO 27001 als verzameling van beveiligingsmaatregelen om ons continue proces van risicoafweging en maatregelen welke negatieve effecten verminderen of wegnemen, vorm te geven. Verder gelden security en privacy by design. Dit zorgt er ook voor dat informatiebeveiliging en privacy (IBP) geen papieren tijger is of wordt maar een onderdeel van onze dagelijkse werkwijze.

Peter Truijens

directeur-bestuurder Samenwerkingsverband Passend Onderwijs IJmond

1. Het belang van informatiebeveiliging en privacy

Uitwisselen van bijzondere persoonsgegevens is onderdeel van het dagelijks werk in het Samenwerkingsverband Passend Onderwijs IJmond, hierna te noemen SWV PO IJmond.

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 (Cyber)aanval, een vergissing of de natuur (zoals een overstroming of brand).

Datalekken, incorrecte gegevens of diensten die niet beschikbaar zijn schaden in het ergste geval 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 PO IJmond, 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 audit en controle.

Dit beleid biedt elke belanghebbende – medewerker, school, ouder, gemeente (CJG), samenwerkende partner (w.o. Jeugdhulp) of leverancier – een inzage in de manier waarop we omgaan met persoonsgegevens.

1.1. De scope van het informatiebeveiligings- en privacy beleid

Het informatiebeveiligings- en privacy beleid is van toepassing op alle informatieverwerking binnen en namens het SWV PO IJmond. Het beleid is van toepassing op onze eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen voor of namens onze organisatie.

1.2. Het doel van informatiebeveiliging en privacy

Het Informatiebeveiligings- en privacy beleid heeft de volgende doelen:
- Het waarborgen van de continuïteit van de dienstverlening;
- Het beschermen van de privacy van eenieder van wie het SWV PO IJmond 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 PO IJmond 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 PO IJmond maakt om de doelen rond informatiebeveiliging en privacy te bereiken.

2.1. Voorbeeldrol

Het SWV PO IJmond heeft een voorbeeldrol in de onderwijsketen en communiceert helder en actief over informatiebeveiliging en privacy. Alle medewerkers en diensten van het SWV PO IJmond dienen voorbeeldig te zijn wat betreft informatiebeveiliging en privacy.

2.2. Wet- en regelgeving

Het SWV PO IJmond houdt zich aan alle relevante wet- en regelgeving. Twee regels vormen daarbij de basis:
• De directeur-bestuurder van het SWV PO IJmond is eindverantwoordelijk voor de bescherming van persoonsgegevens.
• Het SWV PO IJmond 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 PO IJmond 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 PO IJmond bijdraagt aan informatiebeveiliging en privacy, zijn de rollen en verantwoordelijkheden rondom informatiebeveiliging en privacy duidelijk vastgelegd.

2.5. ISO 27001 als basis

Het SWV PO IJmond kiest ISO 27001 (en ISO 27002) als een verzameling van geschikte beveiligingsmaatregelen. Hierbij is het proces voor informatiebeveiliging doorlopend en cyclisch. Dat betekent dat het SWV PO IJmond jaarlijks de organisatie als geheel evalueert, controleert en verbetert.

Nieuwe ontwikkelingen of incidenten, binnen en buiten het SWV PO IJmond, aanschaf van diensten of bedrijfsmiddelen en grote wijzigingen in de dienstverlening zijn aanleiding tot extra valuatie, controle en eventuele bijstelling. Het SWV PO IJmond past 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 PO IJmond aandacht aan een aantal zaken.

3.1. Bewustzijn

Het bevorderen van bewustzijn rondom informatiebeveiliging en privacy is de verantwoordelijkheid van alle medewerkers. Het beveiligingsbewustzijn wordt vergroot door:
• Voorlichting (security awareness training)
• Opstellen en uitdragen van gedragsregels (handleiding aanvaardbaar gebruik bedrijfsmiddelen)

Deze middelen dragen het volgende uit:
• Het belang van informatiebeveiliging en privacy voor het SWV PO IJmond
• Nieuwe ontwikkelingen op het gebied van informatiebeveiliging en privacy (bijvoorbeeld actuele incidenten)
• De belangrijkste veiligheidsmaatregelen rond dagelijkse werkzaamheden
• Waar mensen terecht kunnen bij incidenten of met ideeën en vragen

3.2. Incidenten en datalekken

Medewerkers 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 als incident gemeld worden. Alle meldingen worden volgens een vast proces behandeld.

Een interne medewerker kan melding doen via de website of via een email naar: info@passendonderwijsijmond.nl

Wanneer het om persoonsgegevens gaat, wordt de Functionaris voor de Gegevensbescherming (FG) ingeschakeld. Na afhandeling van het incident wordt de melder ingelicht over de afhandeling daarvan.

Een melding van incidenten of verzoeken rondom persoonsgegevens door externe partijen kan gedaan worden bij het secretariaat, of via email naar: info@passendonderwijsijmond.nl.

Op de website van het SWV PO IJmond, www.passendonderwijsijmond.nl, staat deze procedure vermeld.

Externe partijen, scholen en betrokkene(n) kunnen op de website terecht voor:
• Algemene informatie over de verwerking van persoonsgegevens.
• Verzoeken voor inzage van de eigen verwerkte persoonsgegevens en eventuele wijziging of verwijdering daarvan.

3.3. Naleving

Schending van de wetgeving, voorschriften of regels rond informatiebeveiliging en privacy kan leiden tot corrigerende maatregelen zoals non-actiefstelling, disciplinaire straffen en beëindiging van een contract of dienstverband.

3.4. Actualiteit

Het SWV PO IJmond houdt rekening met actuele ontwikkelingen. Daarom wordt dit beleid minimaal elke twee jaar getoetst en bijgesteld door het bestuur 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 dient te worden aangepast c.q. te worden herzien
• Wet- en regelgeving

3.5. Wet- en regelgeving

Het SWV PO IJmond voldoet aan alle wet- en regelgeving die relevant is in dit verband zoals maar niet beperkt tot:
• De Algemene Verordening Gegevensbescherming;
• De Archiefwet – in het bijzonder bewaartermijnen;
• Het Privacyconvenant onderwijs;
• Privacyregels.
Ter uitvoering van de privacyregels heeft het SWV PO IJmond een privacyreglement vastgesteld

3.6. De vijf vuistregels van privacy

Het SWV PO IJmond 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 PO IJmond legt aan betrokkenen (zoals leerlingen, hun ouders en medewerkers) 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 PO IJmond worden vastgelegd en up-to-date gehouden in een dataregister.

3.8. Planning & controle

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

• Risico-inventarisatie en selectie van maatregelen.
In het eerste kwartaal van elk jaar vindt een risicoworkshop plaats om de grootste risico's te identificeren. De resultaten hiervan bepalen welke informatie beveiligingsmaatregelen geïmplementeerd of verbeterd dienen te worden in dat jaar.

• Controle en rapportage
Operationele controle op de naleving van beleid en richtlijnen wordt verricht in opdracht van het bestuur door de aangewezen medewerker(s).
De FG rapporteert elk kwartaal aan het bestuur over de informatiebeveiliging binnen het SWV PO IJmond, de vorderingen rond implementatie en verbetering van maatregelen en de incidenten in dat kwartaal. Aan het einde van het jaar rapporteert de FG-er over de implementatie van informatiebeveiligingsmaatregelen die uit de risicoworkshop zijn gekomen.

• Interne audit
Controle op de implementatie en borging van het informatiebeveiligings- en privacy beleid en de richtlijnen en maatregelen die hieruit voortkomen. Deze vindt gedurende het jaar plaats en wordt gedetailleerd beschreven in het 'DPIA SWV PO IJmond'. De uitkomst van deze audit wordt gerapporteerd aan de directeur-bestuurder van het SWV PO IJmond.

• Externe audit
Op verzoek van het bestuur vindt een onafhankelijke controle van de informatiebeveiliging van één of meerdere onderdelen van de primaire bedrijfsvoering van het SWV PO IJmond plaats. De uitkomst van deze audit wordt gerapporteerd aan het bestuur.

4. Organisatie

Het SWV PO IJmond verdeelt de rollen en verantwoordelijkheden voor informatiebeveiliging en privacy als volgt:

4.1. Medewerkers

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden, zoals beschreven in het Handboek personeel SWV PO IJmond en de 'Handleiding acceptabel gebruikmaken van bedrijfsmiddelen'. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Wij vragen medewerkers zich actief bezig te houden met informatiebeveiliging. Bijvoorbeeld door meldingen te maken van security incidenten, verbetervoorstellen te doen en invloed uit te oefenen op het beleid binnen het SWV PO IJmond.

4.2. Management

De directeur-bestuurder is de eindverantwoordelijke voor informatiebeveiliging en privacy.

Het bestuur is verantwoordelijk voor:
• Het vaststellen van het informatiebeveiligingsbeleid en de daaruit volgende richtlijnen voor het SWV PO IJmond.
• Het evalueren van de toepassing en werking van het informatiebeveiligings-beleid op basis van rapportages.
Binnen het toezichthoudend bestuur is een portefeuillehouder voor informatiebeveiliging en privacy aangewezen.

Verdere verantwoordelijkheid van het bestuur:
• Ziet toe op de naleving van het informatiebeveiligings- en privacybeleid door medewerkers.
• Heeft een positieve en actieve houding ten aanzien van informatiebeveiliging en privacy.
• Fungeert als voorbeeldfunctie.
• Behandelt informatiebeveiliging in bijvoorbeeld werkoverleg en beoordelingen.
• Handelt vertrouwelijke informatiebeveiligingsincidenten af.

4.3. Specifieke verantwoordelijkheden

Voor de uitvoering van het informatiebeveiligings- en privacy beleid zijn onder meer nodig: beleidsvoorbereiding, beheer van de processen, richtlijnen en procedures en controle op de naleving daarvan. Het SWV PO IJmond verdeelt deze verantwoordelijkheden als volgt:

• Het secretariaat houdt de centrale geautomatiseerde informatievoorziening en de beveiliging daarvan in stand.

• De FG is het technische aanspreekpunt rond informatiebeveiliging binnen het SWV PO IJmond.

• De directeur-bestuurder beheert het personeelsbeleid van het SWV PO IJmond.
Dit raakt de informatiebeveiliging en privacy wat betreft de selectie, de voorlichting en het ontslag

van personeel en het gebruik en delen van personeelsgegevens.

• Het secretariaat is verantwoordelijk voor de huisvesting. Binnen informatiebeveiliging is vooral de fysieke beveiliging van het kantoorpand een belangrijk thema.

• Het secretariaat is verantwoordelijk voor de informatiebeveiliging rond administratieve procedures.

• De Functionaris voor de Gegevensbescherming (FG) houdt toezicht op de naleving van de Wet bescherming persoonsgegevens binnen het SWV PO IJmond. Hij of zij doet aanbevelingen voor een betere bescherming van persoonsgegevens. De FG meldt voorgenomen verwerking van persoonsgegevens, indien nodig, aan de toezichthouder (toezichthoudend bestuur).

• Het secretariaat beheert de website TOP dossier platform voor inzageverzoeken en meldingen van interne en externe partijen.