Normenkader
Informatiebeveiliging en Privacy
voor het onderwijs

Beleid informatiebeveiliging & Privacy

Versie: 1.1

Versie Kennisnet: Januari 2025 (aanvulling AR dec 2025)

Documentgeschiedenis

Revisies

Versie	Datum	Auteur	Review
1		*Alex Raaijmakers* *a.raaijmakers@privaty.nl*	*Concept* 20250402 *Voorgaande versie is herzien n.a.v. feedback en stijl wensen*
2	*11-09-2025*	*Mark van den Bos*	*Revisie n.a.v. feedback KBG & Richard*
3	*15-12-2025*	*Richard Mutters*	*Verbeterde leesbaarheid en lay-out van het eerder opgestelde en besproken beleidsdocument eb verwerking feedback FG AR*

Vaststelling

Naam	Functie	Versie	Datum
Ingrid van Doesburg	Voorzitter	1.1	10-02-2026

Documentclassificatie

Classificatie	Beschrijving
Openbaar	Dit document mag zonder beperkingen worden gedeeld
Vertrouwelijk	Dit document mag worden gedeeld met medewerkers van PCBO.
Geheim	Dit document is exclusief bestemd voor de medewerkers en relevante stakeholders van PCBO

Inhoudsopgave

1. Inleiding

Dit beleidsdocument sluit aan bij het visiedocument van PCBO ten aanzien van de informatiebeveiliging en de naleving van de privacyregelgeving en beschrijft hoe PCBO Rotterdam dit in de praktijk toepast om de continuïteit van het onderwijs te waarborgen en te voldoen aan wettelijke eisen, met name het Normenkader IBP-FO.

2. Doel en Reikwijdte

2.1 Doelstellingen

Ons IBP-beleid is gericht op:

- Continuïteit van het onderwijs en de bedrijfsvoering.
- Waarborgen van Privacy voor alle betrokkenen (leerlingen, ouders, medewerkers, etc.).
- Het voorkomen en, indien nodig, beperken van de gevolgen van beveiligings- en privacy-incidenten.
- Aantoonbaar voldoen aan de AVG en het Normenkader IBP-FO (Governance, Risk & Compliance - GRC).

Het uitgangspunt is het respecteren van de privacy van de betrokkene, waarbij een juiste balans wordt gezocht tussen privacy, functionaliteit en veiligheid.

2.2 Reikwijdte

Dit beleid geldt voor:

- **Alle betrokkenen:** Medewerkers, leerlingen, ouders/verzorgers, bezoekers en externe relaties (inhuur/outsourcing).
- **Alle systemen en data:** Alle apparaten/devices (inclusief BYOD), het schoolnetwerk, alle geautomatiseerde en niet-geautomatiseerde verwerkingen van persoonsgegevens, en alle informatie (gecontroleerd en niet-gecontroleerd) waarvoor PCBO verwerkingsverantwoordelijk is.

3 Definities en Kaders

3.1 Wat is IBP?

Informatiebeveiliging en Privacy zijn nauw met elkaar verbonden en worden daarom als één proces behandeld: IBP.

Aspect	Definitie	Toelichting
Informatiebeveiliging	Het nemen van samenhangende, aantoonbare en passende maatregelen om de betrouwbaarheid van de informatievoorziening en privacy te garanderen.	Richt zich op BIV (Beschikbaarheid, Integriteit, Vertrouwelijkheid) om risico's zoals financiële schade of digitaal isolement (Ransomware) te voorkomen.
Privacy (AVG)	Zorgvuldige omgang met persoonsgegevens om de (grond)rechten van betrokkenen te beschermen.	Persoonsgegevens zijn alle gegevens die een natuurlijk persoon direct of indirect kunnen identificeren. Verwerking is elke handeling met die gegevens.

3.2 Wettelijke Kaders

De basis voor ons beleid wordt gevormd door de Europese standaard **GDPR** (in Nederland de **AVG**) en de internationale standaard **ISO-NEN/IEC 27001** (voor informatiebeveiliging). Dit alles wordt samengebracht in het **Normenkader IBP-FO** (uitgebracht door OCW, PO- en VO-raden).

4 Ons IBP-Beleid: Hoe doen we dat?

PCBO hanteert de volgende 14 beleidsuitgangspunten:

Nr.	Beleidsuitgangspunt	Kern van de Actie
1.	**Eigenaarschap en Verantwoording**	Het Schoolbestuur neemt de verantwoordelijkheid en is de verwerkingsverantwoordelijke.
2.	**Naleving Wet- en Regelgeving**	PCBO voldoet aan alle relevante wet- en regelgeving (AVG, IBP-FO, e.d.).
3.	**Doelbinding en Grondslag**	De verwerking van persoonsgegevens is altijd gekoppeld aan een specifiek doel en gebaseerd op één van de zes wettelijke grondslagen (bijv. toestemming, wettelijke verplichting). Betrokkenen behouden hun rechten (inzage, bezwaar, etc.).
4.	**Transparante Informatievoorziening**	Betrokkenen worden actief en correct geïnformeerd over de verwerking van hun persoonsgegevens en hun bijbehorende rechten.

Nr.	Beleidsuitgangspunt	Kern van de Actie
5.	**Documentatieplicht (Register van Verwerkingen)**	Alle verwerkingen, leveranciers en beveiligingsmaatregelen worden vastgelegd in een geautomatiseerd GRC-systeem (o.a. het Register van Verwerkingen) om aantoonbaar te voldoen aan de documentatieplicht.
6.	**Verantwoordelijkheid van Iedereen**	Veilig omgaan met informatie is de verantwoordelijkheid van iedereen. Het bestuur faciliteert training en bewustwordingsactiviteiten.
7.	**Eigenaarschap van Informatie**	PCBO is eigenaar van de informatie die onder haar verantwoordelijkheid wordt verwerkt. Medewerkers en leerlingen worden geïnformeerd over de regels.
8.	**Classificatie en Risicoanalyse**	Informatie wordt geclassificeerd op basis van BIV-eisen (Beschikbaarheid, Integriteit, Vertrouwelijkheid). De classificatie is het uitgangspunt voor risicoanalyses en passende beveiligingsmaatregelen.
9.	**Verwerkersovereenkomsten**	Met alle verwerkers (leveranciers van digitale middelen) worden voorafgaand aan het gebruik verwerkersovereenkomsten afgesloten. PCBO beoordeelt deze op basis van het Privacy Convenant 4.0.
10.	**Gedrag en Bewustzijn**	Van alle betrokkenen wordt 'fatsoenlijk' gedrag en een eigen verantwoordelijkheid verwacht. PCBO waarborgt dit met een gedragscode en faciliteert kennis.
11.	**Continu Verbeterproces**	IBP is een continu proces dat minimaal jaarlijks wordt geëvalueerd. Afwijkingen worden via de GRC-cyclus (risicogestuurd en taakgericht) verbeterd.
12.	**IBP by Design**	Voorafgaand aan wijzigingen, aanschaf van nieuwe systemen of nieuwe verwerkingen, wordt een risicoanalyse doorlopen (o.a. Pre-DPIA) om tijdig passende maatregelen te nemen.
13.	**Passende Beveiligingsmaatregelen**	PCBO neemt passende technische en organisatorische maatregelen. Bij uitbesteding worden deze eisen opgelegd aan de verwerker(s) via de Verwerkersovereenkomst.
14.	**Incidenten en Datalekken**	Alle incidenten worden vastgelegd in het GRC-systeem, afgehandeld en gemeld (zoals de meldplicht datalekken vereist). Melden wordt gestimuleerd via Responsible Disclosure.[1]

[1] Responsible disclosure is het proces waarbij beveiligingsonderzoekers kwetsbaarheden in systemen of software op een verantwoorde manier melden aan de betrokken organisatie, zodat deze de kans krijgt om het probleem op te lossen voordat het publiekelijk wordt gemaakt.

5 Uitwerking in de Praktijk

5.1 Basisregels bij Persoonsgegevens ()

Bij de verwerking van persoonsgegevens zijn de volgende vuistregels leidend:

1. **Doelbepaling en doelbinding:** Gegevens worden alleen gebruikt voor vooraf vastgestelde en gerechtvaardigde doeleinden.
2. **Grondslag:** De verwerking is gebaseerd op één van de zes wettelijke grondslagen.
3. **Dataminimalisatie:** De hoeveelheid en het soort gegevens zijn beperkt tot wat noodzakelijk en proportioneel is. Gegevens worden niet langer bewaard dan nodig (bewaartermijnen).
4. **Transparantie:** De school legt op transparante wijze verantwoording af over de verwerking van persoonsgegevens. Betrokkenen hebben recht op inzage, verbetering, etc.
5. **BIV-waarborging:** Er zijn passende en aantoonbare maatregelen getroffen om de Beschikbaarheid, Integriteit en Vertrouwelijkheid te garanderen.
6. **Opslagbeperking:** niet meer gegevens verwerker of opslaan als strikt noodzakelijk voor het doel. (dit gaat over proportionaliteit en subsidiariteit)
7. **Bewaartermijnen en vernietigingsbeleid**: Na het verstrijken van de bewaartermijn vernietigen we actief de gegevens ter voorkoming van openbaring bij datalekken.

5.2 Voorlichting en Bewustzijn

- Kennis en bewustwording zijn cruciaal, aangezien 80% van de incidenten voortkomt uit menselijk handelen.
- PCBO zorgt voor **regelmatig terugkerende bewustwordingscampagnes** en stelt een **minimaal vereist kennisniveau IBP** vast voor medewerkers.

5.3 Risicoanalyse en IBP by Design

- Het niveau van de beveiligingsmaatregelen hangt af van de BIV-classificatie[2] van de gegevens.
- Voorafgaand aan elk nieuw (ICT-)project of verwerking wordt een Pre-DPIA en een beoordeling van de Verwerkersovereenkomst doorlopen. Bij restrisico's volgt een volledige DPIA. De resultaten worden aangeboden aan de Functionaris voor Gegevensbescherming (FG) ter waarborging.

5.4 Planning, Controle en Naleving

- Het IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door het bestuur, op basis van actuele risico's, wetgeving en de effectiviteit van de genomen maatregelen.
- Het GRC-systeem [3]is leidend voor de beoordeling van de effectiviteit en verantwoording.

[2] BIV-classificatie is een systeem dat binnen de informatiebeveiliging wordt gebruikt om de Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie en systemen te waarborgen.
[3] Een GRC-systeem (Governance, Risk, and Compliance) is een framework dat organisaties helpt bij het effectief besturen, risico's beheren en voldoen aan wet- en regelgeving.

- De Functionaris voor Gegevensbescherming (FG) vervult een belangrijke, onafhankelijke toezichthoudende en adviserende rol op de naleving van de AVG.
- Bij ernstige tekortkomingen in de naleving kunnen sancties worden opgelegd binnen de wettelijke en CAO-kaders.

5.5 Logging en Monitoring

- De IT-afdeling bewaakt gebeurtenissen en toegang tot systemen (in- en uitloggen, ongeautoriseerde toegangspogingen).
- Gezien verwerkingen vaak in de cloud plaatsvinden, worden **frequente rapportages** van verwerkers beoordeeld door PCBO (verwerkingsverantwoordelijke).

6 Rollen en verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol.
Het sturen op- en besturen van IBP-beleid is de verantwoordelijkheid van het bestuur en in uitvoer toebedeeld aan IBP-teamleden welke op basis van rollen, taken, verantwoordelijkheden en bevoegdheden benoemd zijn. Taken om aan het IBP-beleid te voldoen en blijven voldoen worden geprioriteerd op basis van risicoanalyse. Taken worden gedocumenteerd vastgelegd om eigenaarschap, doorlooptijd en onderlinge samenhang te koppelen aan het volwassenheidsniveau van de organisatie.

Onderstaand schema geeft een overzicht van taken, verantwoordelijkheden en bevoegdheden per rol e/o functie welke horen bij PCBO.

Niveau	**Wie** **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **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 • Communiceren met- en informeren van stakeholders IBP voorafgaande aan veranderingen ten aanzien van IT en verwerking van persoonsgegevens.	• Informatiebeveiligings- en privacy beleid • Actief betrekken van FG bij totstandkoming IBP jaarplan, geplande en ongeplande wijzigingen m.b.t. IBP • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen • Bedrijfscontinuïteitsplan (BCP) vaststellen en frequent testen.
	Privacy Officer (de persoon die namens en in opdracht van de bestuurder IBP belangen inhoudelijk	• IBP-planning en controle • Adviseert bestuur/CvB/directie over IBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse	Processen, richtlijnen en procedures IBP, waaronder: • activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten

	beantwoord) Deze functionaris is operationeel aanspreekpunt intern en extern voor IBP aangelegenheden en vervuld deze taak uit in opdracht en op instructie van het bestuur of bestuurder.	• 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 • Betrokkenheid en actief in contact staan met de organisatie en medewerkers om tijdig IBP activiteiten te signaleren en bij te sturen waar nodig. •	beoordelen en waarborgen • Brief toestemming gebruik beeldmateriaal • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ict en internetgebruik • Gedragscode medewerkers en leerlingen • Responsible Disclosure • GRC beheren en actueel houden •
	Functionaris voor Gegevensbescherming (de FG is een onafhankelijke toezichthouder welke niet in opdracht van- of onder aansturing of regie van de bestuurder gevraagd en ongevraagd advies uitbrengt aan de bestuurder)	• Toezicht op naleving privacy wetgeving • Voorlichting privacy en stimuleren bewustwording • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten • Adviseren en instrueren van de PO op verzoek • Beoordelen van mogelijke rest risico's bij veiligheidsonderzoeken als VO's, DPIA's en rechten van betrokkenen.	• Privacyreglement, • procedure IBP-incident afhandeling • Inrichten meldpunt datalekken •
	Proceseigenaren Waaronder o.a.: ICT, (1e aanspreekpunt bij leverancier is de RolfGroep Functionarissen voor de processen: HRM / P&O, facilitair, onderwijs, financiën, inkoop en administratie (aangesteld door de bestuurder van de onderwijsinstelling)	• **Classificatie / risicoanalyse** in samenwerking met Manager IBP (Informatiemanager / verantwoordelijke IBP / privacy officer) • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur/CvB/directie • 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); input dataregister • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk en daarin verwerkte gegevens.

Uitvoerend (operationeel)		• 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 betrokkenen; 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. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur.	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 •