PCPO
Barendrecht & Ridderkerk

Informatiebeveiligings- en privacy beleid

BESLUIT BESTUURDER	10-11-2025
INSTEMMING GMR	10-12-2025

Inhoud

1. Verantwoording en richtlijnen

1.1 MISSIE/VISIE PCPO BARENDRECHT EN RIDDERKERK OP IBP

PCPO Barendrecht en Ridderkerk wil op haar scholen een veilige werk- en leeromgeving bieden met waarborging van de privacy. Wij zijn transparant en gaan zorgvuldig om met de ons toevertrouwde persoonsgegevens.

Daarnaast zien wij het als een missie om medewerkers en leerlingen bewust en zorgvuldig om te laten gaan met de persoonsgegevens van zichzelf en anderen. Ouders mogen erop vertrouwen dat wij zorgvuldig met de data van hun kind omgaan.

1.2 HET BELANG VAN INFORMATIEBEVEILIGING EN PRIVACY

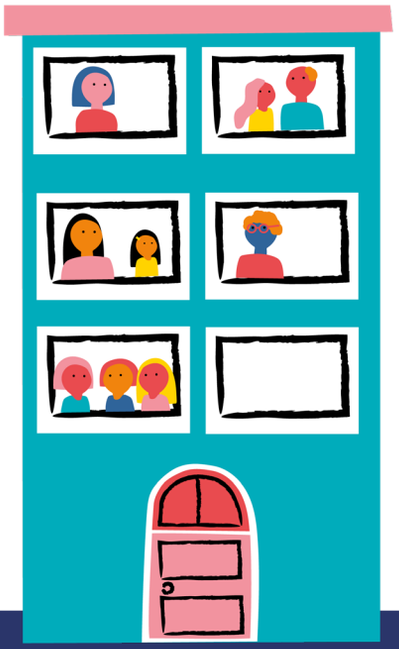
Het onderwijs is in toenemende mate afhankelijk van informatie en ict. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ict en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van **informatiebeveiliging en privacy** (afgekort tot IBP) in een IBP-beleid en de daaraan verbonden afspraken en procedures is voor PCPO Barendrecht en Ridderkerk noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

1.3 TOELICHTING INFORMATIEBEVEILIGING

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van 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 onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.



1.4 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 natuurlijk persoon (een individu die in het recht wordt erkend als drager van rechten en plichten) 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.

1.5 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: Informatiebeveiliging en privacy. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis om IBP binnen PCPO Barendrecht en Ridderkerk te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

2. Verantwoording en richtlijnen

2.1 DOEL

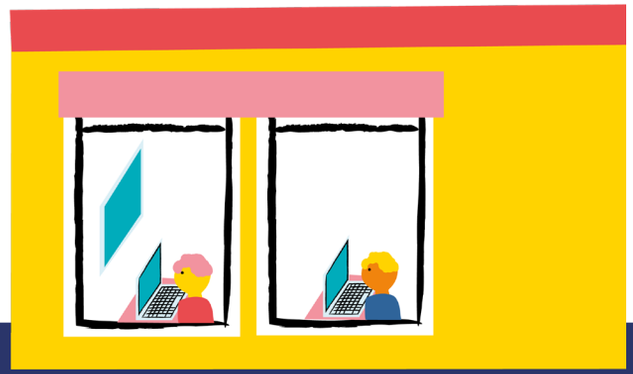
Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan PCPO Barendrecht en Ridderkerk persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.
- Bewustwording vergroten over het belang van zorgvuldig omgaan met informatie, systemen en persoonsgegevens.

Het 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, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en PCPO Barendrecht en Ridderkerk voldoet aan relevante wet- en regelgeving.

2.2 REIKWIJDTE

- Het IBP-beleid binnen PCPO Barendrecht en Ridderkerk geldt voor alle betrokkenen, te weten: medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing).
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van het bestuur van PCPO Barendrecht en Ridderkerk. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd, wordt beheerd. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/ systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van PCPO Barendrecht en Ridderkerk 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.
- IBP-beleid heeft binnen PCPO Barendrecht en Ridderkerk 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 leerlingen, hun ouders/verzorgers en medewerkers.



2.3 CONCRETISERING[1] VAN HET BELEID - HOE DOEN WE DAT?

Het bestuur van PCPO Barendrecht en Ridderkerk hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het bestuur van PCPO Barendrecht en Ridderkerk neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld is. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
2. Het bestuur van PCPO Barendrecht en Ridderkerk voldoet aan alle relevante wet- en regelgeving.
3. Bij PCPO Barendrecht en Ridderkerk 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 het bestuur van PCPO Barendrecht en Ridderkerk 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 op elk moment hun toestemming herzien.
4. PCPO Barendrecht en Ridderkerk zal alle betrokkenen helder en actief informeren over de verwerkingen van de hun 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 van hun persoonsgegevens.
5. PCPO Barendrecht en Ridderkerk legt alle verwerkingen van persoonsgegevens vast in een register voor verwerkingsactiviteiten (het dataregister), en zal deze up-to-date houden. Het bestuur van PCPO Barendrecht en Ridderkerk voldoet hiermee aan de documentatieplicht, zoals benoemd in de AVG.
6. Binnen het bestuur van PCPO Barendrecht en Ridderkerk 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. Het bestuur van PCPO Barendrecht en Ridderkerk is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen mogen geen content downloaden waar intellectuele eigendomsrechten op rusten als er geen licentie door het PCPO Barendrecht en Ridderkerk is afgesloten.
8. PCPO Barendrecht en Ridderkerk 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, de benodigde investeringen en de te nemen maatregelen.
9. PCPO Barendrecht en Ridderkerk sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken.

1. PCPO Barendrecht en Ridderkerk zal aansluiting zoeken bij het Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs, dat in 2023 gelanceerd is door de overheid i.s.m. de sector.

10. Het bestuur van PCPO Barendrecht en Ridderkerk verwacht van alle medewerkers, leerlingen, (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. PCPO Barendrecht en Ridderkerk heeft hiervoor afspraken in de gedragscode IBP geformuleerd, vastgesteld en geïmplementeerd. Hierin staan afspraken over onder andere het computergebruik, applicatiegebruik, opslag (persoons)gegevens, communicatie, digitale veiligheid en het melden van beveiligingsincidenten en datalekken.
11. IBP is bij PCPO Barendrecht en Ridderkerk een continu kwaliteitsproces, waarbij regelmatig (minimaal jaarlijks) op basis van evaluatie, audit of zelf-assessment wordt gekeken of aanpassing gewenst dan wel noodzakelijk is. (zie bijlage 3)
12. PCPO Barendrecht en Ridderkerk kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy. Indien noodzakelijk wordt er een Data Protectie Impact Assessment (DPIA). De uitkomst van de DPIA bepaalt de te nemen aanvullende maatregelen.
13. PCPO Barendrecht en Ridderkerk neemt passende organisatorische en/of technische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren. Afspraken rondom de technische maatregelen zijn vastgelegd in de verwerkersovereenkomst met de externe ICT-dienstverlener.
14. PCPO Barendrecht en Ridderkerk zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en (indien nodig) melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.
15. PCPO Barendrecht en Ridderkerk gaat ten aanzien van informatiebeveiliging (autorisatie en authenticatie) ervan uit dat "Alles is in principe verboden tenzij het uitdrukkelijk is toegelaten" en niet van het uitgangspunt "Alles is in principe toegelaten tenzij het uitdrukkelijk is verboden".

3. 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.

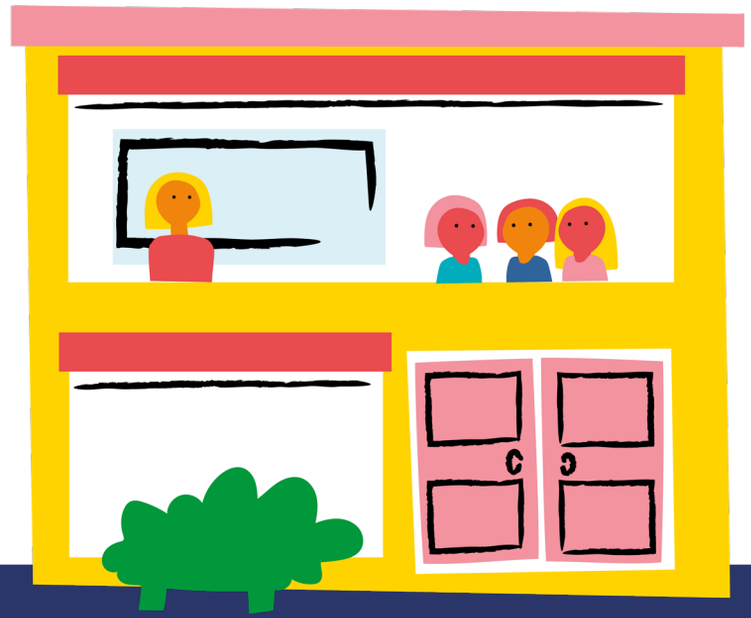
3.1 RELEVANTE WET- EN REGELGEVING

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

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra;
- Wet goed onderwijs en goed bestuur PO/VO;
- Wet onderwijstoezicht;
- Algemene Verordening Gegevensbescherming (AVG);
- Archiefwet;
- Leerplichtwet;
- Auteurswet;
- Wetboek van Strafrecht.

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 is leidend voor de te nemen beveiligingsmaatregelen. Tevens wordt gewerkt volgens het Normenkader IBP. De up-to-date kaders zijn te vinden op de website van Kennisnet: https://normenkaderibp.kennisnet.nl/

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' (terug te vinden op https://www.privacyconvenant.nl/over/) zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.



3.2 BASISREGELS BIJ HET OMGAAN MET PERSOONSGEGEVENS

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake 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 (toestemming, uitvoering van een overeenkomst, wettelijke verplichting, vitaal belang, algemeen belang en 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 tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiair). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk. (zie Toegang - Opschoon - Toezicht beleid PCPO)
4. **Transparantie:** de school legt aan betrokkenen (leerlingen, hun ouders/verzorgers en medewerkers) op transparante manier verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Het geven van deze informatie vindt ongevraagd plaats. Daarnaast hebben betrokkenen recht op inzage, verbetering, aanvulling, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit, afscherming en profilering 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 volledig, juist en actueel zijn.

3.3 ONDERSTEUNENDE BELEIDSAFSPRAKEN EN PROCEDURES

Diverse aanvullende beleidsafspraken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de diverse aanvullende documenten. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

3.4 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 e-learning en bewustwordingscampagnes voor medewerkers en leerlingen.

Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de directeuren, Privacy Officer (PO) en Functionaris Gegevensbescherming (FG), met het bestuur als eindverantwoordelijke.

3.5 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 kwaliteitscriteria 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. Op basis van de uitkomst van een centraal ingeregelde DPIA (Data Protection Impact Assessment) worden vervolgens passende maatregelen genomen. Vanaf de start van nieuwe (ict)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

3.6 INCIDENTEN EN DATALEKKEN

Alle medewerkers en leerlingen, 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 aangegeven via de meldknop op het intranet of op privacy@pcpobr.nl. Deze incidenten worden besproken met de Functionaris Gegevensbescherming van PrivacyopSchool. (zie Protocol informatiebeveiligingsincidenten en datalekken)

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

Ondanks onze zorg om alle systemen goed te beveiligen kan het voorkomen dat een zwakke plek wordt ontdekt. Van deze kwetsbaarheden kan melding worden gemaakt op basis van het Responsible Disclosure beleid.

3.7 PLANNING EN CONTROLE

Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten PCPO Barendrecht en Ridderkerk maken het noodzakelijk om periodiek te controleren of het beleid nog voldoet aan de eisen. Dit IBP-beleid wordt minimaal elke drie jaar getoetst en indien nodig door het bestuur bijgesteld. Hierbij wordt rekening gehouden met:

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

PCPO Barendrecht en Ridderkerk kent tevens een jaarlijkse verbetercyclus voor IBP. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het IBP-beleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen. Het resultaat hiervan wordt vastgelegd in een jaarplan IBP. Er is nu een IBP-planning om te voldoen aan het normenkader, deze zal daarna omvormen tot een jaarplan IBP.

3.8 NALEVING EN SANCTIES

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid, richtlijnen en procedures.

Naleving van het IBP-beleid is een primaire verantwoordelijkheid van alle medewerkers binnen PCPO Barendrecht en Ridderkerk. Daarnaast nemen leidinggevenden en proceseigenaren hun verantwoordelijkheid om medewerkers aan te spreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een gedragscode, met periodieke bewustwordingscampagnes, etc.

Voor toezicht op de naleving van de AVG vervult de Functionaris Gegevensbescherming (FG) een belangrijke rol. De FG wordt 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 het bestuur van PCPO Barendrecht en Ridderkerk de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

3.9 LOGGING EN MONITORING

Logging en monitoring door de ICT-afdeling of externe ICT-dienstverlener zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens worden vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk. PCPO Barendrecht en Ridderkerk zal deze logging regelmatig opvragen en beoordelen.

4. Governance - wie doet wat?

4.1 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. Voor een optimaal IBP beleid moet dit goed ingeregeld zijn, met andere woorden de governance moet op orde zijn.

Het bestuur van PCPO Barendrecht en Ridderkerk hanteert het three lines of defence model (3LoD).

De eerste lijn binnen dit model is cruciaal. Hierin is vastgelegd dat directeuren en management toezien op het verantwoord omgaan met persoonsgegevens. Hiervoor zijn alle directeuren en management geschoold en zien zij erop toe dat al hun teamleden handelen volgens het vastgestelde IBP beleid en de daarbij behorende afspraken en procedures.

De tweede lijn ondersteunt de 1e lijn en adviseert, coördineert en bewaakt of het centraal management team hun verantwoordelijkheden ook daadwerkelijk neemt. Daarnaast zijn bepaalde beleidsvoorbereidende taken en het organiseren van integrale risicoanalyses taken van de tweede lijn.

De derde lijn controleert en beoordeelt de effectieve werking van de tweede lijn en eerste lijn en geeft daarover een objectief, onafhankelijk oordeel met mogelijkheden tot verbetering. Het bestuur is als verwerkingsverantwoordelijke eindverantwoordelijk voor het beschermen van de privacy van alle betrokkenen.

4.2 DE FIRST LINE OF DEFENCE IS PRIMAIR VERANTWOORDELIJK

Hieronder vallen de directeuren en management, functioneel beheer en/of applicatiebeheer en de verschillende proceseigenaren. Onder het management verstaan we: hoofd Bedrijfsvoering, hoofd Personeel en Organisatie, hoofd Onderwijs, Kwaliteit en Innovatie.

De eerste lijn bewaakt het IBP-beleid binnen hun eigen organisatorische onderdeel. Zij vormen de first line of defence als het gaat om de bescherming van persoonsgegevens. Zij voeren de daarbij horende operationele taken uit op basis van het door de tweede lijn ontwikkelde beleid en daarbij behorende richtlijnen en procedures, zoals:

- toetsen dat er geen andere verwerkingen plaatsvinden dan die zijn vastgelegd in de registers voor verwerkingen; de dataregisters voor leerlingen, medewerkers en relaties;
- toetsen op het afsluiten van verwerkersovereenkomsten of privacyregelingen, als persoonsgegevens worden overgedragen aan externe partijen;
- signaleren en beoordelen van incidenten waarbij persoonsgegevens betrokken zijn en het intern melden daarvan als het vermoeden bestaat dat het gaat om een datalek.

Directeuren en management voeren bovendien de volgende operationele taken uit:

- toetsen dat hun medewerkers voldoende zijn geschoold in het kader van de AVG;
- vastleggen van de extra taken en rollen van medewerkers en de daarbij behorende rechten binnen de bijbehorende systemen/processen.

4.3 DE SECOND LINE OF DEFENCE: HET BESTUUR EN DE (BOVENSCHOOLSE) PRIVACY OFFICER

Het bestuur en de (bovenschoolse) IBP-verantwooordelijke werken samen binnen de second line of defence als het gaat om de bescherming van persoonsgegevens. De tweede lijn:

- ontwikkelt waar nodig beleid op het gebied van informatiebeveiliging en privacy. Het bestuur stelt het voorgenomen beleid vast;
- monitort en evalueert de toepassing en naleving van het informatiebeveiligings- en privacybeleid en de daaraan gekoppelde afspraken en procedures;
- adviseert over informatiebeveiliging en privacybescherming;
- ondersteunt de eerste lijn bij het identificeren en bewaken van risico's.

4.4 DE THIRD LINE OF DEFENCE: FUNCTIONARIS GEGEVENSBESCHERMING (FG) ALS INTERNE AUDITOR

PCPO Barendrecht en Ridderkerk heeft een interne toezichthouder op de verwerking van persoonsgegevens aangesteld, de FG. De FG zal door PCPO Barendrecht en Ridderkerk tijdig worden betrokken bij alle aangelegenheden waar persoonsgegevens bij komen kijken.

De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. PCPO Barendrecht en Ridderkerk heeft de FG aangemeld bij de Autoriteit Persoonsgegevens.

De taken van de FG houden in:

- het informeren en adviseren van alle betrokken partijen over hun verplichtingen onder de AVG;
- het toezien op de naleving van de AVG en andere relevante privacywetgeving;
- het toezien op de naleving van dit IBP-beleid van het bestuur van PCPO Barendrecht en Ridderkerk;
- het toezien op een Data Protection Impact Assessment (DPIA);
- het behandelen van klachten over de toepassing van het privacyreglement;
- het fungeren als eerste aanspreekpunt voor en samenwerken met de Autoriteit Persoonsgegevens.

De taken en bevoegdheden van de FG zijn vastgelegd in het reglement taken en bevoegdheden FG.

4.5 MEDEZEGGENSCHAP

PCPO Barendrecht en Ridderkerk betrekt de gemeenschappelijke medezeggenschapsraad (GMR) bij besluiten over regelingen en procedures ten aanzien van de bescherming van persoonsgegevens. Het bestuur is eindverantwoordelijk voor het informeren van de GMR.

Deze regeling is vastgelegd in het 'Medezeggenschapsreglement Gemeenschappelijke Medezeggenschapsraad (GMR)'. Vastgesteld op 11 december 2023.

4.6 IMPLEMENTATIE BELEID

Het bestuur van PCPO Barendrecht en Ridderkerk is verantwoordelijk voor verwerkingen van persoonsgegevens waarvoor zij het doel en de middelen vaststelt. Als verwerkingsverantwoordelijke in de zin van de AVG houdt de verantwoordelijkheid kort samengevat in dat :

- persoonsgegevens worden alleen verwerkt in overeenstemming met de vastgestelde doelen voor de verwerking. Deze doelen moeten gerechtvaardigd zijn en de verwerking moet zorgvuldig gebeuren;
- hierover aantoonbaar verantwoording kan worden afgelegd aan de Autoriteit Persoonsgegevens.

De feitelijke verwerking van persoonsgegevens wordt op verschillende lagen binnen PCPO Barendrecht en Ridderkerk uitgevoerd. Er is een onderscheid tussen centrale verwerkingen, waarvoor het bestuursbureau verantwoordelijk is en decentrale verwerkingen, waarvoor organisatieonderdelen of locaties verantwoordelijk zijn. Echter, in alle gevallen behoudt het bestuur als verantwoordelijke in de zin van de AVG, de eindverantwoordelijkheid voor de zorgvuldige verwerking van persoonsgegevens binnen de gehele organisatie.

4.7 VERDELING VAN DE VERANTWOORDELIJKHEDEN

Het bestuur van PCPO Barendrecht en Ridderkerk onderscheidt een aantal verwerkingen van persoonsgegevens met daarbij benoemde proceseigenaar:

- Degene die de leerlingadministratie verzorgt, is als proceseigenaar verantwoordelijk voor de verwerkingen van persoonsgegevens van alle leerlingen die bij PCPO Barendrecht en Ridderkerk onderwijs volgen. De leerlingadministratie wordt bijgehouden op schoolniveau. De directeur is daarmee eindverantwoordelijk voor de leerlingadministratie. Het register van verwerkingsactiviteiten wordt centraalbijgehouden door de Privacy Officer. Periodiek vindt er een controle plaats door Privacy Officer en proceseigenaar.
- Degene die de personeelsadministratie verzorgt, is als proceseigenaar verantwoordelijk voor de verwerkingen van persoonsgegevens van alle medewerkers die in opdracht van het bestuur van PCPO Barendrecht en Ridderkerk, zowel centraal als decentraal, werk verrichten. Hoofd personeel en organisatie is eindverantwoordelijk voor de personeelsadministratie. Het register van verwerkingen wordt centraal bijgehouden door de Privacy Officer. Periodiek vindt er een controle plaats door Privacy Officer en proceseigenaar.
- Diegenen die de PR en communicatie verzorgen voor hun afdeling zijn als proceseigenaar verantwoordelijk voor de verwerkingen van persoonsgegevens van alle mensen waarmee het bestuur van PCPO Barendrecht en Ridderkerk centraal een relatie onderhoudt. Dit kunnen zijn belangstellenden, sollicitanten, oud-werknemers, contactpersonen van de stage-verlenende organisaties, leveranciers en alumni. De directeur van die betreffende afdeling is hiervoo eindverantwoordelijk. Het register van verwerkingen wordt centraal bijgehouden door de Privacy Officer. Periodiek vindt er een controle plaats door Privacy Officer en proceseigenaar.

Deze toewijzing van verantwoordelijkheden houdt ook in dat elke directeur die buiten de genoemde afdelingen om andere categorieën persoonsgegevens verwerkt dan zijn vastgelegd in de verwerkingsregisters, zélf verantwoordelijk is voor die aanvullende persoonsgegevens. Zij moeten deze verwerkingen melden bij de Privacy Officer en documenteren.

4.8 AFSTEMMING OP VERSCHILLENDE NIVEAUS

Het is belangrijk dat de samenhang met betrekking tot de bescherming van (persoons)gegevens voor iedereen duidelijk is. Op die manier kunnen initiatieven en activiteiten op het gebied van verwerking van persoonsgegevens binnen de verschillende afdelingen op elkaar worden afgestemd. Hiervoor is gestructureerd overleg over het onderwerp privacy op alle niveaus van belang.

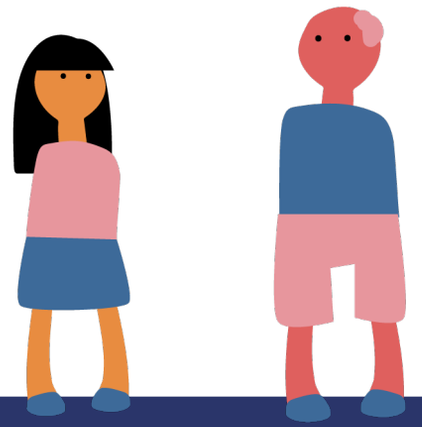
- Binnen het centraal management teamoverleg (CMT) wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van privacyaspecten.
- Het directeuren beraad (DB) buigt zich over plannen, te hanteren normen, en evaluatiemethoden. Deze plannen en normen zijn sturend voor de uitvoering.
- Op operationeel niveau worden de onderwerpen besproken die de dagelijkse bedrijfsvoering aangaan. Het operationeel niveau wordt ingevuld door het teamoverleg.

4.9 CONTROLE EN NALEVING

Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit. De FG initieert met de tweede lijn de controle op het rechtmatig en zorgvuldig verwerken van persoonsgegevens.

Eventuele externe controles worden uitgevoerd door onafhankelijke accountants. Deze externe controles worden gepland en geformuleerd in overleg met de FG van PCPO Barendrecht en Ridderkerk.

Het verwerken van persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten PCPO Barendrecht en Ridderkerk maken het noodzakelijk om periodiek te bezien of het beleid nog voldoet.



Bijlage I: Uitwerking hoofdstuk 2.3

Deze bijlage bevat de uitwerking van hoofdstuk 2.3 en de verwijzing naar onderliggende documenten.

	IBP beleid 2.3 Concretisering	PCPO Barendrecht en Ridderkerk document
1	Bestuur, verwerkingsverantwoordelijke	IBP-beleid PCPO Barendrecht en Ridderkerk, hoofdstuk 3
2	Relevante wet- en regelgeving	IBP-beleid PCPO Barendrecht en Ridderkerk, hoofdstuk 2
3	Specifiek doel en wettelijke grondslag	Register voor verwerkingsactiviteiten (Verwerkingsregisters) Toestemmingsverklaring
4	Betrokkenen helder en actief informeren	Privacy verklaring voor leerlingen en medewerkers Privacyreglement leerlingen PCPO Barendrecht en Ridderkerk
5	Verwerkingen van persoonsgegevens (dataregisters)	Verwerkingsregisters medewerkers Verwerkingsregisters leerlingen Verwerkingsregisters relaties
6	Veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen	Privacyreglement medewerkers Privacyreglement leerlingen
7	Eigendom toebehoort aan derden	Gedragscode
8	Classificeren informatie en informatiesystemen	BIV classificatie in dataregisters
9	Leveranciers van digitale onderwijsmiddelen	Laatste versie Model verwerkersovereenkomsten
10	Medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties gedragen zich ‘fatsoenlijk’	gedragsregels leerlingen PCPO Barendrecht en Ridderkerk Gedragscode veilig gebruik ict-middelen en persoonsgegevens
11	Informatiebeveiliging en privacy is een continu kwaliteitsproces	Toetsingskader IBP 4.0 gebaseerd op ISO27001/2 en AVG
12	Wijzigingen en aanschaf van nieuwe (informatie)systemen	Privacy by design/default Data Protection Impact Assessment (DPIA)
13	Passende organisatorische of technische (beveiligings-) maatregelen	DPIA, deel 2 Toetsingskader IBP 4.0
14	Beveiligingsincidenten en datalekken	Beleid datalekken PCPO Barendrecht en Ridderkerk Responsible disclosure
15	Autorisatie en authenticatie	Autorisatie- en authenticatiebeleid PCPO Barendrecht en Ridderkerk

Bijlage 2: Aanvullende documenten en richtlijnen

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming (AVG) verplicht.

IBP beleid 2.3 Concretisering		Verplichte verantwoording vanuit de AVG	
Procedure toestemming gebruik beeldmateriaal	Richtlijn voor gebruik en toestemming beeldmateriaal	Procesbeschrijving melden datalekken	Protocol informatie-beveiligingsincidenten en datalekken
Procedure voor verwijderen van gegevens	Toegang - toezicht - opschoonbeleid	Registratie beveiligingsincidenten	YourSafetyNet
Procedure rondom training medewerkers		Register voor verwerkingsactiviteiten (Dataregister)	YourSafetyNet
Communicatie rechten betrokkenen	Protocol uitoefening privacyrechten betrokkenen	Verwerkersovereenkomsten	YourSafetyNet
Procedure uitvoeren rechten betrokkenen	Protocol uitoefening privacyrechten betrokkenen	Procedure Gegevensbeschermings-effectbeoordeling DPIA	Protocol Aanpak Proces-DPIA
Privacyreglement (*leerlingen en **medewerkers)	Privacyreglement	Risicoanalyse	
Privacyverklaring	Privacyverklaring leerlingen en ouders/ verzorgers	Functionaris Gegevensbescherming	Reglement taken en bevoegdheden Functionaris Gegevensbescherming
Autorisatiebeleid en Autorisatiematrices	Toegang - toezicht - opschoonbeleid		
Beleid fysieke toegang			
Cameratoezicht	n.v.t.		
Wachtwoordbeleid	Gedragscode verantwoord gebruik bedrijfsmiddelen medewerkers		
Responsible disclosure			
Gedragscode veilig gebruik ict-middelen en persoonsgegevens	Gedragscode verantwoord gebruik bedrijfsmiddelen medewerkers		
Procedure rondom uitwisselen gegevens	Regeling uitwisseling persoonsgegevens		
Handreiking bewaartermijnen	Handreiking bewaartermijnen		
Geheimhoudingsverklaring			

Bijlage 3: Taken van medewerkers

Onderstaand overzicht geeft de relaties tussen de three lines of defence aan bij een aantal AVG-gerelateerde onderwerpen.

Onderwerp	Verantwoordelijk voor	Rol/functie
Privacyreglement	Opstellen	Privacy Officer
	Vaststellen	Bestuurder en GMR
	Communicatie met ouders/verzorgers	Directeur
	Toetst kwaliteit en werking goedgekeurde reglement	Functionaris Gegevensbescherming
Gebruik beeldmateriaal en online diensten	Opstellen toestemmingsformulieren	Privacy Officer
	Toestemming vragen aan ouders/verzorgers en registreren	Directeur
	Toetst werking procedure toestemming	Functionaris Gegevensbescherming
Uitwisseling persoonsgegevens	Bepalen met welke partijen persoonsgegevens uitgewisseld mogen worden en op welke wijze.	Privacy Officer
	Toestemming vragen aan ouders/verzorgers en registreren	Intern Begeleider Kwaliteitscoördinator
	Toetst werking procedure uitwisseling persoonsgegevens	Functionaris Gegevensbescherming
IBP-beleid	Opstellen IBP-beleid	Privacy Officer
	Vaststellen	Bestuurder en GMR
	Communicatie naar medewerkers	Directeur
	Training bewustwording IBP medewerkers	Directeur
	Toetst kwaliteit en werking goedgekeurde beleid	Functionaris Gegevensbescherming
Gedragscode	Opstellen gedragscode	Privacy Officer
	Vaststellen	Bestuurder en GMR
	Bewustwording en toezien op naleving gedragscode en toepassing handboek	Directeur
	Toepassen gedragscode	Medewerkers
	Opstellen en toepassen protocol sociale media en ICT voor leerlingen	Directeur
	Toetst kwaliteit en werking goedgekeurde gedragscode	Functionaris Gegevensbescherming

Onderwerp	Verantwoordelijk voor	Rol/functie
Document- en datamanagement	Toepassen van technische beveiligingsmaatregelen (backup, encryptie, etc.)	Bovenschoolse ICT-er Externe partij: Cloudwise
	Vaststellen bewaarplaatsen	Directeur/Intern Begeleider / Kwaliteitscoördinator
	Vaststellen bewaartermijnen	Bestuurder
	Vernietiging persoonsgegevens conform bewaartermijnen	Directeur
	Toetst naleving bewaartermijnen	Functionaris Gegevensbescherming
Toegangsbeleid	Vaststellen autorisatie / autorisatiematrix	Privacy Officer
	Verstrekken en intrekken accounts conform autorisatiematrixen	Directie en bestuurder (voor staf)
	Toepassen technische beveiligingsmaatregelen (o.a. automatisch vernieuwen en sterkte wachtwoord)	Beleidsmedewerker ICT Externe partij: Cloudwise
	Doorvoeren autorisaties in systemen	functioneel beheerder
	Toetst naleving en werking toegangsbeleid	Functionaris Gegevensbescherming
Verwerkersovereenkomsten	Doorgeven nieuwe verwerkers (leveranciers) aan bestuurssecretariaat/Privacy Officer	Directeur
	Afsluiten verwerkersovereenkomsten voor meerdere scholen	Bestuurder
	Afsluiten verwerkersovereenkomsten voor individuele scholen	Bestuurder
	Toets verwerkersovereenkomsten op rechtmatigheid en volledigheid	Functionaris Gegevensbescherming
Datalekken	Protocol vaststellen	Bestuurder en GMR
	Datalekken doorgeven aan Meldpunt	Medewerkers (Ontdekkers)
	Verzamelen meldingen en benodigde informatie	Directeur (Meldpunt) i.o.m. Privacy Officer en/of externe ICT-dienstverlener: Cloudwise
	Melden en registreren	Privacy Officer
	Afweging maken tot melding Autoriteit Persoonsgegevens	Functionaris Gegevensbescherming i.o.m. Bestuurder
	Melding maken bij Autoriteit Persoonsgegevens	Functionaris Gegevensbescherming

Onderwerp	Verantwoordelijk voor	Rol/functie
Devices in bruikleen	Afsluiten gebruikersovereenkomst voor devices die in bruikleen worden gegeven.	Directeuren
Handboek IBP	Opstellen en goedkeuren inhoud handboek	Directieoverleg
	Controle en toezicht op toepassing handboek	Bestuurder, stafhoofden en directeuren
	Toetst naleving en werking handboek	FG
DPIA	Aandragen nieuw ICT-project	Directeuren
	Op basis van pré-DPIA wel/geen DPIA	Privacy Officer en Functionaris Gegevensbescherming
	Uitvoeren DPIA	Privacy Officer en vertegenwoordiging gebruikers
	Advies	Functionaris Gegevensbescherming
Rechten betrokkenen	Aanvraag verzoek	Privacy Officer
	Ondersteuning afhandeling	Directeuren
	Toetst naleving procedure rechten betrokkenen	Functionaris Gegevensbescherming
Vastlegging verwerkingen (dataregister)	Vastlegging verwerkingen persoonsgegevens conform artikel 30 AVG	Directeuren, Privacy Officer
	Adviseert en controleert op volledigheid	Privacy Officer
	Toetst of vastlegging voldoet aan wet- en regelgeving	Functionaris Gegevensbescherming