Petrus Canisius College

IBP-beleidsplan

Petrus Canisius College

Document			IBP-beleidsplan
Kenmerk			24/6144c
Bespreking in cdo			9 september 2024
Voorlopig vastgesteld door college van bestuur			
Mr	✓ instemming	☐ advies	18 november 2024
Rvt	☐ goedkeuring	☐ bespreking	
Vaststelling door college van bestuur			18 november 2024

INHOUD

Inleiding

De onderwijsorganisatie is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. Ook neemt de hoeveelheid informatie toe door ontwikkelingen als gepersonaliseerd leren met ICT. Deze afhankelijkheid van ICT en gegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het is van belang om adequate maatregelen te nemen op het gebied van informatiebeveiliging en privacy (IBP) 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. Daarom is het PCC gestart met het ontwikkelen en implementeren van een informatiebeveiligings- en privacy beleid.

Toelichting informatiebeveiliging
Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteit (en veiligheid) van de informatievoorziening te garanderen. Hierbij worden drie kwaliteitsaspecten onderscheiden:

1. Beschikbaarheid — de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten
2. Integriteit — de mate waarin gegevens en/of functionaliteiten juist en volledig zijn
3. Vertrouwelijkheid — de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn

Onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades, imagoverlies en een dalend leerlingaantal.

Toelichting privacy
Privacy gaat onder andere over de bescherming van persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die herleidbaar zijn tot een bepaald individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. De Algemene Verordening Gegevensbescherming (AVG, 2018) 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.*

Vervlechting informatiebeveiliging en privacy
Uit voorgaande blijkt dat informatiebeveiliging een belangrijk onderdeel is van privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar, en zijn van elkaar afhankelijk. Het onderwerp informatiebeveiliging en privacy wordt afgekort tot IBP. Dit beleid, verder te benoemen als het IBP-beleid, ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen het PCC en vormt de kapstok voor de onderliggende afspraken en procedures.

Doel en reikwijdte

Doel
Het informatiebeveiligings- en privacy beleid heeft als doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering
- Het garanderen van de privacy van alle betrokkenen waarvan het PCC persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers
- Het voorkomen van beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan beperken

Het beleid is erop gericht om de kwaliteit en beveiliging van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren met een goede balans tussen privacy, functionaliteit en veiligheid. De uitgangspunten van het beleid zijn dat de persoonlijke levenssfeer van de betrokkene, met name van medewerkers en leerlingen, wordt gerespecteerd en dat het PCC voldoet aan relevante wet- en regelgeving.

Reikwijdte

- Het informatiebeveiligings- en privacy beleid van het PCC geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/ outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices waarmee geautoriseerde toegang tot het schoolnetwerk kan worden verkregen.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van het PCC. Het beleid heeft zowel betrekking op gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd, als op niet-gecontroleerde informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies of op (persoonlijke pagina's van) websites.
- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van het PCC, evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het 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.
- Het IBP-beleid van het PCC heeft raakvlakken met:
  - Algemeen veiligheids- en toegangsbeveiligingsbeleid – met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen (integraal veiligheidsplan, calamiteitenplan PCC);
  - Personeels- en organisatiebeleid – met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties;
  - ICT-beleid – met als aandachtspunten aanschaf, beheer en gebruik van ICT-infrastructuur, devices van leerlingen, docenten en overig personeel;
  - Onderwijsbeleid – met als aandachtspunten:
    - Beleid inzake aanschaf en gebruik van digitale leeromgeving, digitale leermiddelen;
    - Toets- en examenbeleid, voorkomen van fraude;
    - Medezeggenschap van leerlingen, hun ouders/verzorgers en medewerkers;
  - Professionaliseringsbeleid – met als aandachtspunten:
    - Digitaal-didactische vaardigheden en mediawijsheid onderwijzend personeel;
    - ICT-vaardigheden en mediawijsheid ondersteunend personeel.

Uitgangspunten

Algemene beleidsuitgangspunten
De belangrijkste beleidsuitgangspunten bij het PCC zijn:

- Het bestuur van het PCC neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy gewaarborgd worden binnen de organisatie. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
- De verwerking van persoonsgegevens is altijd gekoppeld aan een specifiek doel op één van de wettelijke grondslagen, waarbij een goede balans tussen het belang van het PCC om persoonsgegevens te verwerken en het belang van iedere betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen te allen tijde hun toestemming herzien.
- Het PCC zal alle betrokkenen in heldere taal en actief informeren over de verwerkingen van 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.
- Het PCC legt alle verwerkingen van persoonsgegevens vast in een verwerkingsregister en zal deze up-to-date houden. Het PCC voldoet hiermee aan de documentatieplicht.
- Binnen het PCC 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 fysieke documenten.
- De school is als rechtspersoon verantwoordelijk voor de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen worden goed geïnformeerd over de regelgeving rond het gebruik van informatie.
- Het PCC classificeert informatie en informatiesystemen. De classificatie is het uitgangpunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken enerzijds en de benodigde investeringen en de te nemen maatregelen anderzijds.
- Door middel van een overeenkomst worden er met partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken gemaakt over informatiebeveiliging en privacy.
- Persoonsgegevens worden door het PCC of haar verwerkers in principe niet buiten de EU/EER verwerkt. Indien dit het geval is, dan dragen wij er zorg voor dat de persoonsgegevens adequaat worden beschermd.
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich naar behoren en verantwoord gedragen. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Het PCC heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
- Informatiebeveiliging en privacy is bij het PCC een continu proces, dat regelmatig (minimaal jaarlijks) wordt geëvalueerd en waar nodig aangepast.
- Bij wijzigingen in de infrastructuur of de aanschaf en inrichting van nieuwe (informatie)systemen, kijkt het PCC vooraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.
- Het PCC neemt passende 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.
- Het PCC zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij het PCC 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 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 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.
4.	Transparantie	De school 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.

Wet- en regelgeving

Een uitgebreid overzicht van alle wet- en regelgeving is te vinden in Bijlage 3 bij dit Beleidsplan.

3.1 Ondersteunende richtlijnen en procedures
Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 2 geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

3.2 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 bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP, de FG, en de Security Officer met het bestuur als eindverantwoordelijke.

3.3 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 betrouwbaarheidsaspecten die van belang zijn.

3.4 Incidenten en datalekken
Alle medewerkers, 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 gemeld bij ibp@pcc.nu.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig worden aanvullende passende beleidsmaatregelen genomen.

3.5 Planning en controle
Binnen het PCC wordt veel belang gehecht aan risicomanagement; risicomanagement is dan ook een integraal onderdeel van de diverse bedrijfsprocessen. Door het uitvoeren van periodieke risicoassessments per bedrijfsonderdeel, overkoepelend en bij relevante in- en externe veranderingen wordt inzicht verkregen op de relevante risico's. Voor deze risico's wordt een keuze gemaakt uit de risicostrategie per risico. De gedefinieerde risicostrategieën zijn als volgt:

1. Accepteren – dit houdt in dat een risico als aanvaardbaar wordt gezien en er wordt dus geen actie op ondernomen;
2. Mitigeren – dit betekent verminderen van het risico door beleidsmaatregelen te nemen;
3. Vermijden – dit betekent beleidsmaatregelen nemen die ervoor zorgen dat een risico niet plaatsvindt;
4. Overdragen – dit betekent dat (het vermijden of oplossen van) een risico bij een ander wordt neergelegd.

Voor alle risico's die door PCC als 'hoog' of 'extreem' worden geclassificeerd dient een risicobehandelplan opgesteld te worden, bij Risico's geïdentificeerd als 'gemiddeld' of 'laag' is dit niet verplicht. Elke leidinggevende is verantwoordelijk voor het risicomanagement binnen zijn

verantwoordelijkheidsgebied om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie(middelen) te waarborgen.

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door het bestuur. 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.
Daarnaast kent het PCC een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

3.6 Naleving en sancties
De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met periodieke bewustwordingscampagnes, et cetera.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de 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 PCC de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

3.7 Logging en monitoring
Logging en monitoring door de IT-afdeling zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

Organisatie

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.
Dit hoofdstuk beschrijft hoe IBP in het PCC is georganiseerd. Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken wordt bij het PCC een aantal rollen onderkend op de verschillende organisatieniveaus (richtinggevend, sturend en uitvoerend); deze rollen worden belegd bij medewerkers in de staande organisatie. Voor elk niveau en voor elke rol worden de bijbehorende verantwoordelijkheden en taken beschreven (zie bijlage 1).
Op het PCC is een Kernteam IBP van drie personen die een aantal van de sturende en uitvoerende rollen in samenwerking bekleden en de dagelijkse gang van zaken verzorgen. In formele zin zijn de drie rollen wel belegd: er is een Manager IBP, een Privacy Officer en een Information Security Officer.

Richtinggevende rol

Eindverantwoordelijke

Het College van Bestuur is eindverantwoordelijk voor IBP en stelt – in overleg met de directeuren – het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast. De toepassing en werking van het IBP-beleid wordt op basis van rapportages geëvalueerd. De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de manager IBP.

Sturende rol

Manager IBP

Manager IBP is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen aan op uitvoerend niveau. De manager IBP moet:

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

Portefeuillehouder ICT

Adviseert samen met de manager IBP en de Security Officer de eindverantwoordelijke en is – mede namens de collega-directeuren – verantwoordelijk voor de naleving van het IBP-beleid in de primaire processen van het PCC.

Functionaris gegevensbescherming

Houdt toezicht op de naleving van wet- en regelgeving, alsmede naleving van het privacyreglement, adviseert het bestuur ten aanzien van privacy-aangelegenheden en het uitvoeren van een DPIA en fungeert daarnaast als centraal meldpunt voor vragen en klachten over het privacybeleid.

Uitvoerende rol

Privacy Officer

De Privacy Officer (PO) houdt binnen het PCC – gevraagd en ongevraagd – toezicht op de toepassing en naleving van de AVG. De PO zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten en is de contactpersoon voor klachten en vragen van betrokkenen. PO rapporteert aan de manager IBP. De PO treedt namens het PCC op als contactpersoon voor de Autoriteit Persoonsgegevens

Information Security Officer
De Information Security Officer (ISO) vormt het technisch aanspreekpunt inzake informatiebeveiliging voor het management en de medewerkers. De ISO rapporteert aan de manager IBP.

Overige betrokkenen
Proceseigenaren Magister, Zermelo, AFAS, ICT
Het PCC is georganiseerd rond verschillende domeinen/processen, zoals onderwijs verzorgen, toetsen en beoordelen, leerlingadministratie, ICT, personeelszaken, facilitaire- en financiële zaken et cetera. Op elk van deze domeinen/processen is een proceseigenaar verantwoordelijk om – binnen de kaders van het IBP-beleid – te bepalen op welke wijze IBP wordt uitgewerkt in richtlijnen, procedures en instructies. Dit gebeurt in nauw overleg met de Manager IBP.
De proceseigenaar is verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot informatiesystemen. Om deze risico's te verkleinen hebben proceseigenaren de volgende specifieke taken:

- Samen met de eindverantwoordelijke en de Manager IBP stellen zij het beleid voor toegang tot de informatiesystemen vast.
- Samen met het Hoofd ICT zien zij erop toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
- Samen met het Hoofd ICT beoordelen zij regelmatig de toegangsrechten van gebruikers.

Leidinggevenden (directeuren, afdelingsleiders, hoofd bestuursbureau)
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende 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 IBP-onderwerpen waar het personeel mee te maken heeft.

Op het gebied van informatiebeveiliging en privacy hebben leidinggevenden een belangrijke voorbeeldfunctie voor hun medewerkers.

Communication Officer
De Communication Officer (CO) verzorgt de interne en externe communicatie, ook bij incidenten en calamiteiten op het gebied van informatiebeveiliging. De CO rapporteert aan de manager IBP.

Medewerkers OP en OOP
Elke medewerker heeft verantwoordelijkheden met betrekking tot informatiebeveiliging in zijn of haar dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in diverse documenten, zoals benoemd in bijlage 2 bij dit beleidsplan. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.
Medewerkers worden gestimuleerd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel bij de leidinggevende, of via de personeelsraad of MR).

Stuurgroep
De stuurgroep IBP wordt gevormd door de functionarissen met de belangrijkste rollen op dit terrein: manager IBP, information security officer en privacy officer. Zo gewenst kan in voorkomende gevallen het kernteam worden uitgebreid met de eindverantwoordelijke, communication officer en portefeuillehouder ICT.

Bijlage 1: IBP rollen en taken

Niveau	Rol / Functie	Taakgebied	Specifieke taken	Naam
RICHTING GEVEND	Eindverantwoordelijke / Bestuurder	Eindverantwoordelijk voor IBP	- IBP-beleid vaststellen - Privacyreglement vaststellen	Bestuurder
STUREND	Manager IBP / Hoofd Servicebureau	Inhoudelijk verantwoordelijk voor IBP-PCC (processen, richtlijnen, procedures); IBP-planning en controle; advisering bestuurder. Aansturing Privacy Officer (PO), Information Security Officer (ISO), Communication Officer (CO) en FG Aansturing naleving IBP in de secundaire processen	Processen, richtlijnen, procedures waaronder: - Activiteitenkalender - Privacy reglement - Procedure en protocol IBP incidenten en datalekken - Bewerkersovereenkomst regelen - Brief toestemming gebruik foto's en video - Informatie IBP-beleid voor leerlingen, ouders, verzorgers - Bevordering security awareness - Gedragscodes	Aangewezen functionaris
	Portefeuillehouder ICT Onderwijs / Directeur	Aansturing naleving IBP in het primaire proces Advisering Bestuurder i.o.m. Manager IBP en ISO		Portefeuillehouder vanuit het cdo
	Functionaris gegevensbescherming	Toezicht en advisering	- toezicht houden op de naleving van wet- en regelgeving, alsmede naleving van het privacyreglement; - adviseren van het bestuur ten aanzien van privacy-aangelegenheden; - adviseren van het bestuur inzake het uitvoeren van een DPIA; - fungeren als centraal meldpunt voor vragen en klachten over het privacybeleid.	Extern aangesteld
UITVOEREND	Privacy Officer / Beleidsmedewerker Kwaliteit	Toezicht op naleving privacywetgeving in primaire en secundaire processen Inrichting meldpunt datalekken; afwikkeling van klachten en incidenten i.o.m. Manager IBP		stafmedewerker kwaliteit en onderwijs

	Information Security Officer (ISO) / Hoofd ICT	Technisch aanspreekpunt IBP-incidenten Advisering Bestuurder i.o.m. Manager IBP en ISO		teamleider ICT
	Communication Officer / Communicatieadviseur / Mediacoach	Informatievoorziening IBP voor leerlingen, ouders, medewerkers Bevorderen van mediawijsheid en bewustwording bij leerlingen, ouders, medewerkers		Werkgroep IBP

OVERIGE BETROKKENEN	Proceseigenaren	Classificatie/risicoanalyse Toegangsbeleid Controle toegang	Magister	Johan Dekker
			Zermelo	Johan Dekker
			AFAS – HRM	Gertjan Lommerse
			AFAS – Financieel	Hanneke van Soest
			ICT-infrastructuur	Maurice Filee
	Leidinggevenden	Toezien op naleving IBP binnen eigen afdeling/team	Communicatie naar medewerkers over IBP, regels passend onderwijs, omgang leerlingdossiers, wie mag wat zien, mediawijsheid van leerlingen etc.	Directeuren Afdelingsleiders Hoofd Servicebureau
	Medewerkers	Naleving IBP bij PCC-werkzaamheden (op school en thuis)		allen

Bijlage 2. Protocollen en procedures

In deze bijlage de verwijzingen naar documenten die betrekking hebben op gedrag en procedures, te vinden op Weten en Regelen.

- Protocol Beveiligingsincidenten en datalekken (24 6145, 2024)
- IBP-Privacyreglement voor medewerkers (24 6147a, 2024)
- IBP-Privacyreglement voor leerlingen (24 6146a, 2024)
- IBP-privacyreglement voor leerlingen toegelicht (24 6148a, 2024)
- Privacyverklaring (24 6149a, 2024)
- Privacyverklaring (24 6150, webversie 2024, te vinden via pcc.nu/privacyverklaring)
- Privacystatement over websitegebruik en cookies (24 6151, webversie 2024, te vinden via pcc.nu/privacystatement-websitegebruik)
- Beleid bewaartermijnen (24 6152, 2024) inclusief tabel met termijnen (24 6153, 2024)
- Voorbeeld toestemming AVG Leerlingen ouder dan 16
- Voorbeeld toestemming AVG Ouders
- Integriteitscode (2023)
- Gedragscode (2018)
- Internetgedragscode (2016)
- Gedragscode Seksuele intimidatie et cetera (2023)
- Mailetiquette (2024)
- Inkoopbeleid (2023)
- Klokkenluidersregeling (2023)
- Klachtenregeling (2023)
- Taakomschrijving IBP-Ambassadeur (2024)

Bijlage 3. Relevante wet- en regelgeving

Het PCC voldoet aan alle van toepassing zijnde relevante wet- en regelgeving; te denken valt onder meer aan:

- Wet op het voortgezet onderwijs
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming (AVG)
- CAO
- Wet Passend Onderwijs
- Examens en toetsing (gepubliceerd op Examenblad.nl)

Hiernaast zijn de bepalingen van het convenant 'Digitale onderwijsmiddelen en privacy ' leidend bij het maken van afspraken met leveranciers.

A. Internationaal/Europees

- Artikel 17 van het VN-verdrag voor Burgerlijke en Politieke rechten
- Artikel 8 van het Europees Verdrag voor de Rechten van de Mens
- Artikel 7 Handvest grondrechten van de Europese Unie
- Algemene Verordening Gegevensbescherming (AVG) / General Data Protection Regulation (GDPR)
- Richtlijn Netwerk en informatiebeveiliging (NIB)
- Richtlijn gegevensbescherming politie en justitie
- eIDAS - Europese Verordening e-identity en vertrouwensdiensten
- e-Privacyrichtlijn (wetgeving met betrekking tot o.a. cookies)

B. Landelijk

- Uitvoeringswet AVG
- Artikelen 10 tot en met 13 van de Nederlandse Grondwet
- Algemene wet bestuursrecht (hoofdstuk 5)
- Jaarrekeningrecht: Jaarverslag: verantwoording privacybeleid en security
- Telecommunicatiewet (hoofdstuk 11)
- Wet op de ondernemingsraad (instemmingsrecht)
- Auteurswet
- Jeugdwet
- Wet op de Loonbelasting
- Leerplichtwet
- Wet op het Voortgezet Onderwijs
- Wet op de Expertisecentra
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Wet bescherming persoonsgegevens
- Archiefwet
- Leerplichtwet
- Wetboek van Strafrecht
- CAO
- Wet Passend Onderwijs
- Examens en toetsing (gepubliceerd op Examenblad.nl)

C. Beleid Autoriteit Persoonsgegevens (AP)

De AP heeft diverse richtlijnen gepubliceerd, waaronder:

- Richtsnoeren beveiliging van persoonsgegevens
- Beleidsregels Meldplicht datalekken

- Richtlijnen actieve openbaarmaking persoonsgegevens
- Richtlijnen publicatie persoonsgegevens op internet
- Richtlijnen recht op dataportabiliteit
- Richtlijnen voor functionarissen voor de gegevensbescherming
- Richtlijnen De zieke werknemer
- Richtlijnen kopie identiteitsbewijs.

Hiernaast zijn de bepalingen van het convenant ‘Digitale onderwijsmiddelen en privacy ’ leidend bij het maken van afspraken met leveranciers.