# AVG

**(Alg. Verordening Gegevensbescherming)**

## Inclusief cameratoezicht

# AVG

## (Alg. Verordening Gegevensbescherming)
## Inclusief cameratoezicht


**Status van het beleidsdeel:**

| Status | DO | GMR | Kwaliteitscyclus |
|---|---|---|---|
| 2021-10-21<br>- Toevoeging NAW gegevens FG AVG punt 4<br>- Toevoegen bewaartermijn leerlingengegevens<br>- Placemat toegevoegd<br>- Paar tekstuele aanpassingen | | | |
| Instemming GMR wijzigingen | | 2021-12-13 | |
| 2022-01-11 Aanvullingen beeldbellen en cameratoezicht | 2022-01-18 | | |
| 2023-11-22 NAW gegevens fg-er gewijzigd | | | |
| 2024-03-18 Wijzigingen Cameratoezicht/geluidsopnames | | | |
| 2024-06-05 Aanvullingen n.a.v. GMR 27-05-2024 | | 2024-06-17 | |

TEL (076) 2046300
IBAN NL65 RABO 0125 848625
Email info@pcpomiddenbrabant.nl
Web www.pcpomiddenbrabant.nl

# Inhoudsopgave

## 1. Inleiding

Binnen onze organisatie wordt gewerkt met privacygevoelig materiaal, zoals onder andere leerling- en personeelsgegevens en medische gegevens van leerlingen. De huidige digitale wereld vereist dat we de privacy van elk individu goed bewaken en dat iedereen zelf kan en mag beslissingen welke informatie over hem/haar waar terecht komt. Sinds 25 mei 2018 is dan ook de Europese wet, de Algemene Verordening Gegevensbescherming (AVG) in werking gegaan, waarin strenge wettelijke regels zijn opgenomen. De AVG zorgt ervoor dat bedrijven en instellingen zorgvuldig met persoonsgegevens omgaan.

***Persoonsgegevens zijn al die gegevens die één op één terug te voeren zijn naar een specifiek natuurlijk persoon.***

Om aan de strenge wettelijke regels van de AVG te voldoen zijn er veel aanpassingen nodig, bestaande uit gedragsaspecten en technische aspecten. Bij het realiseren van de *technische aspecten* wordt technische ondersteuning ingekocht die het personeel ondersteunt. Binnen de scholen zijn er ict-vaardige collega's die hun collega's hierbij ondersteunen. Met het *gedragsaspect* wordt het bewustwordingsproces van personeel bedoeld. AVG correct handelen moet gedrag worden van iedereen die met privacy gevoelige gegevens werkt.

ICTRECHT, gespecialiseerd in de AVG wetgeving, heeft bij PCPO de verschillende processen bekeken in relatie tot het ontwikkelde beleid. De verbeterpunten zijn opgenomen in de ontwikkelagenda van dit document.

## 2. Leerlingengegevens

Binnen de PCPO-scholen gaan wij zorgvuldig om met de privacy van onze leerlingen, maar voorop staat het garanderen van de veiligheid van de kinderen. Zo is het werken met groepslijsten voor uitjes/schoolreizen, ontruimingsplannen en het delen van medische gegevens van kinderen die extra alertheid vragen noodzakelijk. Het leerlingontwikkelings- en volgsysteem dat gebruikt wordt op de scholen van PCPO maakt gebruik van alias-en voor de leerlingen. Dit houdt in dat de uitwisseling tussen de educatieve software en Parnassys niet meer op naam van het kind verloopt, maar via een unieke code die niet te koppelen is aan de persoonlijke gegevens van de leerlingen.

### 2.1 Bewaartermijn leerlingengegevens

**Bewaartermijn 5 jaar:**

- Gegevens over verzuim en afwezigheid
- Gegevens over in- en uitschrijving

**Bewaartermijn 3 jaar:**

- Gegevens over een leerling die naar een school voor speciaal onderwijs is doorverwezen.

## 3. Beveiligingsmaatregelen

PCPO heeft diverse beveiligingsmaatregelen getroffen:

### 3.1 Beveiligingsincidenten

PCPO heeft een procedure ingericht om beveiligingsincidenten te signaleren, te beoordelen, en passende opvolging te geven. Beveiligingsincidenten die we kwalificeren als ‘datalek’ worden gemeld aan de Autoriteit Persoonsgegevens en/of aan de betrokkenen. Een van de directieleden van PCPO is eerste aanspreekpunt en registreert de datalekken binnen onze organisatie. Er is een datalekregister waar datalekken worden genoteerd die al dan niet aan de Autoriteit Persoonsgegevens gemeld moeten worden. N.a.v. het datalekregister worden de huidige incidenten onderzocht en worden passende maatregelen genomen.

### 3.2 Data Protection Impact Assessment (DPIA)

Als een nieuwe verwerker privacygevoelige gegevens gaat verwerken en de risico’s van de (nieuwe) verwerking zijn nog niet bekend, dan moet de organisatie, nog voordat de nieuwe verwerking van de persoongegevens start, een DPIA uitvoeren. In het privacybeleid worden de medewerkers geïnformeerd wanneer een DPIA moet worden uitgevoerd. De Functionaris Gegevensbescherming (hierna FG) neemt vervolgens een besluit en start een eventuele procedure op. Momenteel onderzoeken we de invoering van tweeweg verificatie voor nog betere beveiliging van sharepoint en het gebruik van de computers.

### 3.3 Rechten van betrokkenen en informatieplicht

De gegevens die door de school worden verwerkt in het leerlingontwikkel- en volgsysteem Parnassys zijn in te zien. Ook zijn alle personeelsdossiers van de medewerkers van PCPO gedigitaliseerd in AFAS. Alleen daartoe bevoegden, waaronder ook het betreffende personeelslid zelf, kan dit dossier raadplegen. Per 01 januari 2022 maakt AFAS gebruik van tweeweg verificatie via de AFAS Pocket app. De informatieplicht richting de medewerkers en de leerlingen/ouders is beschreven in een apart beleidsdeel, te weten in beleidsdeel gedragscode. Dit document is beschikbaar op Sharepoint.

## 3.4 Cameratoezicht

Op scholen hangen steeds vaker camera's. Bijvoorbeeld om vernielingen of diefstal tegen te gaan. Een camera kan echter zorgen voor inbreuk op de privacy van leerlingen, leerkrachten en bezoekers. Daarom mogen scholen alleen camera's ophangen als zij aan een aantal voorwaarden voldoen. Ook moeten zij ervoor zorgen dat de inbreuk op de privacy zo klein mogelijk is. Een camera in bijvoorbeeld een toilet of kleedhokje gaat te ver, omdat mensen dan bloot in beeld kunnen komen.

### 3.4.1 Gerechtvaardigd belang

Het gerechtvaardigd belang van onze scholen voor het cameratoezicht is de beveiliging van werknemers/scholieren en ten behoeve van het tegengaan van diefstal en/of vernieling. Het toepassen van camera's moet een maatregel zijn die proportioneel goed in verhouding is met de te voorkomen situatie. Het gerechtvaardigd belang dient frequent, minimaal één keer per jaar, opnieuw te worden getoetst.

### 3.4.2 Noodzaak cameratoezicht

Het cameratoezicht moet noodzakelijk zijn. Dat wil zeggen dat de school het doel niet op een andere manier kan bereiken. Is er geen andere mogelijkheid, die minder ingrijpend is voor de privacy? Dat moet de school eerst nagaan. Ook mag het cameratoezicht niet op zichzelf staan. Het moet onderdeel zijn van een totaalpakket aan maatregelen. Het cameratoezicht vindt enkel buiten schooltijden plaats. Zo is de inbreuk op de privacy van werknemers en leerlingen het meest beperkt. Als hiervan moet worden afgeweken, wordt hiervan het gerechtvaardigd belang vooraf op papier afgewogen en met de MR besproken.
De camerabeelden worden niet gebruikt om incidenten tussen leerlingen te beoordelen, tenzij daarover door de directie anders wordt beslist i.v.m. de ernst van de situatie.

### 3.4.3 Cameratoezicht en geluidsopnames

Het is niet toegestaan geluidsopnames te maken, anders dan na vooraf schriftelijke toestemming verkregen te hebben. Zie hiervoor ook 3.5. Beeldbellen.

### 3.4.4 Privacytoets

De school moet, voor het ophangen van camera's, eerst een privacytoets uitvoeren. Dit betekent dat de school de belangen van de leerlingen, leerkrachten en bezoekers afweegt tegen het eigen belang. Ook moet de school de plannen vooraf met de Medezeggenschapsraad bespreken.

### 3.4.5 DPIA Camerabeelden

Zet de school grootschalig en/of systematisch cameratoezicht in ter beveiliging van werknemers/scholieren en ten behoeve van het tegengaan van diefstal en/of vernieling? Dan moet de school een Data Protection Impact Assessment (DPIA) uitvoeren. Dit is bijvoorbeeld zo als de school structureel of gedurende een langere periode cameratoezicht inzet voor dit doel. Verborgen camera's worden binnen PCPO niet ingezet.

### 3.4.6 Rechten leerlingen, leerkrachten en bezoekers

De school moet ervoor zorgen dat de leerlingen, leerkrachten en bezoekers weten dat er een camera hangt en voor welk doel deze er hangt. Bijvoorbeeld door bordjes op te hangen.
Daarnaast geeft de Algemene verordening gegevensbescherming (AVG) de volgende privacyrechten aan betrokkenen:

- het recht om gegevens (camerabeelden) in te zien;
- het recht om vergeten te worden;
- het recht op beperking van de verwerking;
- het recht om bezwaar te maken tegen het gebruik van persoonsgegevens.

### 3.4.7 Bewaartermijn camerabeelden

De school mag de camerabeelden niet langer bewaren dan noodzakelijk is. De richtlijn hiervoor is maximaal 4 weken. Is er een incident vastgelegd, zoals diefstal? Dan mag de school de betreffende beelden bewaren tot dit incident is afgehandeld. Op iedere school wordt bepaald wie verantwoordelijk is voor het tijdig wissen van de beelden. Als bijlage zijn vier documenten opgenomen die specifieke informatie geven over de situatie op de scholen waar camera's worden toegepast.

#### *3.4.7.1 Het wissen van de camerabeelden*

De directie zorgt ervoor dat elke week op een, zelf gekozen, vast moment de beelden van vier weken geleden worden gewist.
Als er een incident heeft plaatsgevonden en de directie is daarover ingelicht, worden die beelden niet na vier weken gewist, maar bewaard totdat de situatie is opgelost.
Als er een korte/lange vakantie is geweest, gaan de vier weken in op de eerstvolgende lesdag.
Bij langdurige afwezigheid van de directie wordt, in overleg met het bestuur, een ander directielid uit het cluster gevraagd om deze taak (tijdelijk) op zich te nemen. Hierover wordt de voorzitter van de MR geïnformeerd.

### 3.4.8 Inzagerecht

Op iedere school is één vast directielid bevoegd om de beelden van de camera's te zien. Er wordt geen inzagerecht verstrekt aan derden, anders dan aan functionarissen van politie of justitie.
Het wachtwoord dat toegang geeft tot de camerabeelden is sterk en wordt met regelmaat vernieuwd.

## 3.5 Beeldbellen

Binnen PCPO wordt gebruik gemaakt van beeldbellen, zowel voor toepassingen tijdens vergaderingen als ook in de klassen en voor dialoog tussen ouders/kinderen en de school, zowel in klassen- als in groeps-individueel verband.
Binnen PCPO wordt gebruik gemaakt van Meet (Google) en TEAMS (Microsoft).

### 3.5.1 Wat gebeurt er met de beelden?

Over het algemeen worden er geen beelden van overleggen of lessen bewaard, c.q. er worden geen sessies opgenomen. Als een presentatie dermate belangrijk is dat deze moet worden opgenomen, wordt dit vooraf aan alle deelnemers medegedeeld en worden alleen de spreker en de presentatie opgenomen. Er worden geen sfeerbeelden van de groep/zaal gemaakt. Bij vergaderingen bestaat de mogelijkheid dat de sessie wordt opgenomen. Dit wordt dan van te voren aan de deelnemers medegedeeld en gebeurt dan alleen voor het samenstellen van de notulen. Na het opstellen en vaststellen van de notulen wordt de opname gewist. Beeldbellen wordt alleen toegepast wanneer fysiek contact niet mogelijk is of wanneer beeldbellen efficiënter is dan fysiek overleg, bijvoorbeeld door het uitsparen van reistijd, of omdat reizen agenda technisch niet haalbaar is.

### 3.5.2 Rol van de MR(en)

De MR-en zijn betrokken bij het kiezen van de software voor beeldbellen of de keuze kwam voort uit een al bestaande mantelovereenkomst met een softwareleverancier (Google en MicroSoft)

### 3.5.3 In beeld komen van persoonlijke zaken

Bij beeldbellen is niet altijd te voorkomen dat er persoonlijke zaken in beeld komen. Het gebruik maken van een kunstmatige achtergrond kan helpend zijn om dit te voorkomen. De pakketten die binnen PCPO gebruikt worden bieden deze mogelijkheid. PCPO is verantwoordelijk voor de wijze waarop beeldbellen wordt gebruikt. Gebruikers dienen hun gesprekspartners te informeren over het feit dat er persoonlijke zaken in beeld komen. Er kan worden besloten dat de camera uit blijft, maar dat kan niet altijd. De

gesprekspartner kan ook worden gevraagd een andere plek te zoeken om het gesprek te voeren, of om de persoonlijke zaken buiten beeld te houden.

### 3.5.4 Datalek

Bedenk dat een datalek of ander incident nooit helemaal uit te sluiten valt, hoe goed alles ook wordt ingericht. Binnen PCPO zijn we hierop voorbereid. Wanneer van toepassing wordt dit ook met de gesprekspartner besproken en worden zij gewezen op deze beperking.

### 3.5.5 Onrechtmatig gebruik beelden

Als medewerkers, leerlingen, ouders of externen vermoeden dat beelden onrechtmatig gebruikt of bekeken worden kunnen zij het volgende trajecten kiezen:

1. **Melden bij de directie**
- kan beoordelen of de melding intern opgelost kan/moet worden of dat de melding elders hoort en adviseert de melder hierover
- noteert de melding in het intern formulier AVG
- het formulier wordt jaarlijks, op initiatief van de directie, doorgesproken met de AVG-er van PCPO.

2. **Melden bij de intern vertrouwenspersoon**
- Als de klachten van persoonlijke aard zijn, kan de IVP bespreken of de melding intern opgelost kan/moet worden of dat de melding elders hoort en adviseert de melder hierover.
- noteert de melding in de eigen vertrouwelijke documenten.
- De IVP-er bespreekt de melding indien nodig binnen het IVP netwerk, of geanonimiseerd met de directie/AVG-er van school, of de AVG-er van PCPO.

3. **AVG-er eigen school** (als dit geen directielid is)
- kan beoordelen of de melding intern opgelost kan/moet worden of dat de melding elders hoort en adviseert de melder hierover
- noteert de melding in het intern **Melden bij de AVG-er van de eigen school** formulier AVG
- het formulier wordt jaarlijks, op initiatief van de directie, doorgesproken met de IVP-er van PCPO.

4. **Melden bij de AVG verantwoordelijke van het bestuur**
- kan beoordelen of de melding intern opgelost kan/moet worden of dat de melding elders hoort en adviseert de melder hierover.
- noteert de melding in het bestuurlijk formulier AVG
- het formulier wordt jaarlijks, op initiatief van de AVG-er, doorgesproken met de FG, of geanonimiseerd met het bestuur.

5. **Melden bij de FG**, Functionaris Gegevensbescherming.
- Meldingen kunnen door de AVG-er van PCPO gedaan worden, of rechtstreeks door melders.
- De FG neemt indien nodig in contact met de AVG-er van het bestuur.
- De FG adviseert de melder / AVG-er van het bestuur
- De FG zorgt, op eigen initiatief, minimaal één keer per jaar voor een geanonimiseerde terugkoppeling met de AVG-er van PCPO en het bestuur.

## 4. Functionaris Gegevensbescherming (FG)

Voor het naleven van de wet AVG en om boetes te voorkomen heeft PCPO een externe Functionaris Gegevensbescherming (FG-er) aangesteld die onafhankelijk functioneert. Zijn contactgegevens zijn:

ICTRecht B.V.
De heer Christopher Cats
Mail: c.cats@ictrecht.nl
Telefoon: 020-6631941

## 5. Verwerkersovereenkomsten

PCPO is verwerkersovereenkomsten met haar verschillende dienstverleners aangegaan, waarin staat wat er aan privacygevoelige informatie wordt uitgewisseld en onder welke voorwaarden en afspraken dat gebeurt. Tot de groep dienstverleners, waarmee een verwerkersovereenkomst wordt afgesloten, behoren ook de voorscholen /peuterspeelzalen, kinderopvangorganisaties en de schoolfotograaf.

### 5.1 Verwerkingsregister

In het volledig ingevulde verwerkingsregister wordt per leverancier exact opgenomen welke gegevens verwerkt worden. Een medewerker van PCPO (naast de FG) is verantwoordelijk voor het bijhouden van het verwerkingsregister.

## 6. Geheimhoudingsverklaringen & VOG's

Met stagiaires en vrijwilligers die binnen onze scholen toegang krijgen tot privacygevoelige informatie is een geheimhoudingsverklaring afgesloten, zodat zij zich ook bewust zijn van hun verplichtingen op dit vlak. Daarnaast is het wettelijk verplicht dat al onze medewerkers een Verklaring Omtrent Gedrag (VOG) hebben. De VOG is belangrijk omdat blijkt dat een werknemer geen strafbare feiten heeft gepleegd die een risico vormen voor de specifieke functie/taak die de werknemer gaat vervullen.

## 7. Bewaartermijnen

In relatie tot het opslaan van persoonsgegevens zijn wettelijke termijnen van toepassing. Deze termijnen zijn verzameld op een A4-tje. Het overzicht staat op Sharepoint in de map 'AVG'. Persoonsgegevens worden na het verstrijken van de bewaartermijn op doeltreffende wijze verwijderd, vernietigd of geanonimiseerd. Het bewaartermijnenbeleid is intern gecommuniceerd en doorgevoerd in de betreffende systemen.

## 8. Bewustwording

Het allergrootste risico op datalekken en fouten bij het verwerken van privacygevoelige informatie vormen wij als mens/functionaris zelf. Ons gedrag en de wijze waarop wij verantwoordelijkheid nemen in ons dagelijks functioneren bepalen de veiligheid van de gegevens waar we mee werken.

Een aantal voorbeelden: vragen/verwerken we altijd alleen maar die gegevens die nodig zijn? Voorbeeld: 'Piet Hendriks uit groep 3 is rechtstreeks terug te voeren tot een persoon, maar 'Piet H uit groep 3' wordt al lastiger, vooral met meerdere 'Pieten' in een klas en 'Piet H' zonder klasaanduiding maakt het terugvoeren naar één leerling al haast onmogelijk. Zo ook met het noteren van geboortedata op een lijst. Een naam met een geboortedatum is heel specifiek: 'Piet Hendriks geboren 23-12-2012'. 'Piet H, 5 jaar oud' beduidend minder. Nog een voorbeeld bij het maken van foto's: denken we na over wat voor foto's we maken in relatie tot het doel van de foto? Een foto van een badjesmiddag met kinderen in zwemkleding op het internet is géén goed idee, een foto van kinderen achter hun zelfgemaakte masker weer wel.

PCPO voert een continue AVG bewustwordingscampagne onder medewerkers, zodat de medewerkers weten hoe om te gaan met bijvoorbeeld wachtwoorden en de beveiliging van persoonsgegevens. In een korte checklist staat vermeld waarop gelet dient te worden bij de verwerking van persoonsgegevens en deze bevat de meest voorkomende verwerkingen binnen de basisscholen. De FG-er draagt ook bij aan meer bewustwording binnen de organisatie. Doordat het voor medewerkers duidelijk is bij wie ze kunnen zijn voor vragen over de AVG, wordt er bewuster omgegaan met privacy. Daarnaast bezoekt de FG-er de scholen ook onverwachts als een 'mystery guest'. Medewerkers weten dan dat ze altijd alert moeten blijven ten aanzien van de gegevensbescherming.

## 9. Intern privacyreglement & gedragscode

PCPO heeft een intern privacyreglement en een actuele gedragscode, die voorschrijft welke regels medewerkers in acht moeten nemen bij het verwerken van persoonsgegevens. Het document dient voor de medewerkers als naslagwerk. Binnen de organisatie is een medewerker verantwoordelijk voor het up-to-date houden van het document.

## 10. Gemaakte interne afspraken

Om boetes te voorkomen en om onze verantwoordelijkheid goed invulling te geven is bewustzijn, verantwoordelijkheid en medewerking van iedereen die met persoonsgegevens werkt nodig. Met alle personeelsleden die werken met persoonsgegevens heeft PCPO de volgende afspraken gemaakt:

- Deel alleen het hoognodige aan persoonsgegevens (need to know);
- Deel alleen persoonsgegevens met instellingen waarmee dat mag (swv, ander scholen, bedrijven instellingen waarmee een verwerkersovereenkomst werd afgesloten);
- Zorg ervoor dat er met bedrijven/instellingen (bv. ONS Onderwijsbureau, Kennisnet etc.) die persoonsgegevens vanuit PCPO bewerken een verwerkersovereenkomst is afgesloten;
- Zorg ervoor dat alleen zij die echt inzicht moeten hebben in persoonsgegevens toegang krijgen tot deze gegevens en ook alleen tot die gegevens die echt nodig zijn;
- Zorg voor een geheimhoudingsovereenkomst met derden die inzicht hebben in persoonsgegevens vanuit PCPO (denk aan onderzoekers, externe RT-ers, maar ook eventueel stagiaires en vrijwilligers).

*Je moet, volgens de AVG, steeds kunnen bewijzen dat je gegevens verwerkt of verstrekt met toestemming van de belanghebbenden. Voorbeeld: een ouder vraagt je om contact te leggen met een door hen ingehuurde RT-er en deze 'bij te praten' over de leervorderingen en/of medische problematiek van het kind. Laat de ouder die toestemming met een mailtje bevestigen en sla dit mailtje op in het dossier van de leerling.*

## 11. Systeem

- Ieder systeem waarop privacygevoelige informatie kan worden benaderd of wordt verwerkt is momenteel voorzien van een toegangswachtwoord. Om de veiligheid te verhogen is inloggen binnenkort alleen nog mogelijk via tweeweg verificatie;
- Systemen van PCPO/de school worden aan het eind van de werkdag afgesloten (monitoren uit, i.v.m. brandgevaar en overbodig energieverbruik) en indien van toepassing opgeslagen in de daarvoor beschikbare voorzieningen;
- Iedere PCPO-locatie dient te beschikken over een beveiligd (WIFI) basisnetwerk en een beveiligd gastnetwerk. Gasten, ouders en leerlingen die op een PCPO-locatie werken met eigen 'devices' doen dat via het gastnetwerk. Personeel werkt via het basisnetwerk. Het gastnetwerk sluit toegang tot onze bestanden uit;
- Het werken op een computer zonder bijgewerkte virusbescherming en firewall is vanaf 01-05-2018 verboden. Dat geldt ook voor je thuis computer(s) wanneer die wordt gebruikt voor 'werkzaken'. Alle Windowscomputers zijn standaard beveiligd via Windows Defender;
- Maak je foto's van leerlingen, op school of daarbuiten, bijvoorbeeld om op Klasbord te plaatsen: verwijder de foto's van je telefoon nadat je die geplaatst hebt. Vergeet ook het mapje 'recent verwijderd' niet en wanneer je een back up maakt van je telefoon. Denk hierbij ook aan OneDrive, GoogleDrive of ICloud;
- Verlies je je telefoon of tablet waarop 'werkzaken' staan, dan meld je dat direct bij de schoolict-er en bij het directielid die verantwoordelijk is voor AVG-veiligheidszaken;

- Wanneer je wegloopt bij een systeem vergrendel je het systeem. Op Windowssystemen doe je dat door de Windowstoets en de L-toets tegelijk in te drukken. Géén systeem blijft dus onbemand en onvergrendeld achter.

### 11.1 Voorgeschreven beveiligingsmaatregelen voor ict-apparatuur

#### 11.1.1 Smartphone beveiliging
- De smartphone is beveiligd met PIN, vingerafdruk of gezichtsherkenning
- Automatische updates staan ingeschakeld

#### 11.1.2 Computer beveiliging
- Een sterk wachtwoord is ingesteld (zie Wachtwoordbeleid)
- De computer gaat automatisch naar het vergrendelscherm na 5 minuten
- Geen informatie opslaan op interne harde schijf, of losse gegevensdragers, of de betreffende map wordt extra beveiligd met een wachtwoord
- Het besturingssysteem wordt bijgewerkt via automatische updates
- Virusscanner is geïnstalleerd en ingeschakeld binnen Windows Defender
- Er worden geen werk gerelateerde gegevens opgeslagen buiten de beveiligde opslag

#### 11.1.3 Wachtwoordbeleid ten aanzien van werk gerelateerde hulpmiddelen
- Gebruik van minimaal twaalf karakters
- Gebruik van ten minste één numeriek teken
- Gebruik van minstens één hoofdletter en minstens één kleine letter
- Gebruik van ten minste één speciaal teken
- Niet gebaseerd op persoonlijke gegevens (bijv. geboortedatum, adres, naam familielid, etc.)
- Mag niet gelijk zijn aan het laatste wachtwoord
- Moet elke 90 dagen worden vernieuwd

## 12. Website
De websites worden beheerd door een externe partij, waarmee een verwerkersovereenkomst is afgesloten. Wijzigingen en online documentatie worden centraal aangestuurd en beoordeeld. Op de website is de privacy- en cookieverklaring goed vindbaar. Tevens is een cookiebanner aanwezig waarbij toestemming kan worden gegeven voor het plaatsen van de cookies. Deze toestemming kan later ook weer gemakkelijk worden ingetrokken.

## 13. Softwarepakketten
- Op scholen wordt ervoor gezorgd dat de rechtenstructuur binnen de gebruikte pakketten up-to-date is;
- Gebruikers van een app die privacygevoelige informatie verwerkt worden gemeld bij de leidinggevende. Het gebruik van apps waarvan de data verwerkt wordt buiten de EU zijn niet toegestaan.

## 14. Externe gegevensdragers
- Het gebruik van mobiele datadragers (usb-sticks, mobiele harddisks e.d.) wordt per 01-05-2018 zoveel mogelijk vermeden. Privacygevoelige informatie wordt nooit op mobiele gegevensdragers gezet.

## 15. Opslag van gegevens
- De klassenmap ligt alleen op het bureau als die in gebruik is, anders ligt de map achter slot en grendel;

- Het 'lokaal' opslaan (op de harde schijf van het werkstation of laptop, maar ook op de persoonlijke Onedrive) van persoonsgegevens en privacygevoelige informatie is per 01-05-2018 niet meer toegestaan;
- Bedrijfsinformatie op 'lokale' harde schijven (documentmappen) is sinds 01-05-2018 niet meer toegestaan. Ter voorkoming wordt ook de downloadmap geleegd. Gegevens worden in de Cloud (Sharepoint of bedrijfs OneDrive) of eventueel op de schoolserver opgeslagen;
- Minimaal eenmaal per maand wordt de downloadmap op de computer geleegd;
- Het opslaan van persoons- en privacygevoelige gegevens gerelateerd aan het werk mag sinds 01-05-2018 niet meer op clouddiensten buiten de eigen PCPO Sharepointomgeving.

## 16. Uitwisselen van gegevens

- Het uitwisselen van privacygevoelige gegevens vindt, waar mogelijk, plaats via een beveiligde omgeving. Bijvoorbeeld via OSO;
- Het uitwisselen van privacygevoelige gegevens met derden, via mail, geschiedt alleen via je PCPO-mailadres, met de informatie als bijlage. Deze bijlage wordt beveiligd en de code wordt via een aparte mail, Whatsapp, of sms verzonden. Op deze manier wordt vermeden dat bij het kiezen van een geadresseerde, privacygevoelige info bij de verkeerde persoon terecht komt;
- Per ongeluk versturen van **niet beveiligde** privacygevoelige gegevens, naar een verkeerde persoon of instantie is een datalek en wordt direct gemeld aan de intern verantwoordelijke.

## 17. Social media

- Medewerkers zijn zich ervan bewust dat het privacyreglement van Facebook (FB) niet voldoet aan de voorschriften van de AVG. Zoals het feit dat iedere foto die geplaatst wordt op Facebook wettelijk eigendom is van Facebook en mag worden gebruikt door dit bedrijf. Dat geldt ook voor foto's die via WhatsApp (eigendom van Facebook) worden verstuurd;
- Op schoolniveau zijn er afspraken wie welk medium bijhoudt, wie de informatie plaatst en wie aanspreekbaar is op de inhoud. Per school is één account per medium aangemaakt, en niet ook nog voor klassen apart;
- Communicatie met leerlingen, ouders en andere stakeholders is professioneel en verloopt niet via social Media, maar alleen via afgesloten kanalen;
- Het contact met ouders/verzorgers is professioneel en gebeurt via een beveiligd medium zoals Klasbord e.d. Een medewerker is geen lid van een appgroep van ouders;
- Een medewerker is zich bewust van zijn rol inzake het delen van informatie via bv Facebook, ook indien de medewerker een ouder als 'vriend' heeft. De medewerker is persoonlijk aanspreekbaar op eventuele gevolgen;
- Een medewerker is zich bewust van de toestemming die hij/zij geeft bij het gebruik van zijn/haar beeltenis op de verschillende media en denkt na over hoe de privcaywens overeenkomt met dat wat op social media gecommuniceerd wordt (Facebook, Whatsapp, Snapchat, Tinder e.d.);
- Er is een social mediabeleid voor de medewerkers dat toeziet op het gebruik van beeldmateriaal van leerlingen en medewerkers op social media-platforms, zodat men weet hoe men hiermee om dient te gaan en wat wel en niet is toegestaan.

## 18. Toestemmingsformulier gebruik beeldmateriaal

Zowel het personeel als de ouders van de leerlingen geven door middel van een ondertekend toestemmingsformulier hun goedkeuring voor het gebruik van beeldmateriaal in diverse situatie. Het toestemmingsformulier wordt in principe 1x ingevuld. Indien er wijzigingen aan het formulier zijn aangebracht dienen ouders opnieuw het formulier ter ondertekening aangeboden te krijgen. Nieuwe ouders ontvangen het te ondertekenen formulier bij het inschrijffomulier.

## 19. Drukwerk

- Bij het gebruik van foto's in drukwerk (Schoolgids, kalender, krant) wordt er extra toestemming gevraagd aan de ouders van wie de kinderen op het fotomateriaal in de publicatie te zien zijn en met de betreffende collega's op de foto's, voordat de opdracht wordt gegeven;
- Het integraal verspreiden van klassenlijsten gebeurt alleen indien de ouders op de lijst toestemming geven en de lijst een bijdrage levert aan de veiligheid van kinderen.

## 20. E-mail

- Werkgerelateerde mails worden alleen verstuurd vanuit @pcpomiddenbrabant.nl-mailadressen. Berichten vanuit dit adres worden allen voorzien van een bedrijfshandtekening, zoals afgesproken binnen de school/het cluster;
- Er wordt geen privémail verstuurd vanuit het werkmailadres. Privé-accounts worden niet aangemaakt met het werkmailadres;
- Geadresseerden van groepsmails worden, buiten PCPO, geplaatst onder BCC;
- De optie 'allen beantwoorden' wordt alleen gebruikt wanneer dit echt noodzakelijk is.

## 21. Werkomgeving

- Externe partijen krijgen pas na het ondertekenen van een geheimhoudingsverklaring toegang tot privacygevoelig materiaal;
- Het versturen (e-mail inclusief) van privacygevoelige informatie vanaf onbeveiligde of openbare netwerken is sinds 01-05-2018 verboden;
- Niemand werkt in een account van een ander, ook niet in een leerlingenaccount: de houder van het account is verantwoordelijk voor de verrichtingen gemaakt binnen en met het account;
- Het bestuur is gerechtigd om, steekproefsgewijs, verrichtingen op werkaccounts te monitoren. Bij een datalek of een andere privacy-schending wordt standaard onderzoek gedaan naar de oorzaak van het lek;
- Sommige Clouddiensten zijn niet veilig. Het delen van zakelijke privacygevoelige informatie mag alleen via de OneDrive binnen een PCPO-account of via PCPO's Sharepoint. Het extern delen van privacygevoelige informatie mag alleen nog via daarvoor beschikbare pakketten zoals PCPOInsite, Parnassys, OSO e.d. Dus niet via bijvoorbeeld Dropbox, Wetransfer e.d.;
- Invallers krijgen een apart invallersaccount waarmee zij wel hun werk kunnen doen met bijvoorbeeld leerlingsoftware, maar niet direct toegang krijgen tot privacygevoelige informatie wanneer dit niet direct nodig is.

## 22. Wachtwoordbeleid

- PCPO heeft voor iedere leerling een alias gegenereerd (256 tekens). Deze aliassen zorgen ervoor dat, onzichtbaar in de software, kinderen anoniem gebruik kunnen maken van educatieve software. Pakketten als Basispoort verwerken zo alleen de alias en niet meer de naam, groep en leeftijd van de leerling. Deze code heet een keten-id of ECK-id;
- Systeembeheerders en andere functionarissen die wachtwoorden beheren slaan eventuele lijsten veilig op. PCPO-personeel gaat nauwkeurig om met wachtwoorden en bewaart wachtwoorden op een veilige plaats (bijvoorbeeld op je persoonlijke OneDrive in een beveiligd bestand). Dat kan in Word, maar ook via Keypass, of Lastpass bijvoorbeeld.
- Niemand legt wachtwoorden schriftelijk vast op voor derden toegankelijke plaatsen;

- Een medewerker beveiligt zijn/haar telefoon, tablet, pc of laptop waarop werkkoppelingen (Sharepoint, OneDrive, Parnassys e.d.) zijn aangebracht met een sterk wachtwoord[1], een cijfercode en/of met vingerafdruk- of irisscanbeveiliging; Het is niet toegestaan om werkkoppelingen te installeren, binnen een gebruikersaccount, op een telefoon, tablet, laptop e.d. waarvan ook anderen (bijvoorbeeld leerlingen, kinderen en partners) gebruik maken;
- Een medewerker verandert uitgereikte wachtwoorden direct in eigen wachtwoorden;
- Niemand deelt wachtwoorden die toegang geven tot werk- of persoonsgegevens met anderen, ook niet met duo-collega's. Iedere medewerker dient eigen wachtwoorden en accounts te hebben ten behoeve van zijn werkzaamheden.

## 23. Meldingsplicht

- Iedere leidinggevende informeert de systeembeheerder en/of het directielid met coördinerende ICT-taken tijdig bij (onvrijwillig) ontslag/ einde dienstverband van een medewerker en vraagt hem direct het toegangsbeheer aan te passen;
- Iedere medewerker informeert de systeembeheerder en het directielid met coördinerende ICT-taken onmiddellijk bij verlies van zijn telefoon, laptop of tablet en vraagt hem direct het toegangsbeheer aan te passen. Dit geldt alleen wanneer er een app/software is geïnstalleerd die toegang geeft tot privacygevoelige informatie, of wanneer privacygevoelige info is opgeslagen op het betreffende apparaat (Dit is ten zeerste verboden). In andere gevallen geldt deze meldplicht alleen voor PCPO-apparatuur;
- Iedere medewerker is verplicht het niet naleven van deze afspraken, door wie dan ook, te melden bij zijn leidinggevende.

## 24. Ontwikkelagenda

De aanwezige kennis, ook binnen de twee besturen (HGL en Markant-onderwijs) waarmee wordt samengewerkt, wordt onderling uitgewisseld, door periodiek bij elkaar te komen om de kennis te delen onder leiding van een projectleider of de FG-er. Er zijn afspraken gemaakt over wat door de juristen opgepakt zal worden en wat door het bestuur zelf opgepakt wordt. Als bepaalde actiepunten door de school zelf uitgevoerd worden, dan gelden daar heldere deadlines voor. Er is een nieuwe (gezamenlijke) FG aangesteld voor PCPO.

Hieronder een opsomming van de ontwikkelpunten:

- Bewustwordingscampagne voeren (2021-2022).
- De privacyverklaring aangepassen/aanvullen. Hiervoor dient in kaart te worden gebracht welke verschillende verwerkingen plaatsvinden op de website(s). Ook dienen de persoonsgegevens specifiek benoemd te worden die worden verwerkt en onder welke grondslag en dienen de rechten van de betrokkenen benoemd te worden. Tevens moet gecontroleerd worden of de auteursrechten van de website worden overgedragen aan PCPO middels een akte van overdracht. In het geval dat de auteursrechten bij de externe partij liggen zorgt dat een risico op het vlak van continuïteit. Dit kan juridische/financiële consequenties hebben indien dit niet goed geregeld is.
- Een clean desk policy ontwikkelen.

Afgehandelde ontwikkelpunten

- Alias-en leerlingontwikkelings- en volgsysteem in gebruik nemen (i.s.m. PO-Raad/Kennisnet/Parnassys). De aanvraag loopt.

[1] Waar wordt gesproken over een sterk wachtwoord wordt een wachtwoord bedoeld dat minimaal bestaat uit 8 tekens en wat bestaat uit cijfers, letters, waarvan minimaal één hoofdletter en een speciaal teken (bijv. % & # @). Kies bij voorkeur voor een wachtwoordzin en vermijdt voor de hand liggende wachtwoorden als de naam van je kinderen, partner, welkom123 e.d.)

- In het privacybeleid medewerkers wijzen op DPIA.
- Beter informeren van betrokkenen inzake hun rechten tot inzage en controleren of aan de informatieplicht richting de medewerkers en de leerlingen/ouders wordt voldaan aan de hand van het interne privacybeleid en de privacyverklaring op de website. Protocol voor opstellen en de betreffende medewerkers instrueren.
- Verwerkingsregister opstellen.
- Bewaartermijnenbeleid intern communiceren.
- Er dient te worden gecheckt of het toestemmingsformulier voldoet aan de wettelijke eisen van de AVG, maar ook aan de verwerkingen die plaatsvinden binnen PCPO. Daarnaast dient gecontroleerd te worden of het toestemmingsformulier altijd vereist is of dat er ook een beroep kan worden gedaan op een andere rechtsgrond.
- Werkbaarheid van het datalekkenprotocol is onderzocht en datalekregister is ontwikkeld.

# 25. Bijlage

## 25.1 Leeg inventarisatieformulier (bewakings)camera's

1. Naam school: Naam school
2. Schoollocatie: Schoollocatie
   (per locatie een formulier invullen)
3. Is sprake van camera's binnen het gebouw: ☐ JA / ☐ NEE
4. Plaats waar camera's worden ingezet Klik of tik om tekst in te voeren.
   (per camera vermelden)
5. Doel van inzet van camera's Klik of tik om tekst in te voeren.
   (per camera vermelden)
6. Gedurende welke periode zijn de camera's aan:
   (dagen en tijden vermelden)

| | | |
|---|---|---|
| ☐Maandag | : van tijd | tot: tijd |
| ☐Dinsdag | : van tijd | tot: tijd |
| ☐Woensdag | : van tijd | tot: tijd |
| ☐Donderdag | : van tijd | tot: tijd |
| ☐Vrijdag | : van tijd | tot: tijd |
| ☐Zaterdag | : van tijd | tot: tijd |
| ☐Zondag | : van tijd | tot: tijd |

7. Wat is het gerechtvaardigd belang van de inzet van camera's Klik of tik om tekst in te voeren.
   (per camera vermelden)
8. Wanneer is het gerechtvaardigd belang voor het laatst getoetst: datum
9. Is overleg gevoerd met de MR over inzet van de camera's: ☐ JA / ☐ NEE
   a. Wat is de datum waarop MR positief advies gaf over inzet van de camera's datum
10. Is een DPIA uitgevoerd voorafgaand aan de inzet van de camera's: ☐ JA / ☐ NEE
    a. Indien NEE, waarom is geen DPIA uitgevoerd? Klik of tik om tekst in te voeren.
11. Wie is verantwoordelijk voor het na vier weken verwijderen van de beelden: naam functionaris(sen)
12. Wie hebben er toegang tot de camerabeelden: naam functionaris(sen)

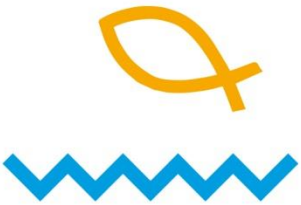
## 25.2 Inventarisatieformulieren (bewakings)camera's scholen

Voor de inventarisaties van de scholen verwijzen we graag naar de bijlage: Cameratoezicht: schoolspecifieke documenten.

## 25.3 Checklist AVG voor in de klas

- Vergrendel je computer wanneer je erbij wegloopt (Windowsteken-L);
- Denk goed na voor je informatie deelt met anderen. Deel alleen noodzakelijke informatie (dataminimalisatie);
- Surf zorgvuldig, bewaar privé dingen voor thuis;
- Gebruik werkmedia alleen voor werk gerelateerde doelen
- Maak en gebruik alleen en sterke wachtwoorden;
- Houd je wachtwoord en je account alleen voor jezelf: jij bent verantwoordelijk voor wat er vanuit jouw account gebeurt;
- Bewaar je wachtwoorden veilig;
- Maak je gebruik van social media: denk na wat je post, houd je functie daarbij in gedachten, zeker als je ook ouders als 'vriend' hebt
- Deel persoonlijke informatie alleen via een beveiligde website (let op het slotje voor de url);
- Maak geen gebruik van losse datadragers (USB-sticks e.d.);
- Zorg ervoor dat je privacygevoelige werk gerelateerde gegevens bewaart achter slot en grendel: zowel thuis als op je werkplek;
- Kijk alleen naar gegevens die je nodig hebt voor je functie/werk: het bekijken van niet voor het uitoefenen van je functie noodzakelijke gegevens is strafbaar (datalek);
- Meld het verloren gaan van hardware met privacy gevoelige informatie erop (telefoons, laptops, tablets etc.)
- Beveilig je hardware. Maak meerdere gebruikersaccounts aan wanneer hardware door meerdere personen wordt gebruikt;

# DE VIJF PIJLERS VAN PCPO

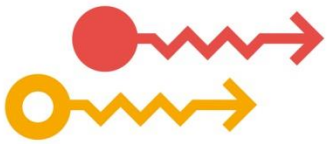


Christelijke normen en waarden als uitgangspunt

Brede talent ontwikkeling

Zorg voor elk kind

Zorg en aandacht voor de omgeving



Ondernemend