Informatiebeveiligings- en privacy beleid (IBP) CBS Coolsma

Versie 2: maart 2022

Goedgekeurd door:

Directie: 19-05-2022

Bestuur: 19-05-2022

Ter kennisgeving:

Functionaris Gegevensbescherming Angela Groen (CED): 20-05-2022

CBS Coolsma Coolsmalaan 3-5 3971 KW Driebergen

Tel: 0343 513735 E-mail: info@cbscoolsma.nl Website: www.cbscoolsma.nl

1. Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ict. En ict wordt in toenemende mate ingezet voor het onderwijs. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ict. 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 is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang en de kwaliteit van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

2. Toelichting informatiebeveiliging en privacy

2.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid 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 schade, imagoverlies en privacy-aangelegenheden.

2.2 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 natuurlijke persoon 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.

2.3 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: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis om informatiebeveiliging en privacy binnen school CBS Instituut Coolsma te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3. Doel en reikwijdte

3.1 Doel

De hoofddoelstelling van het IBP-beleid is het richting geven aan het inrichten van informatiebeveiliging binnen de school; er worden doelen gesteld, verantwoordelijkheden beschreven, structuur geschetst en de middelen benoemd waarmee dit beleid moet worden vormgegeven. Dit proces hanteert een Plan Do Check Act Cyclus (PDCA) en moet aansluiten bij de Planning en Control (P&C) Cyclus van de school in komt terug in de Maand Rapportage van directie en bestuur.

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het reduceren van beveiligingsrisico's.
- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen bij CBS Instituut Coolsma.
- Het verwerken van persoonsgegevens , waaronder die van leerlingen, hun ouders/verzorgers en medewerkers
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.
- Bevordering van het bewustzijn van het eigenaarschap bij leerlingen en medewerkers van Coolsma.

Het informatiebeveiligings- en privacy beleid (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 betrokkenen (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en CBS Instituut Coolsma voldoet aan relevante wet- en regelgeving.

Het IBP-beleid is de kapstok voor aanvullend beleid, operationele plannen, procedures en standaarden binnen de school of samenwerkingsverband ZOUT. Door het informatiebeveiligingsbeleid te ondertekenen laten bestuur en directie van de school zien dat men dit belangrijk vindt.

3.2 Reikwijdte

- Het IBP-beleid binnen CBS Instituut Coolsma geldt voor alle medewerkers, leerlingen, ouders/verzorgers, gastgebruikers, bezoekers en externe relaties (inhuur / outsourcing) van Coolsma. Onder dit beleid vallen ook alle devices waarmee geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.

- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen CBS Instituut Coolsma waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, () bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan CBS Instituut Coolsma persoonsgegevens verwerkt.

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van CBS Instituut Coolsma. Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (b.v. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media.)

- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van CBS Instituut Coolsma 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.

- Het IBP-beleid heeft binnen CBS Instituut Coolsma raakvlakken met:
  - *Algemeen veiligheids- en toegangsbeveiligingbeleid;* 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.

4. Beleid – Hoe doen we dat?

CBS Instituut Coolsma hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van CBS Instituut Coolsma neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. De Security Officer (SO) van Coolsma zorgt voor de tactische en operationele uitvoering. Directie en bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerking verantwoordelijke.

2. CBS Instituut Coolsma voldoet aan alle relevante wet- en regelgeving.

3. Bij CBS Instituut Coolsma 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 CBS Instituut Coolsma 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 te allen tijde hun toestemming herzien.

4. CBS Instituut Coolsma zal alle betrokkenen helder 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.

5. CBS Instituut Coolsma legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. CBS Instituut Coolsma voldoet hiermee aan de documentatieplicht.

6. Binnen CBS Instituut Coolsma 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. CBS Instituut Coolsma 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 worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. CBS Instituut Coolsma 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 Coolsma wil afdekken en de benodigde investeringen en de te nemen maatregelen.

9. CBS Instituut Coolsma sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.

10. CBS Instituut Coolsma verwacht van alle medewerkers, leerlingen, ouders/verzorgers, () 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. CBS Instituut Coolsma heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij CBS Instituut Coolsma een continue proces, wordt opgenomen in de rapportagecyclus en wordt minimaal jaarlijks geëvalueerd, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt beoordeeld of aanpassing gewenst is.

12. CBS Instituut Coolsma kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vooraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

13. CBS Instituut Coolsma 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. Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt CBS Instituut Coolsma aanvullende afspraken vast over de technische maatregelen.

14. CBS Instituut Coolsma zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

5. Uitwerking van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de invulling van het beleid.

5.1 Relevante wet- en regelgeving

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken. De toepassing van het ISO normen kader wordt door Coolsma risicogebaseerd en pragmatisch toegepast. Het is een middel om het doel van beveiliging te realiseren en geen doel op zich.

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

- Wet op het primair onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)*
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen.

ISO 27002 normenkader bestaat uit 114 items onderverdeeld in 14 hoofdstukken.

• 1 Beveiligingsbeleid
• 2 Organisatie van informatiebeveiliging
• 3 Personele beveiligingseisen
• 4 Beheer van bedrijfsmiddelen
• 5 Toegangsbeveiliging
• 6 Cryptografie
• 7 Fysieke beveiliging en beveiliging van de omgeving
• 8 Beveiliging bedrijfsvoering
• 9 Beheer van communicatie en bedieningsprocessen
• 10 Acquisitie Verwerving, ontwikkeling en onderhoud van informatiesystemen
• 11 Leveranciersrelaties
• 12 Beheer van informatiebeveiligingsincidenten
• 13 Informatiebeveiligingsaspecten van de bedrijfscontinuïteitsbeheer
• 14 Naleving

5.2 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.

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 staan 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. Hiervoor hanteert de school een dataretensieschema.

4. **Transparantie**: de school legt aan betrokkenen (leerlingen, hun ouders/verzorgers 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 betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming 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 juist en actueel zijn.

5.3 Ondersteunende richtlijnen en procedures

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

5.4 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 hierbij 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 bewustwordingscampagnes voor medewerkers, leerlingen, ouders en bezoekers. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de directie, de Functionaris Gegevensbescherming (FG) en de Security Officer (SO) met het bestuur als eindverantwoordelijke. Hiervoor is een jaarplanning waarin activiteiten/controles weggezet worden: directie communiceert deze ook intern en met het bestuur.

5.5 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 betrouwbaarheidsaspecten die van belang zijn.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vooraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ict)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

5.6 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 door te mailen naar info@cbscoolsma.nl of te melden bij bij de directeur van de school.
Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.7 Planning en controle

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en 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
- Uitkomsten van audits en FG- toetsingen
- Externe ontwikkelingen en eisen t.a.v. informatiebeveiliging, privacy en AVG

Daarnaast kent CBS Instituut Coolsma een jaarlijkse plannings- en controlcyclus 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.

5.8 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 directie en en aangestelde security officer hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, 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 het schoolbestuur van Vereniging voor Christelijk Onderwijs Instituut Coolsma, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het schoolbestuur vastgestelde reglement.

Mocht de naleving van dit beleid ernstig tekort schieten, dan kan CBS Instituut Coolsma de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

6. Organisatie - Wie doet wat?

6.1 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. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij CBS Instituut Coolsma.

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richting gevend (strate-gisch)	**Bestuur** (ingevuld door de voorzitter van het bestuur)	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacy beleid • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
Sturend (tactisch)	**Manager IBP** (ingevuld door de directeur van de school)	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert bestuur over IBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	Processen, richtlijnen en procedures IBP, waaronder: • Activiteitenkalender/jaarplanning • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Brief toestemming gebruik beeldmateriaal • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ict en internetgebruik • Gedragscode medewerkers en leerlingen De werkdocumenten van de jaarplanning en uitgevoerde acties worden frequent aangepast en zijn te vinden op de drive AVG
	Domeinverantwoordelijke/ Proceseigenaren Waaronder o.a.: ICT, HRM / P&O, facilitair, onderwijs, financiën, inkoop en administratie	• Classificatie / risicoanalyse in samenwerking met de Security officer • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur • Samen met functioneel beheer en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • Samen met ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk De werkdocumenten van de jaarplanning en uitgevoerde acties worden frequent aangepast en zijn te vinden op de drive AVG

	Functionaris voor Gegevens-bescherming (FG) (ingevuld door de externe FG)	● Toezicht op naleving privacy wetgeving ● Voorlichting privacy en stimuleren bewustwording ● Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens ● Afwikkeling klachten en incidenten	● Privacyreglement en IBP ● Procedure IBP-incident afhandeling ● Inrichten meldpunt datalekken
Uit-voerend (opera-tioneel)	**Security officer** (ingevuld door de ICT'er van de school) Applicatie beheerder (ingevuld door de ICT'er van de school) Medewerker Directie van de school	● Incidentafhandeling (registreren en evalueren). ● Technisch aanspreekpunt voor IBP-incidenten. ● Uitvoeren taken conform gegeven richtlijnen en procedures. ● Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. ● Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. ● Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. ● Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. ● Implementeren IBP-maatregelen. ● Periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, vergaderingen, beoordelingen etc.; ● Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur.	Communiceren, informeren en toezien op naleving van o.a.: ● IBP in het algemeen ● Regels passend onderwijs ● Hoe omgaan met leerling dossiers ● Wie mogen wat zien ● Gedragscode ● Omgaan met sociale media ● Mediawijs maken

De verdere uitwerking van de rollen en taken staan beschreven in bijlage 1.

Bijlage 1: Organisatie; wie doet wat

Deze bijlage beschrijft hoe IBP op drie niveaus wordt georganiseerd.

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij CBS Instituut Coolsma voor elk niveau een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen. Beschreven wordt welke rollen, welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

Richtinggevend

Eindverantwoordelijke
De voorzitter van het bestuur van Vereniging voor Christelijk Onderwijs Instituut Coolsma is eindverantwoordelijk voor het IBP en stelt 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 regelmatige rapportages geëvalueerd.
De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de manager IBP.

Sturend

Manager IBP
Manager IBP, uitgevoerd door de directeur van Coolsma , heeft een rol op sturend niveau. Hij geeft terugkoppeling en advies aan de het bestuur en stuurt de mensen aan op uitvoerend niveau. De manager IBP moet:

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

Functionaris voor Gegevensbescherming
De externe Functionaris voor Gegevensbescherming (FG), houdt binnen CBS Instituut Coolsma toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het verbeteren en stimuleren van bewustwording rondom IBP, het afhandelen van informatiebeveiligingsincidenten, adviseert over het regelen van privacy, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en rapporteert aan de eindverantwoordelijke (het bestuur). De FG heeft regelmatig overleg met de manager IBP. De FG is ook de contactpersoon voor klachten en vragen.

Domeinverantwoordelijke / proceseigenaar
Binnen de school zijn er verschillende domeinen/processen, zoals ict, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, onderwijs et cetera. Op elk van deze domeinen/processen is iemand als proceseigenaar verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

De domeinverantwoordelijke, ingevuld door de directeur van de school, is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben de proceseigenaren de volgende specifieke taken:

- Samen met de eindverantwoordelijke, ingevuld door de voorzitter van het bestuur, stellen zij het beleid voor toegang (autorisaties) vast.
- Samen met functioneel beheer en ICT-beheer, ingevuld door de ICT'er van de school, zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
- Samen met functioneel beheer en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

Uitvoerend

Security Officer (SO)
De Security Officer, ingevuld door de ICT'er van de school, vormt een technisch aanspreekpunt als het gaat over informatiebeveiliging voor de directie en de medewerkers.

Functioneel beheerder of Applicatiebeheerder
Ieder softwarepakket of (web-)applicatie heeft een beheerder. De functioneel beheerder, uitgevoerd door de ICT'er van de school, wordt vanuit de domeinverantwoordelijke / proceseigenaar voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden.

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Medewerkers worden in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren. Medewerkers worden gevraagd 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 of via de MR)

Leidinggevende
Naleving van het IBP is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende, ingevuld door de directeur van de school, heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het IBP-beleid;
- 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 personeel gerelateerde IBP-onderwerpen.

Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

Een IBP-team, bestaande uit directie, bestuurslid en Security officer wordt organisatiebreed zowel preventief als curatief benoemd voor informatiebeveiliging en privacy incidenten. De leden van het IBP-team zijn benoemd door de voorzitter van het bestuur en handelen in diens opdracht. Het IBP-team van CBS Instituut Coolsma heeft de volgende opdracht:

- Het signaleren en registreren van alle privacy verzoeken, beveiligingsincidenten en datalekken. Het coördineren van de maatregelen en het toezien op de oplossing van problemen die tot incidenten hebben geleid of waardoor de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij);
- Het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars, beheerders en eindgebruikers door het verspreiden van informatie;
- Het leveren van managementrapportages en verbetervoorstellen aan de domeinverantwoordelijke/proceseigenaar over de beveiligingsincidenten en verzoeken tot uitoefening privacyrechten van de betrokkenen.

Bij een calamiteit kan het IBP-team terstond bij elkaar worden geroepen op initiatief van de manager IBP, in opdracht van het CBS Instituut Coolsma. Het doel hiervan is om de continuïteit van de informatievoorziening en de privacy te waarborgen. Onder calamiteiten worden verstaan:

- Datalek;
- Grote verstoringen van het netwerk (bijvoorbeeld DDoS aanval);
- Natuurrampen (brand, overstroming, storm, etc.).

Het IBP-team bij CBS Instituut Coolsma behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiligings- en privacy-incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.
De werkzaamheden van het IBP-team bij CBS Instituut Coolsma is gedocumenteerd in het IBP en door de voorzitter van het bestuur, bekrachtigd. De eindverantwoordelijkheid ligt bij het bestuur.