



Stichting Cambium College voor Openbaar Voortgezet Onderwijs

Informatiebeveiliging- en privacybeleid

Datum instemming directie	16 januari 2023
Datum instemming MR	20 april 2024
Opsteller	Frank Andringa & Daniëlla van der Leij
Bron	Kennisnet
Plaatsen op P/beleid	✓ ja
Plaatsen op website	✓ ja
PDCA	2 jaar

1. Inleiding

Het onderwijsveld 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.

1.1 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 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 en imagooverlies.

1.2 Toelichting privacy

Privacy gaat over 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 wet noemt als voorbeelden van verwerking: het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

1.3 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 ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen het Cambium College en vormt de kapstok voor de onderliggende afspraken en procedures.

2. Doel en reikwijdte

2.1 Doel

Dit beleid heeft als doelen:

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

Dit beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet zijn tussen privacy, functionaliteit en veiligheid. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene, met name van medewerkers en leerlingen, wordt gerespecteerd en Cambium College voldoet aan de relevante wet- en regelgeving.

2.2 Reikwijdte

- Het IBP-beleid binnen Cambium College geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen het Cambium College waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Cambium College persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van het Cambium College. 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 Cambium College evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
- IBP-beleid heeft binnen het Cambium College raakvlakken met:
 - *Algemeen veiligheids- en toegangsbeveiligingsbeleid*; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
 - *Personeels- en organisatiebeleid*; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
 - *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen
 - *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers

3.1 *Algemene beleidsuitgangspunten*

Cambium College hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het bestuur van Cambium College neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
2. Cambium College voldoet aan alle relevante wet- en regelgeving.
3. Bij Cambium College is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van het Cambium 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 ten alle tijden hun toestemming herzien.
4. Cambium College zal alle betrokkenen helder en actief informeren over de verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn verkregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabiliteit en profilering.
5. Cambium College legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Het Cambium voldoet hiermee aan de documentatieplicht. Cambium College maakt hierbij gebruik van het IBP systeem van YourSafetyNet.
6. Binnen het Cambium 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. Cambium College 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. Cambium College classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.
9. Cambium College 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. Cambium College verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagooverlies. Het Cambium heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
11. Informatiebeveiliging en privacy is bij Cambium College een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
12. Cambium College kijkt bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen vóóraf naar de impact hiervan op de informatiebeveiliging en privacy, zodat tijdig de juiste maatregelen genomen kunnen worden.

13. Cambium College 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.
14. Cambium College zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

4 *Uitwerking van het beleid – Wat doen we?*

Deze paragraaf geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

4.1 *Relevante wet- en regelgeving*

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

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

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.

4.2 *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 (subsidiar). 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 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.

4.3 Ondersteunende richtlijnen en procedures

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

4.4 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de directie, de FG, en werkgroep AVG met het bestuur als eindverantwoordelijke.

4.5 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 vóóraf 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.

4.6 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 bij helpdesk@cambiumcollege.nl.

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

4.7 Planning en controle

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 Cambium College 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.

4.8 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 leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP met een brede gedragscode en met periodieke bewustwordingscampagnes, etc.

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.

Mocht de naleving van dit beleid ernstig tekort schieten, dan kan Cambium College de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

4.9 Logging en monitoring

Uit dit beleid vloeit voort dat het gebruik van alle ICT middelen binnen het Cambium College automatisch geregistreerd (gelogd) wordt om de continuïteit van de technische infrastructuur te waarborgen, om verstoring van de onderwijsprocessen en andere (financiële) schades tegen te gaan. Deze registratie kan worden gebruikt om achteraf toezicht te kunnen houden op de naleving van toebedeelde autorisaties. Ook is deze registratie noodzakelijk voor mogelijke forensische onderzoeken naar aanleiding van een data lek.

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

Het voor dit toezicht beschikbaar stellen van gegevens die tot een persoon herleidbaar zijn, wordt tot het strikt noodzakelijke beperkt. Onderzoek naar een vermoedelijke overtreding op het gebied van ICT (bijvoorbeeld overtreding van het internetprotocol, oneigenlijk gebruik/toegang digitale bestanden of website) door individuele gebruikers kan alleen worden geïnitieerd door de hoogst leidinggevende van een afdeling, na overleg met het hoofd HRM en in de vorm van een schriftelijke opdracht. Het hoofd HRM beoordeelt of de opdracht van de hoogst leidinggevende voldoet aan de volgende eisen;

- Het verzoek tot onderzoek is deugdelijk gemotiveerd;
- Het onderwerp van onderzoek is duidelijk omschreven;
- Het onderzoek gaat niet verder dan strikt noodzakelijk;

en fiatteert deze daarvoor.

Vervolgens stuurt het hoofd HRM het verzoek naar de teamleider ICT. Deze beoordeelt het verzoek en start – indien akkoord – het onderzoek. De bijlage bij het internetprotocol is hiervoor leidend. Uitgangspunt is een goede balans tussen het beheer en de beveiliging van de ICT-voorzieningen versus de bescherming van de privacy van de gebruiker.

4.10 Beheersing van financiële risico's

Onderdeel van het beleid is een speciaal daartoe afgesloten verzekering welke de aansprakelijkheid van onze school verzekert voor door derden (ouders, leerlingen en medewerkers) geleden schade. Ook de daaruit voortvloeiende gevolgschade van de eigen kosten naar aanleiding van een data lek. Deze risico's kunnen bijvoorbeeld bestaan uit verloren gaan van persoonlijke (o.a. NAW) gegevens door hacken, maar ook het verlies of diefstal van bijvoorbeeld laptops, tablets en/of usb sticks.

De dekking van zo'n verzekering bestaat o.a. uit vergoeding van de redelijke en noodzakelijke kosten en uitgaven in verband met de daadwerkelijke of vermeende beveiligingsfouten, systeemfouten of verlies van onderwijs- en/of persoonsgegevens, bestaande uit:

- Juridische diensten;
- IT-diensten;
- Reconstructie van data;
- Herstel van reputatie;
- Kennisgeving aan betrokkenen.

Maar ook vergoeding van bestuurlijke boetes in verband met verwerking persoonsgegevens die de organisatie wettelijk verplicht is te betalen naar aanleiding van een onderzoek van een toezichthouder alsmede daarbij behorende kosten van verweer.

5 Organisatie – wie doet wat?

5.1 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 het Cambium.

Dit hoofdstuk beschrijft hoe IBP bij het Cambium is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

Voor elk niveau wordt beschreven welke rollen welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

5.1 Rollen (functies) rondom IBP

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Cambium College een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

5.2 Richtinggevend

Eindverantwoordelijke

Het College van Bestuur is eindverantwoordelijk voor IBP. De directie 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 informatiemanager.

5.3 Sturend

conrector bedrijfsvoering

De conrector bedrijfsvoering adviseert het College van Bestuur en de directie en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen het Cambium College.

Informatiemanager

De informatiemanager is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de conrector bedrijfsvoering en stuurt de mensen aan op uitvoerend niveau. Informatiemanager moet:

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

Functionaris voor gegevensbescherming

De functionaris voor gegevensbescherming (FG), houdt binnen Cambium College 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 werkgroep AVG. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

Teamleider ICT

Adviseert samen met de informatiemanager de eindverantwoordelijke en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen het Cambium College.

De teamleider ICT is gesprekspartner voor de manager IBP in kader van informatiebeveiliging en privacy binnen de organisatie.

Domeinverantwoordelijke / proceseigenaar

Binnen de school zijn er verschillende domeinen/processen, zoals ict, personeel, administratie, facilitaire- en financiële zaken, onderwijs etc. Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Deze proceseigenaar 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 proceseigenaren de volgende specifieke taken:

- Samen met de eindverantwoordelijke stellen zij het beleid voor toegang vast.
- Samen met het ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
- Samen met ICT-beheer beoordelen zij regelmatig de toegangsrechten van gebruikers. Leidinggevend hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

5.4 Uitvoerend

Medewerker ICT

De medewerkers van de afdeling ICT vormen een technisch aanspreekpunt inzake informatiebeveiliging voor het management en de medewerkers.

Functioneel beheerder of Applicatiebeheerder

Ieder softwarepakket of (web-)applicatie heeft een beheerder. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden. De functioneel applicatiebeheerder wordt vanuit de domeinverantwoordelijke / proceseigenaar voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in het handboek privacy. Daarnaast worden medewerkers 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 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 personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de informatiemanager. Leidinggevendens hebben hierbij een voorbeeldrol ten opzicht van hun medewerkers.

5.5 Tabel IBP rollen en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Bestuurder Conrector bedrijfsvoering	<ul style="list-style-type: none"> 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 Inhuren/ opdracht verstrekken aan FG 	<ul style="list-style-type: none"> Informatiebeveiligings- en privacy beleid Baseline / basismaatregelen Privacyreglement vaststellen Rapportage risicomanagement, frauderisicoanalyse en cybersecurity
Sturend (tactisch)	Informatie Manager	<ul style="list-style-type: none"> Inhoudelijk verantwoordelijk voor IBP IBP-planning en controle Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse Hanteren IBP normen en wijze van toetsen Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen 	Processen, richtlijnen en procedures IBP, waaronder: <ul style="list-style-type: none"> Security awareness activiteiten procedure IBP-incident afhandeling Inrichten meldpunt datalekken
	Wergroep AVG	<ul style="list-style-type: none"> Adviseert bestuur/directie over IBP Evalueren IBP-beleid en maatregelen 	<ul style="list-style-type: none"> activiteitenkalender Opstellen en actueel houden van alle relevante AVG beleidsdocumenten en protocollen. Opstellen van kwartaalrapportages richting directie en FG. Bijhouden van YourSafetyNet (AVG verantwoordingsprogramma)
	Functionaris gegevens-bescherming (FG) Via ORION	<ul style="list-style-type: none"> informatie verzamelen om verwerkingswerkzaamheden te identificeren; analyseren en controleren in hoeverre verwerkingswerkzaamheden aan de AVG voldoen; en de verantwoordelijke of de verwerker informeren, adviseren of aanbevelingen geven. 	Jaarlijkse rapportage aan College van Bestuur
	Teamleider ICT	<ul style="list-style-type: none"> is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen het Cambium 	
	Domeinverantwoordelijke/ Proceseigenaren waaronder: ict, personeel (P&O), Facilitair, onderwijs, financiën, inkoop en administratie	<ul style="list-style-type: none"> risicoanalyse in samenwerking informatiemanager Toegangsbeleid vaststellen en laten goedkeuren door directie Samen met functioneel beheer en ICT beheer er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. Samen met functioneel beheer en ICT beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren. 	<ul style="list-style-type: none"> Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: Toegangsmatrix diverse informatiesystemen en netwerk

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Uitvoerend (operationeel)	Teamleider ICT	<ul style="list-style-type: none"> • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen 	<ul style="list-style-type: none"> • IBP in het algemeen • Wie mogen wat zien • Omgaan met sociale media • Mediawijs maken
	Senior medewerker ICT	<ul style="list-style-type: none"> • Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. 	
	Medewerker	<ul style="list-style-type: none"> • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. 	
	Dagelijkse leiding / leidinggevende / directie	<ul style="list-style-type: none"> • Communicatie naar alle betrokkenen; er voor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur. 	