Informatiebeveiligings- en privacybeleid

Samenwerkingsverband Voortgezet Onderwijs Zuid-Kennemerland

4 april 2018
Versie 0.22

Bron

Kennisnet; website; 3 december 2017

Bewerkt door:

Samenwerkingsverband VO Zuid-Kennemerland, Johan Vermeer

Ver-sie	Status	Datum	Auteur	Omschrijving
0.1	concept	3 dec 2017	Johan Ver-meer	Format overgenomen; school -> samenwer-kingsverband; kleine aanpassingen. Ter bespreking in consulenten overleg
0.2	Definitief met nog enkele openstaande acties	15 dec 2017	Johan Ver-meer	Besproken in consulentenoverleg. De nog openstaande acties zijn belegd in een werk-groep. Deze versie wordt in december vastge-steld door directeur-bestuurder SWV en ver-spreid onder de aangesloten leden.
0.3	*Definitief zonder open-staande acties*	*1 mei 2018*		

Vastgesteld door SWV – VO - ZK

Versie	Datum	Naam	Functie
0.2	15 dec 2017	Johan Vermeer	directeur-bestuurder
0.21	4 april	Ledenraad SWV	

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 treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening te garanderen.
Deze aspecten zijn:

- 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 imagoverlies.

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 Samenwerkingsverband Voortgezet Onderwijs Zuid-Kennemerland (SWV-VO-ZK).

2 Doel en reikwijdte

2.1 Doel

Dit beleid heeft als doelen:

- ***Het waarborgen van de continuïteit van het samenwerkingsverband en de bedrijfsvoering.***
- ***Het garanderen van de privacy van leerlingen en medewerkers waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen.***

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 SWV-VO-ZK voldoet aan relevante wet- en regelgeving.

2.2 Reikwijdte

- Het informatiebeveiligings- en het privacy beleid binnen SWV-VO-ZK geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het netwerk verkregen kan worden.

- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van SWV-VO-ZK. Het beleid heeft zowel betrekking op gecontroleerde informatie, die door het samenwerkingsverband zelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop het samenwerkingsverband kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites,.

- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen SWV-VO-ZK waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op andere betrokkenen waarvan SWV-VO-ZK persoonsgegevens verwerkt.

- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van SWV-VO-ZK evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

- IBP-beleid binnen SWV-VO-ZK heeft 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 (in de OPR en pMR)
  - Beleid inzake aanschaf en gebruik van digitale leermiddelen

3 Uitgangspunten

3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij SWV-VO-ZK zijn:

- Informatiebeveiliging en het privacy dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming (die 25 mei 2018 in werking treedt).
  De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen. Waarbij een goede balans tussen het belang van SWV-VO-ZK om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is.

- Binnen SWV-VO-ZK is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van fysieke documenten.

- Het samenwerkingsverband is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert het samenwerkingsverband informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen moeten goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.

- Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt bij SWV-VO-ZK geclassificeerd. De classificatie is het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risicoanalyse, waarbij gebruik gemaakt wordt van de classificatie. Er is een balans tussen de risico's van hetgeen we willen beschermen

en de benodigde investeringen en maatregelen.

- SWV-VO-ZK sluit met alle leveranciers van digitale services (zowel van educatieve als bedrijfsapplicaties) bewerkersovereenkomsten af als zij persoonsgegevens ontvangen van het samenwerkingsverband. Hierbij wordt gebruik gemaakt van de meest recente versie van het convenant 'Digitale leermiddelen privacy' (www en de bijbehorende model bewerkersovereenkomst. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis.

- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht 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. *SWV-VO-ZK heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.*

  ACTIE ! gedragscode opstellen

- Informatiebeveiliging en privacy is bij SWV-VO-ZK een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij SWV-VO-ZK vanaf de start rekening gehouden met informatiebeveiliging en privacy.

3.2 Uitgangspunten privacy

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij SWV-VO-ZK zijn:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie**: bij de verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie**: het samenwerkingsverband legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun Persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen. Wettelijke bewaartermijnen worden in acht genomen: persoonsgegevens worden bewaard tot drie jaar nadat een (toewijzings)besluit is genomen. Na het verstrijken van deze termijnen worden de documenten en andere gegevens op een adequate en veilige wijze verwijderd en vernietigd.

Bij alle registraties op basis van toestemming, zal SWV-VO-ZK aan de Betrokkene een eenduidige zogenaamde Opt-out procedure aanbieden.

4 Wet- en regelgeving

SWV-VO-ZK voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs
- Wet op het Passend Onderwijs (2014)
- Wet goed onderwijs en goed bestuur PO/VO
- Wet bescherming persoonsgegevens
- Algemene Verordening Gegevensbescherming (AVG)

- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van het convenant ‘Digitale onderwijsmiddelen en privacy 3.0’ leidend bij het maken van afspraken met leveranciers.

5 Organisatie

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Dit hoofdstuk beschrijft hoe IBP in SWV-VO-ZK 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 SWV-VO-ZK een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

5.2 Richtinggevend

Eindverantwoordelijke
De bestuurder van het samenwerkingsverband is eindverantwoordelijk voor IBP en stelt het beleid en de basis-maatregelen op het gebied van informatiebeveiliging en privacy vast. De toepassing en werking van het IBP-beleid worden op basis van regelmatige rapportages geëvalueerd.
De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de manager IBP, de directeur van het samen-werkingsverband.
NB Deze taken komen in dit samenwerkingsverband bijeen in één natuurlijke persoon: de directeur-bestuurder.

5.3 Sturend

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

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

De Manager IBP is tevens:

- Portefeuillehouder ICT, is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen SWV-VO-ZK.
- Domeinverantwoordelijke / proceseigenaar
  Binnen het samenwerkingsverband 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 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 proces-eigenaren de volgende specifieke taken:
  - Samen met bestuurder stellen zij het beleid voor toegang vast.

- Samen met functioneel beheer en 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 functioneel beheer en ICT-beheer beoordelen zij regelmatig de toegangsrechten van gebruikers.

Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

Functionaris voor Gegevensbescherming
De functionaris voor gegevensbescherming (FG), of Privacy Officer indien er geen FG is aangesteld, houdt binnen SWV-VO-ZK 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 afhandelen van vertrouwelijke informatiebeveiligingsincidenten. FG heeft regelmatig overleg met manager IBP. De FG is meestal ook de contactpersoon voor klachten en vragen van betrokkenen.
De rol van FG kan bij een jurist, ambtelijk secretaris of controller van de instelling worden belegd. <het kan ook een privacy officer zijn, deze heeft geen wettelijke taken en bevoegdheden die een onafhankelijke positie garanderen>.

ACTIE: een FG kiezen

5.4 Uitvoerend

Security Officer
De Security Officer vormt een technisch aanspreekpunt inzake informatiebeveiliging voor het management en de medewerkers.

Functioneel beheerder
De functioneel beheerder 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.

Actie: uitzoeken of deze twee rollen belegd kunnen worden bij Spaarnesant.

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het personeelshandboek en de handleiding acceptabel gebruikmaken van bedrijfsmiddelen. 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 OR)

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 manager IBP.

6 Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar getoetst en bijgesteld door de directie. Hierbij wordt rekening gehouden met:

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

Daarnaast kent SWV-VO-ZK een jaarlijkse planning- en controlcyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst.

Voor alle overlegmomenten geldt dat deze zoveel mogelijk ingepast worden in bestaande overlegvormen met hetzelfde karakter waarbij op:

- **strategisch** niveau richtinggevend wordt gesproken over organisatie en compliance, alsmede over doelen, scope en ambitie op het gebied van IBP.
- **tactisch** niveau de strategie wordt vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering.
- **operationeel** niveau de onderwerpen worden besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm wordt decentraal georganiseerd, en indien nodig in elk organisatieonderdeel van SWV-VO-ZK

6.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij SWV-VO-ZK 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, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de manager IBP / informatie manager/ Security Officer met het College van Bestuur als eindverantwoordelijke.

6.2 Classificatie en risicoanalyse

Bij SWV-VO-ZK heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de 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 kwaliteitsaspecten die van belang voor de informatievoorziening.

6.3 Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij info@swv-vo-zk.nl. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken.
Meld in de titel van de mail: "incident/datalek op grond van IPB".

6.4 Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij SWV-VO-ZK wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.

Actie: bewustwordingsbijeenkomsten beleggen en houden

Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de directeur-bestuurder, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het SWV-VO-ZK vast te stellen reglement.

Actie: reglement FG vaststellen

Mocht de naleving ernstig tekort schieten, dan kan SWV-VO-ZK de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.
Bij SWV-VO-ZK is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

Actie: protocol meldingen beveiligingsincidenten en datalekken vaststellen.

Bijlage 1: Tabel IBP rollen en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Bestuurder	• 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 = directeur	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert bestuur/CvB/directie 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 • Inrichten van een beveiligd platform voor informatie-uitwisseling	Processen, richtlijnen en procedures IBP, waaronder: • activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Bewerkersovereenkomsten regelen • Brief toestemming gebruik foto's en video • Opstellen informatie documentatie richting leerlingen, ouders / verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ict en internetgebruik • Gedragscode medewerkers en leerlingen
	Functionaris voor Gegevensbescherming / Privacy officer	• Toezicht op naleving privacy wetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement, • procedure IBP-incident afhandeling • Inrichten meldpunt datalekken
	Directeur	• **Classificatie / risicoanalyse** *in samenwerking met Manager IBP (Informatiemanager / verantwoordelijke IBP / Security officer)* • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door *bestuur/CvB/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.	• Inventariseren waar persoonsgegevens van het samenwerkingsverband 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 Vanuit de Wiki
Uitvoerend (operationeel)	Security officer	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten.	
	Functioneel beheerder	• Uitvoeren taken conform gegeven richtlijnen en procedures.	
	Medewerker	• Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.	Communiceren, informeren en toezien op naleving van o.a.:
	Dagelijkse leiding / leidinggevende / directie	• 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.	• IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken