IBP

Informatiebeveiligings- en Privacy Beleid

Inhoud

1. Inleiding

Op 25 mei 2018 wordt de nieuwe Europese Algemene Verordening Gegevensbescherming (AVG) van toepassing. Deze AVG is op een aantal punten strenger dan de huidige Wet bescherming persoonsgegevens. Deze nieuwe privacyregels geven leerlingen en ouders meer controle over hun persoonsgegevens. Ook geldt sinds 1 januari 2016 de meldplicht datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

Met dit document geven we vorm aan een adequate informatiebeveiliging en haken we in op de bewustwordingscampagne die in gang in gezet door de PO-Raad en Kennisnet m.b.t. de privacy persoonsgegevens.

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 Onderwijsgroep Perspecto.

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 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 Onderwijsgroep Perspecto voldoet aan de relevante wet- en regelgeving.

2.2 Reikwijdte

- Het informatiebeveiligings- en privacy beleid binnen Onderwijsgroep Perspecto 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 schoolnetwerk verkregen kan worden.
- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van Onderwijsgroep Perspecto. Het beleid heeft zowel betrekking op gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de school 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 Onderwijsgroep Perspecto waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op andere betrokkenen waarvan Onderwijsgroep Perspecto persoonsgegevens verwerkt.
- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van Onderwijsgroep Perspecto 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 Onderwijsgroep Perspecto heeft raakvlakken met:
    - o Algemeen veiligheids- en toegangsbeveiligingsbeleid
    - o Personeels- en organisatiebeleid
    - o ICT-beleid;
    - o Wet Medezeggenschap op scholen

3. Uitgangspunten

3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten zijn:

• Informatiebeveiliging en 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 Onderwijsgroep Perspecto 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 Onderwijsgroep Perspecto is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van fysieke documenten.

• De stichting is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert Onderwijsgroep Perspecto 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 Onderwijsgroep Perspecto 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.

• Onderwijsgroep Perspecto sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij persoonsgegevens ontvangen van de school. Hierbij wordt gebruik gemaakt van de meest recente versie van de verwerkersovereenkomst zoals die is opgenomen binnen de documenten van Your Safety Net. 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, stagiaires en andere bij de school betrokkenen 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.

Onderwijsgroep Perspecto gebruikt de betreffende documenten uit 'Your Safety Net' om gewenst gedrag te duiden. Vanuit deze documenten wordt een gedragscode geformuleerd met "do's en dont's".

• Informatiebeveiliging en privacy is bij Onderwijsgroep Perspecto een continu proces, waarbij regelmatig wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

• Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt binnen Onderwijsgroep Perspecto vanaf de start rekening gehouden met informatiebeveiliging en privacy.

3.2 Uitgangspunten privacy

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens zijn:

1. Doelbepaling en doelbinding: In het onderwijs zijn o.a. de volgende doelen te benoemen: Onderwijs geven en organiseren, leerlingbegeleiding, leermiddelen verstrekken, informatieverstrekking, communicatiekanalen, websites en ouderbijdragen. 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 staan 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: de school legt vooraf 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.
Bij alle registraties op basis van toestemming, zal Onderwijsgroep Perspecto aan alle betrokkenen (leerlingen en ouders) een eenduidige zogenaamde Opt-out procedure worden aangeboden.

4. Wet- en regelgeving

Onderwijsgroep Perspecto voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

. Wet primair onderwijs
. Wet goed bestuur PO
. Wet bescherming persoonsgegevens (tot 25 mei 2018)
. Algemene Verordening Gegevensbescherming (AVG)
. Archiefwet
. Leerplichtwet
. Auteurswet
. Wetboek van Strafrecht

Onderwijsgroep Perspecto maakt gebruik van de diensten van Your Safety Net om te kunnen voldoen aan de AVG.

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 bij Onderwijsgroep Perspecto 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 Onderwijsgroep Perspecto 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 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 het Stafhoofd P&O.

5.3 Sturend

Stafhoofd P&O adviseert het College van Bestuur en is verantwoordelijk voor het organiseren van IBP binnen Onderwijsgroep Perspecto.
Stafhoofd P&O is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies en stuurt de mensen aan op uitvoerend niveau.

Het Stafhoofd P&O moet:

• Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling waaronder beleid voor toegang.

• De uniformiteit bewaken binnen Onderwijsgroep Perspecto

• Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy

• De verdere afhandeling van incidenten binnen Onderwijsgroep Perspecto coördineren

Functionaris voor gegevensbescherming:

De functionaris voor gegevensbescherming (FG) houdt toezicht op de toepassing en naleving van de AVG.

Als onderdeel van deze verplichting erop toe te zien dat de AVG nageleefd wordt, kunnen FG's met name:

• 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.

Onderwijsgroep Perspecto heeft de intentie om, gezamenlijk met collega scholen, een externe FG aan te wijzen. Deze handelt in opdracht van het College van Bestuur en brengt minimaal één keer per jaar verslag uit.

Domeinverantwoordelijke :

Binnen de onderwijsgroep zijn er verschillende domeinen, zoals ict, personeel, administratie, facilitaire- en financiële zaken, onderwijs etc. Voor de domeinen op het stafbureau zijn de stafhoofden domeinverantwoordelijk. Voor elke school de directeur. Zij zijn verantwoordelijk voor de uitrol van IBP binnen hun domein.

Deze domeinverantwoordelijke 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 domeineigenaren de volgende specifieke taken:

• De directie van elke school/het stafhoofd stelt volgens het beleid voor toegang vast wie welke rechten krijgt vanuit zijn/haar team.

• Samen met BICT zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.

• Samen met BICT beoordelen zij regelmatig de toegangsrechten van gebruikers.

Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

5.4 Uitvoerend

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

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Daarnaast worden medewerkers verwacht zich te houden aan hetgeen vastgelegd in de documenten van Your Safety Net rondom ICT gebruiksbeleid en Privacybeleid.

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.

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 wordt in zijn taak ondersteund worden door BICT en/of Stafhoofd P&O.

6. Controle en rapportage

Dit informatiebeveiligings- en privacybeleid 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 effectiviteit van de genomen maatregelen en aantoonbare werking daarvan.

Daarnaast kent Onderwijsgroep Perspecto 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.

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 wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering.

• operationeel niveau worden de onderwerpen besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm wordt decentraal georganiseerd op de scholen en afdelingen van het stafbureau.

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 Onderwijsgroep Perspecto het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de directie waarbij zij wordt ondersteund door het BICT en/of Stafhoofd P&O.

6.2 Classificatie en risicoanalyse

Bij Onderwijsgroep Perspecto 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. Deze risicoanalyse zal worden uitgevoerd door het Stafhoofd P&O en jaarlijks worden bijgewerkt.

6.3 Incidenten en datalekken

Alle incidenten worden gemeld bij nader vast te stellen e-mailadres "privacy@ogperspecto.nl." De afhandeling van deze incidenten verloopt volgens een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken.

6.4 Registratie gebruik van internet, systeem en applicaties

Uit dit beleid vloeit voort dat het gebruik van alle ICT middelen binnen Onderwijsgroep Perspecto 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.

Alle registraties van persoonsgegevens vallen onder de Wet Bescherming Persoonsgegevens (WBP), dus ook de in dit beleid genoemde registraties. De WBP verstaat onder een persoonsgegeven ‘elk gegeven betreffende een geïdentificeerde of identificeerbare persoon’.

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 directeur van een school of een stafhoofd binnen het stafbureau, na overleg met het College van Bestuur in de vorm van een schriftelijke opdracht. Het CvB beoordeelt of de opdracht voldoet aan de volgende eisen en fiatteert deze daarvoor:

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

6.5 Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat leidinggevenden hun verantwoordelijkheid nemen en medewerkers aanspreken in geval van tekortkomingen. Bij Onderwijsgroep Perspecto wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken en bij uitdienst treden.

Mocht de naleving ernstig tekort schieten, dan kan Onderwijsgroep Perspecto betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

6.6. 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.

Bijlage 1: Tabel IBP rollen en taken

Niveau	**Wie** **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**
Richtinggevend (strategisch)	CvB Stafhoofd P&O	-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	 - Informatiebeveiligings- en privacy beleid - Baseline / basismaatregelen - Privacyreglement vaststellen
Sturend (tactisch)	Stafhoofd P&O	- Inhoudelijk verantwoordelijk voor IBP -IBP-planning en controle - Adviseert CvB 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, gevat binnen Your Safety Net, waaronder: -Activiteitenkalender -Protocol beveiligingsincidenten en datalekken -Verwerkersovereenkomsten 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 -Procedure IBP-incident afhandeling - Inrichten meldpunt datalekken
Functionaris gegevensbescherming (FG)		-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
Domeinverantwoordelijke: Directeuren en Stafhoofden		-Classificatie / risicoanalyse in samenwerking met Stafhoofd P&O -Samen met BICTer op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	-Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) -Classificatie- en risicoanalyse documenten.

	-Samen met BICT de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	

Niveau	**Wie** **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen** **Vanuit Your Safety Net**
Uitvoerend (operationeel)	Directeuren/Stafhoofden BICT	-Incidentafhandeling (registreren en evalueren). -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, 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
	BICT	-Technisch aanspreekpunt voor IBP-incidenten.	