Stichting De Hoeksche School,
openbaar primair en voortgezet onderwijs
Hoeksche Waard

Beleid Informatiebeveiliging en Privacy (IBP)

Vastgesteld door het College van Bestuur d.d. 18 mei 2018
na instemming van de Gemeenschappelijke Medezeggenschapsraad d.d. 15 mei 2018

Biezenvijver 5
3297 GK Puttershoek

www.dehoekscheschool.nl
Telefoon: (078) 629 59 99
secretariaat@dehoekscheschool.nl

Voorwoord

Wetgeving bepaalt niet alleen onder welke voorwaarden persoonsgegevens gebruikt mogen worden, maar geeft ook aan dat er passende technische en organisatorische maatregelen genomen moeten worden om de persoonsgegevens te beschermen.
Om hieraan te voldoen zal een school moeten vastleggen wat er wel en niet met persoonsgegevens gedaan mag worden. Als school moet je weten waar de risico's liggen en wat je eraan kan doen.

Vanaf 25 mei 2018 geldt nog maar één privacywet in de hele Europese Unie. De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer. De AVG is een verordening, dit houdt in dat er rechtstreeks verplichtingen worden opgelegd aan degene die persoonsgegevens verwerken en rechten toekent aan betrokkenen.

Het gaat in eerste instantie niet om technische maatregelen, niet om ict, maar om gedrag, cultuur en bewustwording. Een vastgesteld en bij iedereen bekend gemaakt Informatiebeveligings- en Privacybeleid (IBP-beleid) met duidelijke doelen, uitgangspunten en vastgelegde verantwoordelijkheden vormen dan ook de basis, de kapstok, om IBP goed te regelen.

Het IBP-beleid, met de onderliggende afspraken, procedures en verantwoordelijkheden moet school-breed geïmplementeerd zijn, dan pas is ict aan zet bij de 'technische' uitvoer en monitoring.
IBP is geen techniek feestje, het is een constant bewustzijn van de risico's die een school loopt. Niet alleen risico's waardoor haar continuïteit in zowel het onderwijs als de bedrijfsvoering in gevaar kan komen, maar ook risico's rondom het beschermen van de privacy van leerlingen en medewerkers. Het regelen van IBP begint dan ook met een goedgekeurd en bij iedereen bekend gemaakt IBP-beleid. Dat is de basis om processen, richtlijnen en procedures rondom IBP uit te werken.

Puttershoek, april 2018

1 Inleiding

Het onderwijs 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.

2 Toelichting informatiebeveiliging en privacy

2.1 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.

2.2 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.

2.3 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 Stichting De Hoeksche School, openbaar primair en voortgezet onderwijs Hoeksche Waard en haar scholen.

3 Doel en reikwijdte

3.1 Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan Stichting De Hoeksche School c.q. de scholen persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers
- Beveilgings- 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 er een goede balans moet zijn tussen privacy, functionaliteit en veiligheid. Uitgangspunt is

dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en Stichting De Hoeksche School en haar scholen voldoen aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het informatiebeveiligings- en het privacy beleid binnen Stichting De Hoeksche School geldt voor alle medewerkers (w.o. vrijwilligers), 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.

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van elke school c.q. Stichting De Hoeksche School. Hieronder valt tevens de gecontroleerde informatie, die door de school of het bestuurskantoor zelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop het bestuurskantoor of de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media.

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

- Het beleid geldt voor de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van elke school en het bestuurskantoor van Stichting De Hoeksche School 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. Onder 'bestand' wordt verstaan: een gestructureerde verzameling persoonsgegevens die via een bepaalde logica toegankelijk is.

- Informatiebeveiligings- en privacybeleid binnen Stichting De Hoeksche School 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
  - Beleid inzake aanschaf en gebruik van digitale leermiddelen

4 Uitgangspunten van beleid

De belangrijkste beleidsuitgangspunten bij Stichting De Hoeksche School zijn:

- Stichting De Hoeksche School neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld worden. Het bestuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.

- Stichting De Hoeksche School voldoet aan alle relevante wet- en regelgeving.

- Bij Stichting De Hoeksche School, waaronder alle scholen, 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 Stichting De Hoeksche School om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen te allen tijde hun toestemming intrekken.

- Stichting De Hoeksche School, waaronder alle scholen, 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.

- Stichting De Hoeksche School, waaronder de scholen, legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Stichting De Hoeksche School voldoet hiermee aan de documentatieplicht.

- Binnen Stichting De Hoeksche School 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.

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

- Stichting De Hoeksche School 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.

- Elke school c.q. het college van bestuur sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school c.q. het bestuur, persoonsgegevens verwerken. Dit geldt ook voor 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.

- Informatiebeveiliging en privacy is een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geevalueerd en wordt gekeken of aanpassing gewenst is.

- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij elke school en het bestuurskantoor vanaf de start rekening gehouden met informatiebeveiliging en privacy.

- Stichting De Hoeksche School c.q. de scholen nemen 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 Stichting De Hoeksche School aanvullende afspraken vast over de technische maatregelen.

5 Uitwerking van het beleid

5.1 Relevante wet- en regelgeving

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

- Wet op het primair onderwijs
- Wet op het voortgezet onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet Onderwijstoezicht
- Wet bescherming persoonsgegevens (tot 25 mei 2018)
- Algemene Verordening Gegevensbescherming (AVG) (vanaf 25 mei 2018)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy'

leidend bij het maken van afspraken met leveranciers die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

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 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 is.
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, invulling, 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 binnen Stichting De Hoeksche School geven invulling aan de uitwerking van het beleid. Daarnaast worden alle verwerkingen van persoonsgegevens 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 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.

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 ge-

structureerd 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 FG@dehoekscheschool.nl.
Periodiek zullen de beveiligingsincidenten worden besproken en waar nodig aanvullende passende beleidsmaatregelen worden genomen.

5.7 Planning en controle

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar getoetst en bijgesteld door het college van 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 Stichting De Hoeksche School een jaarlijkse planning en control cyclus voor informatiebeveilging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier eventuele actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving enz. 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 leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Binnen Stichting De Hoeksche School wordt actief aandacht besteed aan IBP ondermeer bij de aanstelling en tijdens functioneringsgesprekken.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het college van bestuur, en heeft een wettelijk omschreven toezichthoudende taak.
Mocht de naleving ernstig tekort schieten, dan kan het college van bestuur de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.9 Logging en monitoring

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

6 Organisatie – wie doet wat?

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.
In tabelvorm wordt weergegeven hoe IBP bij Stichting De Hoeksche School is georganiseerd.

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

Niveau	Wie (Rollen)	Hoe (Verantwoordelijkheid / taken)	Wat (Realiseren/vastleggen)
Richtinggevend (strategisch)	College van Bestuur (cvb)	• 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 • Inhoudelijk verantwoordelijk voor IBP	• Informatiebeveiligings- en privacybeleid • Baseline / basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
Sturend (tactisch)	Functionaris voor gegevensbescherming (FG)	• 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 • 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, in samenspraak met cvb • Afwikkeling klachten en incidenten in samenspraak met cvb • Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • Uitvoeren taken conform gegeven richtlijnen en procedures.	Processen, richtlijnen en procedures IBP, waaronder: • Activiteitenkalender • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Brief toestemming gebruik beeldmateriaal • Opstellen informatie documentatie richting leerlingen, ouders/verzorgers in samenspraak met schoolleiding en cvb • Security awareness activiteiten • Sociale media reglement • Gedragscode ict en internetgebruik • Gedragscode medewerkers en leerlingen • Privacyreglement, • Procedure IBP-incident afhandeling • Inrichten meldpunt datalekken
	Domeinverantwoordelijke/proces-eigenaren, waaronder o.a.: ICT HRM/P&O facilitair onderwijs financiën inkoop administratie	• **Classificatie/ risicoanalyse** in samenwerking met FG • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door cvb • 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 de school terechtkomen (leveranciers lijst); input dataregister • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk

Uitvoerend (operationeel)	Functioneel en/of applicatiebeheerder/ medewerker --- Schoolleiders	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.	--- 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

Bijlage: wie doet wat?

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 op elke school is gemandateerd aan de schoolleider.

Sturend
Functionaris voor Gegevensbescherming (FG)

De FG is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen aan op uitvoerend niveau. De FG moet:
- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de school
- De uniformiteit bewaken binnen de school
- Het aanspreekpunt op school zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen de school coördineren

De FG houdt binnen Stichting De Hoeksche School toezicht op de toepassing en naleving van de AVG. 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 het college van bestuur. De FG heeft regelmatig overleg met het college van bestuur. De FG is meestal ook de contactpersoon voor klachten en vragen van betrokkenen.

Domeinverantwoordelijken binnen de scholen c.q. het bestuurskantoor
Adviseren samen met de schoolleider c.q. de FG het college van bestuur en zijn verantwoordelijk voor het organiseren van informatiebeveiliging binnen hun domein binnen de betreffende school c.q. het bestuurskantoor.

Uitvoerend
Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. 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)

Schoolleiders
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 FG of het college van bestuur.

Toelichting

2.1 Onder informatievoorziening wordt verstaan: apparatuur, programmatuur, gegevens, procedures en mensen.
3.1 Betrokkenen kunnen ook zijn sollicitanten, vrijwilligers en stagiaires.
3.2 Onder ‘bestand’ wordt verstaan: een gestructureerde verzameling persoonsgegevens die via een bepaalde logica toegankelijk is. Denk hierbij bijvoorbeeld aan een archiefkast of een geordende verzameling naam-kaartjes, Er is ook sprake van de verwerking van persoonsgegevens wanneer deze in een bestand worden opgenomen of bestemd zijn om daarin opgenomen te worden. Wat losse papieren op een bureau met daarin de namen van personen vormen geen bestand (mits deze niet digitaal zijn opgeslagen).
4.2 Voldoen aan alle wet- en regelgeving betekent o.a. ook dat er geen illegale software aanwezig is op school en dat leerlingen geen films en games mogen downloaden.