SCHOONHOVENS COLLEGE

Informatiebeveiligings- en privacy beleid (versie 2.0)

Stichting Openbaar Voortgezet Onderwijs Schoonhoven,
handelend onder Schoonhovens College

Formele versie gericht op compliance ***Het informatiebeveiligings- en privacybeleid is aangepast aan de eisen en termen vanuit de AVG. Elke organisatie moet niet alleen de privacywetgeving naleven, maar moet ook aantoonbaar voldoen aan de AVG.***

Bij het template hoort een document met dezelfde inhoud, maar dan voorzien van een aparte toelichting. Die toelichting bevat verdere uitleg en verwijzingen naar onderliggende documenten, afspraken en procedures. Hiermee wordt de 'kapstokfunctie' van het beleid inzichtelijker.

Bron Kennisnet

Bewerkt door: Berend Buddingh' , Wouter Vellema

Versie	Status	Datum	Auteur	Omschrijving
1.0	concept	25 mei		besproken in DV
22 mei 2018	1.1			ter bespreking in DV
29 mei 2018				

Vastgesteld door College van Bestuur StOVOS:

Versie	Datum	Naam	Functie
1.0	25 mei	Berend J. Buddingh'	Voorzitter College van Bestuur

Inhoudsopgave

1 Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ict. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ict. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ict en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van **informatiebeveiliging en privacy** (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

1.1 (hernieuwde) Aanleiding

Op 1 januari 2016 is de meldplicht datalekken ingegaan. Deze meldplicht houdt in dat organisaties een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. In een aantal gevallen moet de organisatie het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Door de invoering van de AVG op 25 mei 2018 is de procedure voor melding aangepast.

1.2. Kader

Iedereen heeft recht op eerbiediging en bescherming van zijn persoonlijke levenssfeer en een zorgvuldige omgang met zijn persoonsgegevens. De regels hiervoor zijn vastgelegd in de AVG. Hierin staat dat de persoonsgegevens die het Schoonhovens College verwerkt moeten worden beveiligd tegen verlies en tegen onrechtmatige verwerking.

Een datalek moet vanaf 1 januari 2016 worden gemeld aan de Autoriteit Persoonsgegevens als het leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Het datalek moet daarnaast ook worden gemeld aan de betrokkene indien het waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.

Het Schoonhovens College hecht grote waarde aan de bescherming van de persoonlijke levenssfeer en een zorgvuldige omgang met persoonsgegevens. Medewerkers van het Schoonhovens College verrichten hun werkzaamheden binnen de kaders van het Schoonhovens College Privacy protocol. Dit protocol vindt zijn oorsprong in en volgt de AVG. Met anderen die gegevens verwerken voor het Schoonhovens College (de zogenaamde verwerkers) is een verwerkersovereenkomst afgesloten. Binnen deze verwerkersovereenkomst wordt het protocol datalekken meegenomen.

2 Toelichting informatiebeveiliging en privacy

Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden. Informatiebeveiliging richt zich op de volgende aspecten:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot ongewenste risico's in het onderwijsproces en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking: *Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.*

Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis voor informatiebeveiliging en privacy, binnen het Schoonhovens College te regelen, en vormt de kapstok voor de onderliggende afspraken en procedures.

3 Doel en reikwijdte

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 het Schoonhovens College persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers.

➢ Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid (IBP-beleid) is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren, waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene (o.a. medewerkers, leerlingen en hun ouders/verzorgers) wordt gerespecteerd en het Schoonhovens College voldoet aan relevante wet- en regelgeving.

Reikwijdte

- Het IBP-beleid binnen het Schoonhovens 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 Schoonhovens College, waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Schoonhovens College persoonsgegevens verwerkt.

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van het Schoonhovens 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 het Schoonhovens 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 Schoonhovens College raakvlakken met:

o *Algemeen veiligheids- en toegangsbeveiligingsbeleid*; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
o *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers,
functiewisselingen, functiescheiding en vertrouwensfuncties
o *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen o *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers

4 Beleid – Hoe doen we dat?

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

1. StOVOS, schoolbestuur van Schoonhovens 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. Schoonhovens College voldoet aan alle relevante wet- en regelgeving.

3. Bij Schoonhovens 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 Schoonhovens College om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen te allen tijde hun toestemming herzien.

4. Schoonhovens 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. Schoonhovens College legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Schoonhovens College voldoet hiermee aan de documentatieplicht.

6. Binnen Schoonhovens College 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. Schoonhovens 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. Schoonhovens 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. Schoonhovens 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. Schoonhovens College verwacht van alle medewerkers, leerlingen, bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen, met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Schoonhovens College heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij Schoonhovens College een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

12. Schoonhovens 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. Schoonhovens 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. Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt, legt Schoonhovens College aanvullende afspraken vast over de technische maatregelen.

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

5 Uitwerking van het beleid – Wat doen we?

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

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
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Wet bescherming persoonsgegevens
- Algemene Verordening Gegevensbescherming (AVG; vanaf 25 mei 2018)*
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

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

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.

Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens (art.5 AVG) leidend. Deze zijn samengevat in de **vijf vuistregels** met betrekking tot de omgang met persoonsgegevens te weten:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.

3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding staan tot het doel (proportioneel). Het doel kan niet

met minder, alternatieve of andere gegevens worden bereikt (subsidiair). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

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.

Ondersteunende richtlijnen en procedures

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

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. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP, de FG, en de Security Officer met het bestuur als eindverantwoordelijke.

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.

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 in het kader van de privacy worden vastgelegd in een incidentenregister. Deze (beveiligings)incidenten kunnen worden gemeld bij

incidentenregister@schoonhovenscollege.nl Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

Planning en controle

Dit IBP-beleid wordt minimaal elke drie 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 Schoonhovens College 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. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

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 bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, etcetera. Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het bestuur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement.

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

Logging en monitoring

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

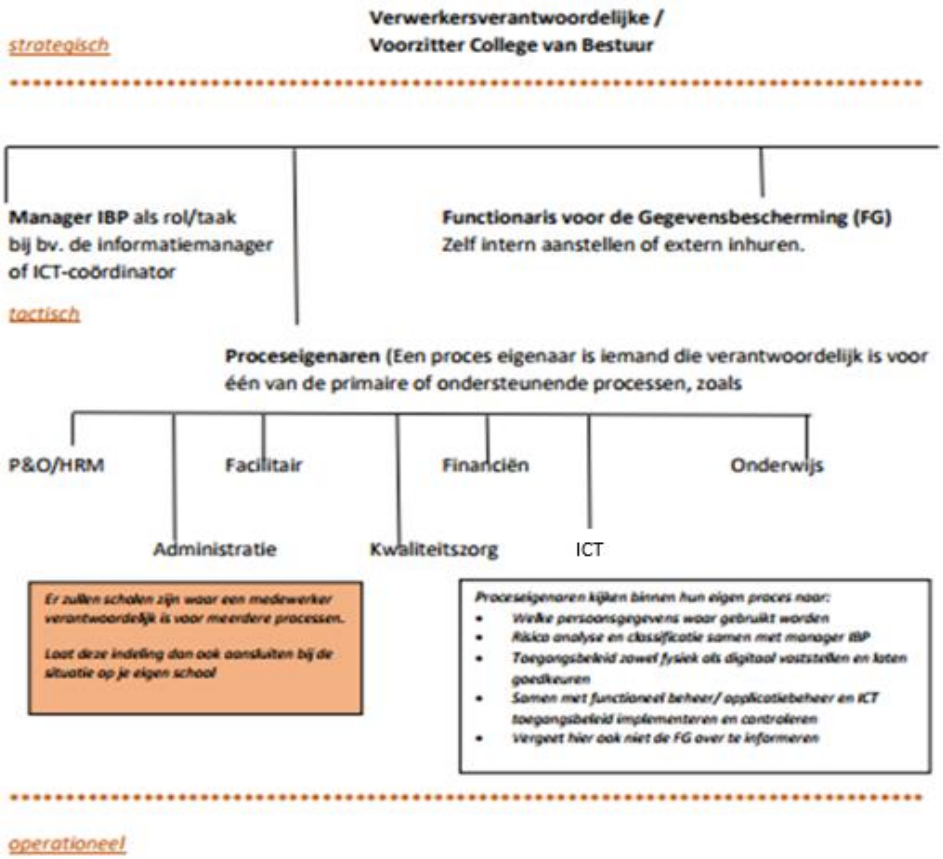
6 Organisatie - Wie doet wat?

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. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij Schoonhovens College.

De vormgeving van IBP

De rollen binnen IBP zijn hieronder schematisch weergegeven:



- **Security Officer of hoofd ict**: het technisch aanspreekpunt als gaat om het oplossen en uitzoeken van beveiligingsincidenten (in samenwerking met de manager IBP).
  LET OP: *Als de school het ict-beheer elders heeft ondergebracht (bv bij outsourcing), dan moeten er afspraken gemaakt worden over waar welke verantwoordelijkheden en taken liggen.*
- **Functioneel beheer/ applicatiebeheer** : uitvoeren van toegangsrechten, instellingen en procedures zoals aangegeven in de goedgekeurde richtlijnen.
- **Dagelijkse leiding/ locatiedirectie**: Communiceren, informeren en toezien op naleving van de gemaakte afspraken en procedures.
- **Medewerkers:** IBP toepassen in dagelijkse werkzaamheden; IBP is de verantwoordelijkheid van ieder individu.

Elke rol

De rol van de verwerkersverantwoordelijke:

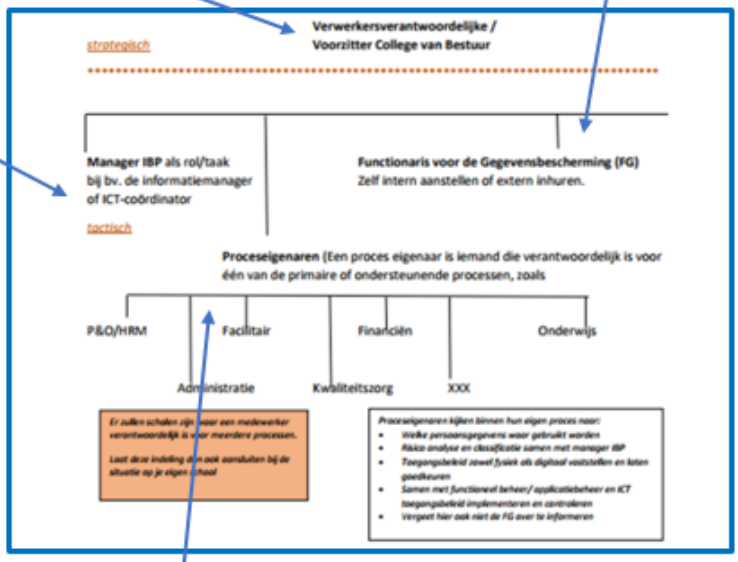
Verantwoordelijkheden	Taken
• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren van toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacy beleid • Baseline/basismaatregelen • Privacyreglement vaststellen

De rol van de Manager IBP:

Verantwoordelijkheden
• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert bestuur/CVB/directie over IBP • Voorbereiden uitvoering 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.
Taken
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

Gegevensbescherming (FG):

Een FG is een interne toezichthouder op de verwerking van persoonsgegevens binnen een organisatie. Deze functionaris heeft geen formele sanctiebevoegdheden, maar wel controlebevoegdheden. Hij adviseert het schoolbestuur (bevoegd gezag) over privacy en houdt toezicht daarop, handelt vragen en klachten over privacy af, ontwikkelt (interne) regelingen rondom privacy en geeft advies over technologie en beveiliging (privacy by design).



ICT

De rol van de proceseigenaren:

Verantwoordelijkheden	Taken
• Classificatie/risicoanalyse in samenwerking met Manager IBP • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur/cvb/directie • Samen met functioneel beheer en ICT-beheer erop toezien dat gebruikers allen 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 terecht komen (Leverancierslijst) • Classificatie- en risicoanalyse • Toegangsmatrix diverse informatiesystemen en netwerk. • Overige aanvullende beleidsstukken, richtlijnen, procedures en protocollen met manager IBP opstellen.

Onder in het schema bevindt zich het operationele niveau. Hier vindt de uitvoering plaats van dat wat op strategisch en tactisch niveau is vastgesteld.

- **Security Officer of hoofd ict**: het technisch aanspreekpunt als gaat om het oplossen en uitzoeken van beveiligingsincidenten (in samenwerking met de manager IBP).
  LET OP: *Als de school het ict-beheer elders heeft ondergebracht (bv bij outsourcing), dan moeten er afspraken gemaakt worden over waar welke verantwoordelijkheden en taken liggen.*
- **Functioneel beheer/ applicatiebeheer** : uitvoeren van toegangsrechten, instellingen en procedures zoals aangegeven in de goedgekeurde richtlijnen.
- **Dagelijkse leiding/ locatiedirectie**: Communiceren, informeren en toezien op naleving van de gemaakte afspraken en procedures.
- **Medewerkers**: IBP toepassen in dagelijkse werkzaamheden; IBP is de verantwoordelijkheid van ieder individu.

Ook deze rollen hebben verantwoordelijkheden en taken:

Rol	Verantwoordelijkheden	Taken
Security officer	• Incidentafhandeling (registreren en evalueren) • Technisch aanspreekpunt voor IBP-incidenten.	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerlingdossiers • Wie mogen wat zien • Gedragscode • Omgaan met social media • Mediawijs maken Het gaat hier dus om het naleven, signaleren en aanspreken op beleid etc. dat op strategisch en tactisch niveau is vastgesteld. Deze rollen leggen hierover verantwoording af aan de manager IBP en de verwerkersverantwoordelijke.
Functioneel beheerder	• Uitvoeren taken conform gegevens richtlijnen en procedures	
Medewerkers	• Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden	
Dagelijkse leiding/leidinggevende/directie	• Communicatie naar alle betrokkenen; ervoor zorgen dat medewerkers op de hoogte zijn van IBP-beleid en de consequenties hiervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen • Periodiek het onderwerp informatiebeveiliging onder de aandacht brengen in werkoverleggen, beoordelingen etc. • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur.	

Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

Documenten: Aandachtspunten:

- Procedure toestemming gebruik beeldmateriaal (toestemmingsbrief)
- Procedure voor verwijderen van gegevens (bewaartermijnen)
- Communicatierechten betrokkenen (communicatie richting betrokkenen)
- Procesbeschrijving rechten betrokkenen (proces rondom aanvragen van betrokkenen)
- Privacyreglement Autorisatiematrix (wie mogen gegevens inzien, bewerken enz.)
- Afspraken gebruik sociale media
- Procedure rondom training medewerkers (bewustzijn creëren)
- Cameratoezicht
- Wachtwoordbeleid
- Responsible disclosure
- Gedragscode ict en internetgebruik
- Acceptable use policy (verantwoord gebruik bedrijfsmiddelen)
- Procedure rondom uitwisselen gegevens (passend onderwijs, leerlingdossiers, leerplicht enz)

Verplicht vanuit de AVG:

- Procesbeschrijving melden datalekken
- Registratie beveiligingsincidenten
- Dataregister om te voldoen aan de registratieplicht
- Verwerkersovereenkomsten (privacybijlage beschikbaar stellen)
- Procedure gegevensbeschermingseffectbeoordeling (DPIA)
- Risicoanalyse
- Functionaris voor Gegevensbescherming (communicatie hierover richting medewerkers)

Bijlage 2: Organisatie; wie doet wat

Deze bijlage beschrijft hoe IBP op drie niveaus wordt georganiseerd.

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

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

Richtinggevend

Eindverantwoordelijke 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 de manager IBP.

Sturend

Manager IBP

Manager IBP (verantwoordelijke IBP, informatiemanager of privacy officer) is een rol op sturend niveau. Hij geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau. De manager IBP moet:

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

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG), of Privacy Officer indien er geen FG is aangesteld, houdt binnen Schoonhovens 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 manager IBP. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

Portefeuillehouder ICT / ICT beheer (intern)

Adviseert samen met manager IBP (of informatiemanager) de eindverantwoordelijke en is

verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen Schoonhovens College.

Domeinverantwoordelijke / proceseigenaar
Binnen de school zijn er verschillende domeinen/processen, zoals ict, personeel (HRM, P&O), administratie, kwaliteitszorg, 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 proceseigenaren de volgende specifieke taken:

- Samen met de eindverantwoordelijke stellen zij het beleid voor toegang (autorisaties) 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 en voor hun werkzaamheden toegang toe moeten hebben.
- Samen met functioneel beheer en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

Uitvoerend

Security Officer (SO) De Security Officer vormt een technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers. Gezien de omvang van de huidige organisatie wordt deze functie gecombineerd met ICT beheer.

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 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.

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy 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 wordt 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 IBP-beleid;

- toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeelgerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de manager IBP. Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

Indien aan de orde, bij majeure datalekken: Een IBP-team wordt organisatiebreed zowel preventief als curatief benoemd voor informatiebeveiliging en privacy incidenten. De leden van het IBP-team zijn benoemd door de eindverantwoordelijke en handelen in diens opdracht. Het IBP-team van Schoonhovens College heeft de volgende opdracht:

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

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

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

Het IBP-team bij Schoonhovens College behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy-incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident. De werkzaamheden van het IBP-team bij Schoonhovens College is gedocumenteerd en door de eindverantwoordelijke bekrachtigd.

Onderstaande bijlagen worden separaat verstrekt:
Bijlage 4 Overzicht relevante wettelijke bewaartermijnen i.o.

Bijlage 5 Overzicht be- en verwerkersovereenkomsten i.o.

Bijlage 6 Overzicht verwerking persoongegevens dataregister) i.o.

Bijlage 7 Overzicht verwerking leerlinggegevens (dataregister) i.o.

Bijlage 3: De 6 wettelijke grondslagen vd AVG

4 APRIL 2018 BY CHARLOTTE MEINDERSMA

De AVG (GDPR) kent 6 grondslagen. Om persoonsgegevens te mogen verwerken, moet je gebruik kunnen maken van een van deze grondslagen. Kan dat niet, dan mag je ook de persoonsgegevens niet verwerken. Soms kun je zelfs uit meerdere grondslagen kiezen. Iene miene mutte doen is dan niet zo verstandig. Hoe bepaal je dan wel de juiste grondslag?

Waarom moet je weten welke grondslag je gebruikt? De AVG zegt dat de verwerking alleen rechtmatig is als er aan ten minste een van de grondslagen wordt voldaan. Prima, zou je denken, even het lijstje aflopen, kijken of je er een kunt gebruiken en of je er iets extra's voor moet doen en gaan! Niet te moeilijk. Klopt op zich wel, maar je moet vanwege je informatieverplichting ook vertellen van welke grondslag je gebruikmaakt. Bijna iedereen zorgt dat zijn/haar organisatie aan de informatieverplichting voldoet door middel van een privacyverklaring. Je mag niet van grondslag wisselen, dus je moet goed van te voren hebben bedacht van welke grondslag je gebruikmaakt. Je moet dus vooraf de grondslag kiezen en niet achteraf je verwerkingen rechtvaardigen door er een grondslag bij te zoeken.

Toestemming De eerste grondslag die de AVG noemt is de toestemming. Toestemming kan gegeven worden door een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting. De toestemming moet uitdrukkelijk zijn. Stilzwijgende toestemming is niet voldoende. De vereisten voor toestemming zijn strenger geworden dan ze onder onze huidige privacywet, de Wet bescherming persoonsgegevens, waren. Bovendien mag toestemming ook weer worden ingetrokken en moet dat net zo gemakkelijk zijn als het geven van de toestemming. Als dat gebeurt ben je dus je grondslag kwijt en mogen de persoonsgegevens niet meer verwerkt worden. Deze grondslag is vooral een vangnet, een soort restbepaling, voor het geval je van geen van de andere grondslagen gebruik kunt maken.

Uitvoering van de overeenkomst De tweede grondslag maakt verwerking van persoonsgegevens mogelijk wanneer dat nodig is voor de uitvoering van de overeenkomst. Het gaat dan uiteraard om een overeenkomst waarbij de betrokkene (de persoon waarvan de persoonsgegevens zijn) partij is. Belangrijk is dat de overeenkomst niet uitgevoerd kan worden zonder die persoonsgegevens. Denk bijvoorbeeld aan een webwinkel die een naam en adres nodig heeft om producten te kunnen leveren. Is het verwerken van de persoonsgegevens alleen maar handig, maar niet noodzakelijk, dan kan deze grondslag niet gebruikt worden.

Wettelijke verplichting Soms bestaat er een wettelijke verplichting op basis waarvan je persoonsgegevens wel moet verwerken. Die verplichtingen staan dan in een andere wet. Denk bijvoorbeeld aan facturen die 7 jaar bewaard moeten worden. Je bent niet verplicht om daar een contactpersoon in op te nemen, maar gegevens van eenmanszaken zijn ook persoonsgegevens. Je moet dan toch die factuur, juist inclusief die gegevens van de eenmanszaak, bewaren. Ook loonadministratie moet 7 jaar bewaard worden. Daaronder vallen ook de arbeidsovereenkomsten, ziektestaten en een kopie identiteitsbewijs.

Vitale belangen Om de vitale belangen van een natuurlijk persoon te kunnen beschermen, mogen de persoonsgegevens verwerkt worden. Maar alleen als de verwerking noodzakelijk is om die vitale belangen te kunnen beschermen. Er is niet zo snel sprake van een vitaal belang. Vitaal wil zeggen dat het gaat om het leven van de persoon. Niet zozeer de algemene medische gegevens, maar wel in het geval van een ongeval, bijvoorbeeld, waarbij persoonsgegevens verwerkt worden om iemand op dat moment te kunnen behandelen. Van deze grondslag kan, maar ook mag bijna nooit gebruik gemaakt worden. Deze grondslag mag alleen worden gebruikt als een andere grondslag niet mogelijk is en er toch een noodzaak bestaat om de gegevens te verwerken om het vitale belang te beschermen.

Algemeen belang Als er een taak van algemeen belang vervuld moet worden waarvoor de verwerking van persoonsgegevens noodzakelijk is, dan mogen de persoonsgegevens verwerkt worden. Dit geldt ook voor taken in het kader van de uitoefening van het openbaar gezag die aan de verwerkersverantwoordelijke zijn opgedragen. Hieronder vallen onder meer de gebruikelijke verwerkingen van, voor of namens de overheid. Voor deze grondslag zal meestal ook een andere wettelijke grondslag moeten bestaan. Bijvoorbeeld omdat in een wet een bepaalde taak of verplichting is opgenomen. Een van de rechten van de betrokken, uit de AVG, is het recht op gegevenswissing. Ook wel bekend als het recht op vergetelheid. Als persoonsgegevens echter op de grondslag algemeen belang worden verwerkt, dan bestaat het recht op gegevenswissing niet. Misschien ook niet zo gek, want anders zouden gemeenten de BRP (Basisregistratie Personen, waaronder het voormalige GBA valt) niet bij kunnen houden.

Gerechtvaardigd belang Het gerechtvaardigd belang is eigenlijk vooral een belangenafweging. De verwerking moet noodzakelijk zijn voor de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of een derde, tenzij de privacybelangen van de betrokkene zwaarder wegen. Hierbij moet bijvoorbeeld rekening gehouden worden met de vraag in hoeverre de betrokkene had mogen verwachten dat de verwerking plaats zou vinden en met welk doel dan. Dit belang kan bijvoorbeeld gebruikt worden om direct marketing mogelijk te maken. Let wel op dat een betrokkene altijd bezwaar mag maken tegen direct marketing en de verwerking dan moet stoppen. Het gerechtvaardigd belang is ook belangrijk voor fotografen die bijvoorbeeld fotograferen op evenementen, journalistieke of documentaire fotografie verzorgen waarbij een quitclaim niet mogelijk is of wanneer het gaat om straatfotografie.

Doelbinding Naast een geldige grondslag, is er ook nog een gerechtvaardigd doel nodig. Gegevens mogen op basis van een grondslag verwerkt worden, maar dat mag alleen voor een bepaald doel. Die doelen staan niet in de AVG genoemd, maar moeten dus wel gerechtvaardigd zijn. De verwerking van de persoonsgegevens mag alleen plaatsvinden voor dat doel. Ook die doelen moeten in de privacyverklaring worden opgenomen. Zo kun je bijvoorbeeld op basis van het gerechtvaardigd belang persoonsgegevens verwerken voor direct marketingdoeleinden. Soms kan een grondslag ook samenvallen met een doel. Zo kun je op basis van de grondslag wettelijke verplichting persoonsgegevens verzamelen met als doel te voldoen aan de administratieve bewaarplicht.