



Informatiebeveiligings- en privacybeleid

Bron

Stichting Kennisnet

Bewerkt voor:

Scholengroep Holland

Vastgesteld door Scholengroep Holland:

Versie	Datum	Naam	Functie
		Denk Tank Directeuren overleg	Feedback ophalen en bespreken Besproken en positief advies.
		G.M.R R.v.T. C.vB.	13 november 2024 20 november 2024/17 februari 2025 24 Maart 2025

In het beleidsplan vind je tussen rechte haken [x.x] de referentie naar de norm uit het Normenkader IBP.

Inhoud

HET BELANG VAN INFORMATIEBEVEILIGING EN PRIVACY	3
TOELICHTING INFORMATIEBEVEILIGING EN PRIVACY	3
TOELICHTING PRIVACY	4
VERVLECHTING INFORMATIEBEVEILIGING EN PRIVACY	4
DOEL EN REIKWIJDTE	4
DOEL	4
REIKWIJDTE	5
BELEID – HOE DOEN WE DAT?	5
UITWERKING VAN HET BELEID – WAT DOEN WE?	8
RELEVANTE WET- EN REGELGEVING	8
BASISREGELS BIJ HET OMGAAN MET PERSOONSGEGEVENS	8
ONDERSTEUNENDE RICHTLIJNEN EN PROCEDURES	9
VOORLICHTING EN BEWUSTZIJN	9
CLASSIFICATIE EN RISICOANALYSE	9
INCIDENTEN EN DATALEKKEN	10
PLANNING EN CONTROLE	10
NALEVING EN SANCTIES	10
LOGGING EN MONITORING	11
CONFIGURATIEMANAGEMENT	11
DATAOPSLAG EN ARCHIVERING	11
KADERS VOOR AUTHENTICATIE	11
ORGANISATIE - WIE DOET WAT?	12
ROLLEN EN VERANTWOORDELIJKHEDEN	12
BIJLAGE 1: ONDERSTEUNENDE RICHTLIJNEN EN PROCEDURES	14
DOCUMENTEN	14
VERPLICHT VANUIT DE AVG:	14

Visie op ICT in het onderwijs

Voor kinderen is (digitale) geletterdheid- en gecijferdheid een voorwaarde om zelfstandig onderdeel te kunnen zijn van - en bij te dragen aan onze maatschappij. Scholengroep Holland zet zich in voor eerlijke kansen voor ieder kind. ICT is een middel om het onderwijs toegankelijk en effectief te maken. Elke leerling krijgt toegang tot een goed werkend device, veilig internet en digitale leermiddelen die aangepast zijn aan hun behoeften, inclusief voor leerlingen met beperkingen. ICT wordt ingezet om leerlingen actief bij hun leerproces te betrekken, samenwerking en kritisch denken te stimuleren, en hen digitale vaardigheden bij te brengen. Het gebruik van adaptieve technologieën zorgt voor gepersonaliseerde ondersteuning, met aandacht voor verantwoorde omgang met data en het voorkomen van vooroordelen. Scholengroep Holland streeft ernaar leerlingen niet alleen digitaal vaardig te maken, maar ook verantwoordelijk en kritisch in hun omgang met de digitale wereld.

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. Om onze leerlingen en ons personeel een veilige werk- en leeromgeving te bieden, is het beschermen van de privacy van groot belang. Het onze plicht 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.

Toelichting informatiebeveiliging en privacy

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 imagooverlies.

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 zijn samengevoegd tot één proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis op informatiebeveiliging en privacy binnen Scholengroep Holland te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

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 Scholengroep Holland 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 Scholengroep Holland voldoet aan relevante wet- en regelgeving.

Reikwijdte

- Het IBP-beleid binnen Scholengroep Holland 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 Scholengroep Holland waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Scholengroep Holland persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Scholengroep Holland. 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 Scholengroep Holland 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 Scholengroep Holland raakvlakken met:
 - *Algemeen veiligheids- en toegangsbeveiligingsbeleid*; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging [PH.01, PH.02], crisismanagement [BC.05], huisvesting en ongevallen;
 - *Personeels- en organisatiebeleid* [OR, HR]; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties;
 - *IT-beleid* [OP]; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen, verantwoord gebruik bedrijfsmiddelen en gebruik eigen devices, toegangsbeheer;
 - *Medezeggenschap* van ouders/verzorgers van leerlingen en medewerkers.

Beleid – Hoe doen we dat?

Scholengroep Holland hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het College van Bestuur van Scholengroep Holland 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. Scholengroep Holland voldoet aan alle relevante wet- en regelgeving.
3. Bij Scholengroep Holland 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 Scholengroep Holland om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming herzien.
4. Scholengroep Holland 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.
5. Scholengroep Holland legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Scholengroep Holland voldoet hiermee aan de documentatieplicht.
6. Binnen Scholengroep Holland 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. Scholengroep Holland is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de organisatie informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en (de ouder(s) / verzorger(s) van de) leerlingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
8. Scholengroep Holland classificeert informatie en informatiesystemen *[DM.02]*. De classificatie is het uitgangspunt voor de risicoanalyse *[RM]* en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken, de benodigde investeringen en de te nemen maatregelen.
9. Scholengroep Holland 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 *[sc]*.

10. Scholengroep Holland verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagooverlies. Scholengroep Holland heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
11. Informatiebeveiliging en privacy is bij Scholengroep Holland een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
12. Scholengroep Holland 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 [CH.01, CH.02].
13. Scholengroep Holland neemt passende technische (beveiligings-)maatregelen [ID, CO, SM] en organisatorische maatregelen [GO, OR, BL, OI] om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.
14. Daar waar de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt, legt Scholengroep Holland aanvullende afspraken vast over de technische maatregelen [SC].
15. Scholengroep Holland zal alle beveiligingsincidenten [IM.01] vastleggen en datalekken volgens een vast protocol afhandelen en waar nodig melden/aangeven bij de Autoriteit Persoonsgegevens, andere toezichthouders en waar nodig aan de betrokkenen.

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 primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra;
- Wet goed onderwijs en goed bestuur PO/VO;
- Wet onderwijstoezicht;
- Algemene Verordening Gegevensbescherming;
- Archiefwet;
- Leerplichtwet;
- Auteurswet;
- Wetboek van Strafrecht.
- Wet medezeggenschap op scholen.

Het Normenkader Informatiebeveiliging en Privacy (IBP), dat voor de onderwijssector voor dit doel is ontwikkeld, gebruiken we als referentiekader voor de te nemen beveiligings- en privacy maatregelen.

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 tot het doel (proportioneel). Het

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

4. **Transparantie:** de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit:** er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

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 *[HR.06]* van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP, de Functionaris voor Gegevensbescherming (FG) en de Privacy Officer met het College van Bestuur als eindverantwoordelijke.

Classificatie en risicoanalyse

Alle informatie heeft waarde. Daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd *[DM.02]*. 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. De aanpak en uitvoering van de risicoanalyse is beschreven in de risicobeoordelingsdocumenten.

Bij wijzigingen *[CH.02]* 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 *[RM.02, RM.03]*. 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 [IM.01]. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken [IM.02]. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister. Alle (beveiligings)incidenten kunnen worden gemeld bij privacyteam@scholengroepholland.nl.

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

Planning en controle

Dit IBP-beleid wordt minimaal elke twee jaar getoetst en bijgesteld door het bestuur [GO.03]. 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 Scholengroep Holland een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen. Aan het einde van elk jaar wordt in een jaarverslag de behaalde doelen en de actuele status van de volwassenheidsniveau's in het IBP Normenkader beschreven. In het Jaarplan worden de te halen doelen voor het volgende jaar beschreven. En de Strategiebepaling stelt hoe volwassenheidsniveau 3 op alle domeinen van het Normenkader IBP behaald gaat worden uiterlijk in 2027.

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 leidinggevend en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling [HR.01]: tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.

Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door het bestuur vast te stellen reglement.

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

Logging en monitoring

Logging [SM.04] en monitoring door de IT-afdeling zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk. Het beheer van de logische toegang is vastgelegd in een identity & access plan [ID.01, ID.02].

Configuratiemanagement

Alle informatie van en over IT-componenten binnen de organisatie wordt bijgehouden. Er wordt vastgelegd welke hardware er zijn, welke software gebruikt wordt, welke updates zijn uitgevoerd en welke instellingen gehanteerd worden [CO.01, CO.02].

Dataopslag en archivering

Er zijn procedures gedefinieerd en geïmplementeerd voor het effectief en veilig opslaan, bewaren en archiveren van gegevens. Hierin worden niet alleen wettelijke vereisten en contractuele verplichtingen meegenomen, maar ook de organisatiedoelstellingen [DM.04].

Kaders voor Authenticatie

Authenticatiemechanismen zorgen voor geoorloofde toegang tot systemen en gegevens door de identiteit van gebruikers vast te stellen. Dit zorgt ook voor het tegengaan van ongeoorloofde toegang. Alle gebruikers moeten uniek identificeerbaar zijn. Er moet periodiek gecontroleerd worden of er onjuiste of inactieve gebruikers zijn [SM.02].

Tweefactorauthenticatie is vereist voor niet vertrouwde omgevingen en kritieke systemen.

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 [OR.01] bij Scholengroep Holland.

Niveau	Wie Rollen	Hoe Verantwoordelijkheid/ taken	Wat Realiseren/ vastleggen
Richtinggevend (Strategisch)	CvB	- Eindverantwoordelijk - IBP-beleidsvorming, -vastlegging en het uitdragen ervan - Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens - Evaluëren toepassing en werking IBP-beleid op basis van rapportages - Organisatie IBP inrichten	- Informatiebeveiligings- en privacy beleid - Baseline/ basismaatregelen - Reglement FG vaststellen - Privacyreglement vaststellen
	Privacy Officer (De persoon die inhoudelijk verantwoordelijk is voor IBP)	- Inhoudelijk verantwoordelijk voor IBP - IBP-planning en controle - Adviseert bestuur/CvB/directie over IBP - Vorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse - Hanteren IBP-normen en wijze van toetsen - Evaluëren 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, waaronder: - Activiteitenkalender - Protocol beveiligingsincidenten en datalekken - Verwerkersovereenkomsten regelen - Brief toestemming gebruik beeldmateriaal - Opstellen informatie documentatie richting leerlingen, ouders/ verzorgers - Security awareness activiteiten - Sociale media reglement - Gedragscode ict en internetgebruik - Gedragscode medewerkers en leerlingen
	Functionaris voor Gegevensbescherming en/of Privacy Officer	- 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 - Afwikkeling klachten en incidenten	- Privacyreglement, - Procedure IBP-incident afhandeling - Inrichten meldpunt datalekken
Sturend (Tactisch)	Domeinverantwoordelijke/ Proceseigenaren Waaronder o.a.:	Classificatie/ risicoanalyse in samenwerking met Manager IBP (Informatiemanager/ verantwoordelijke IBP/ privacy Officer) - Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur/CvB/directie - Samen met functioneel beheer en ICT-beheer erop 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.
	ICT, HRM/ P&O, Facilitair, Onderwijs, Financiën, Inkoop en Administratie		Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: Toegangsmatrix diverse informatiesystemen en netwerk

Uitvoerend (Operationeel)	Privacy 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 leerling dossiers - Wie mogen wat zien - Gedragscodes - Omgaan met sociale media - Mediawijs maken
	Functioneel en/of applicatie beheerder/ ICT-coördinator	Uitvoeren taken conform gegeven richtlijnen en procedures.	
	Medewerker	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 het IBP-beleid en de consequenties ervan. - Toeziën 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.	

Een uitgebreidere beschrijving van de verschillende rollen met de verantwoordelijkheden en de te realiseren doelen zijn vastgelegd in [Voorlopige Rolbeschrijvingen IBP Beleid \(concept 0.9\).pdf](#).

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

- Procedure toestemming gebruik beeldmateriaal (toestemmingsbrief)
- Procedure voor verwijderen van gegevens (bewaartermijnen)
- Communicatie rechten van 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)
- Gedragscodes ICT en internetgebruik (verantwoord gebruik bedrijfsmiddelen)
- Procedure rondom uitwisselen gegevens (passend onderwijs, leerling dossiers, leerplicht enz.)

Verplicht vanuit de AVG:

- Procesbeschrijving melden datalekken
- Registratie beveiligingsincidenten
- Dataregister om te voldoen aan de registratieplicht
- Verwerkersovereenkomsten (privacy bijlage beschikbaar stellen)
- Procedure gegevensbeschermings-effectbeoordeling (DPIA)
- Risicoanalyse
- Functionaris voor Gegevensbescherming (communicatie richting medewerkers)