



IBP Beleidsstuk

Vastgesteld, 27 juni 2018

F. Meeuwes, voorzitter College van Bestuur

1	INLEIDING	4
1.1	TOELICHTING INFORMATIEBEVEILIGING.....	4
1.2	TOELICHTING PRIVACY.....	4
1.3	VERVLECHTING INFORMATIEBEVEILIGING EN PRIVACY.....	4
2	DOEL EN REIKWIJDTE	5
2.1	DOEL.....	5
2.2	REIKWIJDTE.....	5
3	UITGANGSPUNTEN	6
3.1	ALGEMENE BELEIDSUITGANGSPUNTEN	6
3.2	UITGANGSPUNTEN PRIVACY.....	7
4	WET- EN REGELGEVING	8
5	ORGANISATIE	8
5.1	ROLLEN (FUNCTIES) RONDOM IBP	8
5.2	RICHTINGGEVEND.....	9
5.3	STUREND	9
5.4	UITVOEREND.....	10
6	CONTROLE EN RAPPORTAGE.....	10
6.1	VOORLICHTING EN BEWUSTZIJN	11
6.2	CLASSIFICATIE EN RISICOANALYSE.....	11
6.3	INCIDENTEN EN DATALEKKEN	11
6.4	PLANNING EN CONTROLE.....	12
6.5	NALEVING EN SANCTIES	12
6.6	LOGGING EN MONITORING	12
BILAGE 1: TABEL IBP ROLLEN EN TAKEN		13

4

1 Inleiding

Het onderwijsveld is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. Ook neemt de hoeveelheid informatie toe door ontwikkelingen als gepersonaliseerd leren met ICT. Deze afhankelijkheid van ICT en gegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het is van belang om adequate maatregelen te nemen op het gebied van informatiebeveiliging en privacy (IBP) om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

1.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening te garanderen.

Deze aspecten zijn:

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

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

1.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform huidige wet – en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die herleidbaar zijn tot een bepaald individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. De wet noemt als voorbeelden van verwerking: *het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.*

1.3 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijk onderdeel is van privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebe-

4

veiliging. 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 Gewoon Speciaal.

2 Doel en reikwijdte

2.1 Doel

Dit beleid heeft als doelen:

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

Dit beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet zijn tussen privacy, functionaliteit en veiligheid. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene, met name van medewerkers en leerlingen, wordt gerespecteerd en Gewoon Speciaal voldoet aan relevante wet- en regelgeving.

2.2 Reikwijdte

- Het informatiebeveiligings- en het privacy beleid binnen Stichting Gewoon Speciaal geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreeerde) bezoekers en externe relaties (inhuur/ outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van Stichting Gewoon Speciaal. Het beleid heeft zowel betrekking op gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites.
- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Stichting Gewoon Speciaal waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreeerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op andere betrokkenen waarvan Gewoon Speciaal persoonsgegevens verwerkt.
- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van Gewoon Speciaal evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het beleid is ook van toepassing op niet-geautomati-

tl

seerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

- IBP-beleid binnen Stichting Gewoon Speciaal 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

3 Uitgangspunten

3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij Stichting Gewoon Speciaal zijn:

- Informatiebeveiliging en het privacy dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Algemene Verordening Gegevensbescherming (die 25 mei 2018 in werking treedt).

De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen. Waarbij een goede balans tussen het belang van Stichting Gewoon Speciaal om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is.
- Binnen Stichting Gewoon Speciaal is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van fysieke documenten.
- De school 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 moeten goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.
- Stichting Gewoon Speciaal sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) bewerkersovereenkomsten af als zij persoonsgegevens ontvangen van de school. Hierbij wordt gebruik gemaakt van de meest recente versie van het convenant 'Digitale leermiddelen privacy' ([www](#)) en de bijbehorende model bewerkersovereenkomst. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis.

4

- Er wordt van alle medewerkers, leerlingen, (geregistreeerde) 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 imagooverlies. Stichting Gewoon Speciaal heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
- Informatiebeveiliging en privacy is bij Stichting Gewoon Speciaal een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij Stichting Gewoon Speciaal vanaf de start rekening gehouden met informatiebeveiliging en privacy.

3.2 Uitgangspunten privacy

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij Stichting Gewoon Speciaal zijn:

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

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van toestemming, zal Stichting Gewoon Speciaal aan de Betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden.

4 Wet- en regelgeving

Stichting Gewoon Speciaal voldoet aan alle van toepassing zijn de relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van het convenant 'Digitale onderwijsmiddelen en privacy 2.0' leidend bij het maken van afspraken met leveranciers.

5 Organisatie

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol.

Dit hoofdstuk beschrijft hoe IBP in Stichting Gewoon Speciaal is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

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

Een overzicht van de rollen en verantwoordelijkheden binnen Stichting Gewoon Speciaal is toegevoegd in bijlage 1.

5.1 Rollen (functies) rondom IBP

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Gewoon Speciaal een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

5.2 Richtinggevend

Eindverantwoordelijke

Het 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 Adviseur Privacy.

5.3 Sturend

Adviseur Privacy (Privacy Officer)

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

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

Functionaris voor Gegevensbescherming of Privacy Officer

De functionaris voor gegevensbescherming (FG), of Privacy Officer indien er geen FG is aangesteld, houdt binnen Stichting Gewoon Speciaal 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.

Domeinverantwoordelijke / proceseigenaar

Binnen het bestuur en de scholen zijn er verschillende domeinen/processen, zoals ICT, personeel (HRM, P&O), administratie, facilitaire- en financiële zaken, onderwijs et cetera. Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Deze proceseigenaar, in veel gevallen de schooldirecteur, is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Samen met het Bestuur stellen zij het beleid voor toegang vast en zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. Leidinggevend en hebben een voorbeeldrol ten opzichte van hun medewerkers.



5.4 Uitvoerend

Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in het privacy-handboek. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van beveiligingsincidenten, 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 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 Adviseur Privacy.

6 Controle en rapportage

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

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

Daarnaast kent Stichting Gewoon Speciaal een jaarlijkse pdca- cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst.

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

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

6.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij Stichting Gewoon Speciaal het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de Adviseur Privacy met het Bestuur als eindverantwoordelijke.

6.2 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.

6.3 Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij www.gewoonspeciaal.nl/privacy. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken.

6.4 Planning en controle

Dit IBP-beleid wordt minimaal elke 2 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 Stichting Gewoon Speciaal 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.

6.5 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, 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 tekortschieten, dan kan Stichting Gewoon Speciaal de betrokken verantwoordelijke medewerkers een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

6.6 Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt er voor 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.

Bijlage 1: Tabel IBP rollen en taken

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 Stichting Gewoon Speciaal.

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Voorbeelden: Raad van Toezicht/ Bestuur CvB Directeur	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Informatiebeveiligings- en privacy beleid Baseline/ basismaatregelen Reglement FG vaststellen Privacyreglement vaststellen
Sturend (tactisch)	Manager IBP, Verantwoordelijke IBP, Informatiemanager of Privacyofficer (de persoon die inhoudelijk verantwoordelijk is voor IBP)	<ul style="list-style-type: none"> Inhoudelijk verantwoordelijk voor IBP IBP-planning en controle Adviseert RvT/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 	<p>Processen, richtlijnen en procedures IBP, waaronder:</p> <ul style="list-style-type: none"> activiteitenkalender Protocol beveiligingsincidenten en datalekken Verwerkersovereenkomsten regelen Brief toestemming gebruik beeldmateriaal Opstellen informatie documentatie richting leerlingen, ouders/ verzorgers Security awareness activiteiten Sociale mediareglement Gedragscode van ICT en internetgebruik Gedragscode medewerkers en leerlingen
	Functionaris voor Gegevensbescherming en/of Privacyofficer	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Privacyreglement, procedure IBP-incidenta fhandeling Inrichten meldpunt datalekken
	Domeinverantwoordelijke/ Proces eigenaren Waaronder o.a.: ICT, HRM/ P&O, facilitair, onderwijs, financiën, inkoop en administratie	<ul style="list-style-type: none"> 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 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 	<ul style="list-style-type: none"> Inventariseren waar persoonsgegevens van de school terecht komen (leveranciers lijst); Input dataregister Classificatie- en risicoanalyse documenten. <p>Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder:</p> <ul style="list-style-type: none"> Toegangsmatrix diverse informatiesystemen en netwerk

		gebruikers regelmatig beoordelen en controleren.	
Uitvoerend (operationeel)	Privacyofficer	<ul style="list-style-type: none"> • Incidentaafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IEP-incidenten. 	
	Functioneelen/of applicatie beheerder	<ul style="list-style-type: none"> • Uitvoeren taken conform gegeven richtlijnen en procedures. 	
	Medewerker	<ul style="list-style-type: none"> • Verantwoordelijk omgaan met IEP bij hun dagelijkse werkzaamheden. 	
	Dagelijkse leiding/ leidinggevende/directie	<ul style="list-style-type: none"> • Communicatie naar alle betrokkenen: er voor zorgen dat medewerkers op de hoogte zijn van het IEP-beleid en de consequenties ervan. • Toezien op de naleving van het IEP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IEP-beleid. • Implementeren IEP-maatregelen. • periodiek het onderwerp informatiebewailiging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IEP-beleid aan bestuur. 	
		<p>Communiceren, informeren en toezien op naleving van o.a.:</p> <ul style="list-style-type: none"> • IEP in het algemeen • Regels passend ondernijfs • Hoe omgaan met leerlingdossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken 	

GMR Stichting Gewoon Speciaal advies en of instemming

Betreft:

- **Beleidsstuk: Informatie Beveiliging en Privacy Beleid (IBP)**
Versie: 23-5-2018

Korte toelichting document:

De nieuwe wetgeving AVG zal per 25 mei van kracht worden.

Voor SGS is door O21 een Informatiebeveiliging en privacybeleid opgesteld.

Door een wijziging in de wetgeving kan dit beleidsstuk nu pas worden aangeboden.

Dit beleidsstuk is de kapstok voor het handboek en het Privacy protocol en is opgesteld met in achtname van de wet en regelgeving AVG.

Met het handboek en het Privacy protocol behorend bij dit beleidsstuk is in de GMR -vergadering van 21 februari ingestemd.

Behandeld op GMR vergadering van: 23-5-2018

Gevraagde actie:

Omdat de AVG op 25 mei 2018 van kracht gaat en er de verplichting vanuit de wet is om het beleidsstuk vanaf die datum te plaatsen op de website, wordt het stuk als voorgenomen besluit aan u aangeboden, met het verzoek om het in uw vergadering van 27 juni te bespreken en hiermee in te stemmen.

Eventuele wijziging en/ of aanvullingen die uit uw vergadering komen, zullen in het stuk worden aangebracht. Waarna het aangepaste stuk wordt vastgesteld en op de website geplaatst

Opmerkingen (G)MR:

worden nog steeds RGO ontvangen
t.v.

Advies en/of instemming:

De (G)MR geeft stemt in met:

Beleidsstuk Informatie Beveiliging en Privacy Beleid (IBP)

Plaats: Houten

Datum: 27-6-2018


voorzitter GMR: Rob de Goede

Handtekening:

secretaris GMR:

Handtekening:


