



Informatiebeveiliging en Privacy

Vrijheidslaan 94, Postbus 42, 5306 ZG Brakel
0418 – 440234, info@scobommelerwaard.nl

Definitief, mei 2018

Inhoud

Informatiebeveiligings- en privacy beleid	Fout! Bladwijzer niet gedefinieerd.
1. Inleiding.....	Fout! Bladwijzer niet gedefinieerd.
1.1 Toelichting informatiebeveiliging	Fout! Bladwijzer niet gedefinieerd.
1.2 Toelichting privacy	Fout! Bladwijzer niet gedefinieerd.
1.3 Vervlechting informatiebeveiliging en privacy	Fout! Bladwijzer niet gedefinieerd.
2. Doel en reikwijdte	Fout! Bladwijzer niet gedefinieerd.
2.1 Doel.....	Fout! Bladwijzer niet gedefinieerd.
2.2 Reikwijdte	Fout! Bladwijzer niet gedefinieerd.
3. Uitgangspunten.....	Fout! Bladwijzer niet gedefinieerd.
3.1 Algemene beleidsuitgangspunten	Fout! Bladwijzer niet gedefinieerd.
4. Uitwerking van het beleid – Wat doen we?.....	Fout! Bladwijzer niet gedefinieerd.
4.1 Relevante wet- en regelgeving	Fout! Bladwijzer niet gedefinieerd.
4.2 Basisregels bij het omgaan met persoonsgegevens	7
4.3 Ondersteunende richtlijnen en procedures	8
4.4 Voorlichting en bewustzijn	8
4.5 Classificatie en risicoanalyse.....	8
4.6 Incidenten en datalekken	8
4.7 Planning en controle	9
4.8 Naleving en sancties	9
4.9 Logging en monitoring	9
5. Organisatie	10
5.1 Rollen (functies) rondom IBP	10
5.2 Richtinggevend	10
5.3 Sturend.....	10
5.4 Uitvoerend	11
6. Bijlagen.....	Fout! Bladwijzer niet gedefinieerd.
6.1 Bijlage 1: Ondersteunende richtlijnen en procedures.....	13
6.2 Bijlage 2: Tabel IBP rollen en taken	Fout! Bladwijzer niet gedefinieerd.

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 informatiebeveiliging. Beide begrippen staan naast elkaar en zijn van elkaar afhankelijk. Het onderwerp informatiebeveiliging en privacy wordt afgekort tot IBP. Dit beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen SCO Bommelerwaard.

2. Doel en reikwijdte

2.1 Doel

Dit beleid heeft als doel:

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

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

2.2 Reikwijdte

- Het informatiebeveiligings- en het privacybeleid binnen de SCOB geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing) alsmede voor alle organisatie onderdelen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen de SCOB waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing) evenals op andere betrokkenen waarvan de SCOB persoonsgegevens verwerkt.
- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van de SCOB. Het beleid heeft betrekking op gecontroleerde informatie, die door de organisatie zelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de organisatie kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites of sociale media.
- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van de SCOB evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
- Het IBP-beleid binnen de SCOB 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 SCOB hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van de SCOB 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. De SCOB voldoet aan alle relevante wet- en regelgeving.
3. Bij de SCOB 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 de SCOB 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. De SCOB 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. De SCOB legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. De SCOB voldoet hiermee aan de documentatieplicht.
6. Binnen de SCOB 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.
7. De stichting is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de stichting informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen moeten goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.
8. Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt bij de SCOB geclassificeerd. De classificatie is het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risico-analyse, waarbij gebruik gemaakt wordt van de classificatie. Er is een balans tussen de

risico's van hetgeen wij willen beschermen en de benodigde investeringen en maatregelen.

9. De SCOB 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' en het 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. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.
10. Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagooverlies. De SCOB heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
11. Informatiebeveiliging en privacy is bij de SCOB een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
12. Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij de SCOB vanaf de start rekening gehouden met informatiebeveiliging en privacy.
13. De SCOB 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.
14. De SCOB zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen.

4. Uitwerking van het beleid – Wat doen wij?

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

4.1 Relevante wet- en regelgeving

De SCOB voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet bescherming persoonsgegevens
- Algemene Verordening Gegevensbescherming (AVG)
- 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.

4.2 Basisregels bij het omgaan met persoonsgegevens

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

1. **Doelbepaling en doelbinding:** persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag:** verwerking van persoonsgegevens is gebaseerd op één 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 organisatie legt aan betrokkenen (leerlingen, hun ouders/verzorgers 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.

4.3 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.

4.4 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 de SCOB 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 manager IBP, de FG met de directeur-bestuurder als eindverantwoordelijke.

4.5 Classificatie en risico-analyse

Bij de SCOB heeft alle informatie waarde, daarom worden alle gegevens waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risico-analyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang zijn voor de informatievoorziening.

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.

4.6 Incidenten en datalekken

Alle medewerkers, die een beveiligingsincident of datalek vermoeden, dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister.

Alle incidenten worden per e-mail gemeld bij de functionaris gegevensbescherming. Dit kan via het e-mailadres fg@scobommelerwaard.nl

4.7 Planning en controle

Dit IBP-beleid 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 actuele geïnventariseerde risico's;
- de effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent de SCOB 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.

4.8 Naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat leidinggevend en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij de SCOB wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instellingsbrede gedragscode, met periodieke bewustwordingscampagnes, et cetera.

Voor de bevordering van de naleving van de wet bescherming persoonsgegevens vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door de directeur-bestuurder en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De FG werkt via een door de directeur-bestuurder vast te stellen reglement.

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

4.9 Logging en monitoring

Logging 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- en uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

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 de SCOB is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

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

5.1 Rollen (functies) rondom IBP

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

5.2 Richtinggevend

Eindverantwoordelijke

De directeur-bestuurder is eindverantwoordelijk voor het 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.

5.3 Sturend

Manager IBP

Manager IBP is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke 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 de SCOB
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen de SCOB coördineren

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) houdt binnen de SCOB 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 afhandelen van vertrouwelijke informatie beveiligingsincidenten. FG heeft regelmatig overleg met manager IBP. De FG is meestal ook de contactpersoon voor klachten en vragen van betrokkenen.

Portefeuillehouder ICT/ICT beheer

Adviseert samen met manager IBP/ informatiemanager de directeur-bestuurder en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen de SCOB.

Domeinverantwoordelijke/proceseigenaar

Binnen de organisatie 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 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 directeur-bestuurder stellen zij het beleid voor toegang 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.
- Samen met functioneel beheer en ICT-beheer beoordelen zij regelmatig de toegangsrechten van gebruikers.

Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

5.4 Uitvoerend

Functioneel beheerder

De functioneel beheerder wordt vanuit de domeinverantwoordelijke/proceseigenaar voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij/zij, zijn of haar taken uit.

Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging 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 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 manager IBP.

6. Vaststelling

Brakel, mei 2018



G.T. Tissink
directeur-bestuurder

Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidstukken, 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)
Communicatie rechten 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	
Gedragcode ict en internetgebruik	
Acceptable use policy	(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 gegevensbeschermingseffectbeoordeling	(DPIA)
Risicoanalyse	
Functionaris voor Gegevensbescherming	(communicatie hierover richting medewerkers)

Bijlage 2: Tabel IBP rollen en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid/taken	Wat Realiseren/vastleggen
Richtinggevend (strategisch)	Bestuur	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Informatiebeveiligings- en privacy beleid Baseline/basismaatregelen Reglement FG vaststellen Privacyreglement vaststellen
Sturend (tactisch)	Portefeuillehouder Beveiliging & Privacy	<ul style="list-style-type: none"> Inhoudelijk verantwoordelijk voor IBP IBP-planning en controle 	<ul style="list-style-type: none"> Activiteitenkalender
	Manager IBP	<ul style="list-style-type: none"> Adviseert bestuur/D-B/directie over IBP Voorbereiden 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 	<p>Processen, richtlijnen en procedures IBP, waaronder:</p> <ul style="list-style-type: none"> 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
	Functionaris voor Gegevensbescherming	<ul style="list-style-type: none"> Toezicht op naleving privacy wetgeving Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens Afwikkeling klachten en incidenten Voorlichting privacy en stimuleren bewustwording. 	<ul style="list-style-type: none"> Privacyreglement, procedure IBP-incident afhandeling Inrichten meldpunt datalekken
	Domeinverantwoordelijke/ Proceseigenaren waaronder: ict, personeel (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) Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door <i>bestuur/D-B/directie</i> <i>Samen met functioneel beheer en ICT beheer</i> er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. <i>Samen met functioneel beheer en ICT beheer</i> de toegangsrechten van 	<ul style="list-style-type: none"> Inventariseren waar persoonsgegevens van de school/stichting terecht komen (leveranciers lijst) 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

Niveau	Wie Rollen	Hoe Verantwoordelijkheid/taken	Wat Realiseren/vastleggen
		gebruikers regelmatig beoordelen en controleren.	
Uitvoerend (operationeel)	Functioneel beheerder Medewerker Dagelijkse leiding/ leidinggevende/directie	<ul style="list-style-type: none"> • Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • Communicatie naar alle betrokkenen; ervoor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur. 	<p>Communiceren, informeren en toezien op naleving van o.a.:</p> <ul style="list-style-type: none"> • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken