AVG

Informatiebeveiliging en privacy beleid (IBP)

optimus

Inhoud

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 onder andere 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.

2 Toelichting informatiebeveiliging en privacy

2.1 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.

2.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgensde 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 ter beschikkingstelling*, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.*

2.3 Vervlechting informatiebeveiliging en privacy

Informatiebeveiliging is een belangrijke voorwaarde 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: Informatie Beveiliging & Privacy beleid. Dit IPB-beleid vormt de basis voor informatiebeveiliging en privacy binnen Stichting Optimus Onderwijs en vormt de kapstok voor de onderliggende afspraken en procedures.

3 Doel en reikwijdte

3.1 Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan Stichting Optimus persoonsgegevens verwerkt, waaronder leerlingen, hun ouder(s)/verzorger(s)en medewerkers.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het 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 betrokkenen wordt gerespecteerd en Stichting Optimus Onderwijs hiermee voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

Het IBP-beleid binnen Stichting Optimus Onderwijs geldt voor alle medewerkers, leerlingen, ouder(s)/verzorger(s), (geregistreerde) bezoekers, vrijwilligers en externe relaties (inhuur/ outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk mee verkregen kan worden.

- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Stichting Optimus Onderwijs waaronder in ieder geval alle medewerkers, leerlingen, ouder(s)/verzorger(s), (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan Stichting Optimus Onderwijs persoonsgegevens verwerkt.

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Stichting Optimus Onderwijs. 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 (bijvoorbeeld 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 Stichting Optimus Onderwijs 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 Stichting Optimus Onderwijs raakvlakken met:

- *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvestingen ongevallen.
- *HR- en organisatiebeleid;* met als aandachtspunten in- en uitstroom vanmedewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties.
- *ICT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ICT en(digitale) leermiddelen
- *Medezeggenschap* van leerlingen, hun ouder(s)/verzorger(s) en medewerkers.

3.3 Beleid – Hoe doen we dat?

Stichting Optimus Onderwijs hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van Stichting Optimus Onderwijs neemt de verantwoordelijkheid om ervoor te zorgen dat het IBP-beleid goed geregeld wordt. Het bestuur is hierop aanspreekbaar en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.
2. Stichting Optimus Onderwijs voldoet aan alle relevante wet- en regelgeving.
3. Bij Stichting Optimus Onderwijs is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van Stichting Optimus Onderwijs 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. Stichting Optimus Onderwijs 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. Stichting Optimus Onderwijs legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Stichting Optimus Onderwijs voldoet hiermee aan de documentatieplicht.
6. Binnen Stichting Optimus Onderwijs 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. Stichting Optimus Onderwijs 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. Stichting Optimus Onderwijs classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussende risico’s die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.
9. Stichting Optimus Onderwijs sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht vande school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.
10. Stichting Optimus Onderwijs verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers, vrijwilligers 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. Stichting Optimus Onderwijs heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij Stichting Optimus Onderwijs een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
12. Stichting Optimus Onderwijs 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. Stichting Optimus Onderwijs 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. Stichting Optimus Onderwijs 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 we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten.

4.1 Relevante wet- en regelgeving

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

- Wet op het primair onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Algemene Verordening Gegevensbescherming
- Uitvoeringswet 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 verwerkingpersoonsgegevens (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 ookdat 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.

4.3 Ondersteunende richtlijnen en procedures

Stichting Optimus Onderwijs maakt gebruik van het ondersteunende programma: Easy Privacy. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de normen die gehanteerd worden bij Easy Privacy. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

4.4 Voorlichting en bewustzijn

De mens is een belangrijke factor bij het goed kunnen uitvoeren van het IPB-beleid. Stichting Optimus Onderwijs hecht veel waarde aan het bewust maken van de individuele medewerkers zorgvuldig om te gaan met persoonsgegevens. Onderdeel van dit beleid zijn bewustwordingsacties, workshops en schoolbezoeken door de privacy-coördinator. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de Privacy Officer , de FG, en de directeuren met het bestuur als eindverantwoordelijke. Iedere medewerker ontvangt (bij indiensttreding) een privacyreglement en ondertekent een geheimhoudingsverklaring.

4.5 Classificatie en risicoanalyse

Alle informatie heeft waarde. Het niveau van de te nemen beveiligingsmaatregelenis 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. Deze classificatie is een belangrijke taak van de privacy-coördinator. 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.

Data Protection Impact Assessment (DPIA)
Voor sommige risicovolle gegevensverwerkingen is een DPIA verplicht. Stichting Optimus Onderwijs heeft grotendeels dezelfde verwerkingen als andere PO-scholen en sluit zich aan bij de Handreiking DPIA van Kennisnet wat betreft verwerkingen waar het uitvoeren van een voorafgaande DPIA verplicht is, omdat deze een hoog risico met zich meebrengen voor de rechten en vrijheden van betrokkenen. Een nieuwe verwerking wordt altijd gemeld aan de Privacy Officer . Het DPIA beleid is vastgelegd in verschillende procedures en verwerkt in Easy 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. Alle (beveiligings)incidenten kunnen worden gemeld bij privacycoördinator@optimusonderwijs.nl.
De afhandeling van deze incidenten volgt volgens een vast stappenplan uitgevoerd door de privacy-coördinator. Indien er sprake is van een melding bij de Autoriteit Persoonsgegevens wordt dit alleen gedaan in samenspraak met het College van Bestuur.
Alle (beveiligings)incidenten worden vastgelegd in een incidentenregister in Easy Privacy.

4.7 Planning en controle

Dit IBP-beleid wordt jaarlijks 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

Het gevoerde IPB-beleid wordt maandelijks besproken met een vertegenwoordiger van de Lumengroup. Met de Lumengroup is een Advies en Toezicht op Maat (ATOM-aanpak) afgesloten. De aanstelling van de Functionaris Gegevensbescherming vormt een onderdeel van deze ATOM-aanpak. Per maand is recht op 6 uur advies.

Daarnaast kent Stichting Optimus Onderwijs een jaarlijkse planning en control cyclus voor IPB-beleid via Easy Privacy. Zie hiervoor bijlage 1. 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

Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingsacties, workshops en schoolbezoeken.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming(FG) een belangrijke rol. De FG is aangesteld door het bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. Stichting Optimus werkt hiervoor samen met de Lumengroup en de werkzaamheden van de FG zijn een onderdeel van de eerder genoemde ATOM aanpak (zie 4.7). De FG werkt via het door bestuur vastgesteld reglement. De FG heeft inzage in de voortgang van het IBP beleid via Easy Privacy.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan Stichting Optimus Onderwijs 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 I-coaches en de ICT-werkgroep/ leverancier zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens worden vastgelegd. Hieronder vallen onder andere het in- uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

5 Organisatie - Wie doet wat?

5.1 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 Stichting Optimus Onderwijs.

Niveau	Wie Rollen	Hoe Verantwoordelijkheid/ taken	Wat Realiseren/ vastleggen
Richtinggevend (strategisch)	Voorzitter College van Bestuur	• Eindverantwoordelijk • IBP-beleidsvorming, - vastlegging en het uitdragenervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basisvan rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacy beleid vaststellen • Baseline/ basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen • Reglementen vaststellen • Communicatie naar Directeurenoverleg/ RvT en GMR • ATOM aanpak • Rapportage Easy Privacy

Sturend tactis	Privacy-officer	• Inhoudelijk verantwoordelijkvoor IBP • IBP-planning en controle • Adviseert bestuur/CvB/directie overIBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse • Hanteren IBP-normen enwijze van toetsen • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op eenuniforme wijze • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoeringte ondersteunen • Incidentafhandeling (registreren en evalueren). • Voorlichting en bewustwording organiseren • schoolbezoeken	• Processen, richtlijnen en procedures IBP, waaronder: • activiteitenkalender • Verwerkersovereenkomsten regelen • Opstellen informatie documentatie richting leerlingen, ouders/ verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscodes actualiseren en implementeren • Bijhouden van Easy Privacy • Per kwartaal rapporteren via Easy Privacy aan CvB • Maandelijks overleg Lumengroup • Uitwerking ATOM aanpak
	Functionaris voor Gegevens-bescherming (FG)	• Toezicht op naleving privacywetgeving • Voorlichting privacy en stimuleren bewustwording • Richtlijnen, kaders vaststellenen aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten • Onderhoudt contacten met Autoriteit Persoonsgegevens • Rapporteert aan voorzitter van het College van Bestuur • Heeft overleg met Privacy Officer	• procedure IBP-incident afhandeling • toezicht houden • rapporteren • afstemmen beleid

	Domein-verantwoordelijke/ stafmedewerkers o.a.: ICT, HR/ P&O, facilitair, onderwijs, financiën, inkoop en administratie VIP Pool	• **Classificatie/ risicoanalyse** in samenwerking met Privacy Officer • Samen met I-coaches en Privacy Officer erop toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoorzij specifiek bevoegd zijn. • Samen met i-coaches en ICT-werkgroep (beheer) de toegangsrechten van gebruikers regelmatig beoordelen en controleren. • Zorg dragen voor uitreiken privacyreglement, geheimhoudingsverklaring en gedragscode aan nieuwe medewerkers	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input dataregister • Classificatie- en risicoanalyse documenten • Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen implementeren in de organisatie
Uitvoerend (operationeel)	Dagelijkse leiding/ directeur	• 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, richtlijnenen procedures door de medewerkers. • Voorbeeldfunctie met positieveen actieve houding t.a.v. IBP- beleid. • Implementeren IBP-maatregelen. • Periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc. • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur.	• Communiceren, informeren entoezien op naleving van o.a. • IBP in het algemeen implementeren • Het juist uitvoeren van het gebruik van leerlingdossiers. • Wie mogen welke leerlinggegevens zien. • Toepassen gedragscodes • Uitreiken privacyreglement en privacyverklaring • Omgaan met sociale media. • Mediawijs maken leerlingen en medewerkers • Digitaal geletterdheid bevorderen.
Uitvoerend (operationeel I)	i-coaches en werkgroep ICT	• Technisch aanspreekpunt voor IBP-incidenten. • Uitvoeren taken conform gegeven richtlijnen en procedures.	
Uitvoerend operationeel I	Medewerker	• Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.	

De verdere uitwerking van de rollen en taken staan beschreven in bijlage 2.

Bijlage 1: Easy Privacy

Via Easy Privacy wordt het AVG beleid gemonitord op 22 normen.
Beeldmateriaal
Beveiliging van persoonsgegevens
Bewaarplicht en vernietiging
Bewustzijn
Cameratoezicht
Cookies
Datalekken
DPIA
Functionaris gegevensbescherming
Gedragsregels
Gegevensuitwisseling met derden
Informatieplicht
Keten ID
Les en toetsen op afstand
Medische/bijzondere gegevens
Privacy by design en default
Privacybeleid
Rapport commissie van onderzoek (V)SO
Rechten van betrokkenen
Verantwoording
Verwerkersovereenkomsten

Per kwartaal wordt er een rapport gegenereerd door de Privacy Officer en besproken met de verantwoordelijke bestuurder.

1 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 Stichting Optimus Onderwijs voor elk niveau een aantal rollen toegekend aan medewerkers..

Eindverantwoordelijke

De voorzitter van het College van Bestuur is eindverantwoordelijk voor IBP en stelt het beleid ende 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 Privacy Officer .

Privacy Officer

Privacy Officer is een rol op sturend niveau. De PC geeft terugkoppeling en advies aan het CvB en stuurt de mensen aan op uitvoerend niveau. De privacy officer moet:

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

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) van de Lumengroup houdt binnen Stichting Optimus Onderwijs toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG vragen 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 de Privacy Officer .De FG is ook de contactpersoon voor klachten en vragen van betrokkenen. De taken en verantwoordelijkheden van de FG zijn vastgelegd in het FG-reglement.

Stafmedewerkers en domeinverantwoordelijken

Binnen Stichting Optimus Onderwijs zijn er verschillende domeinen zoals ICT, HR, Onderwijs, administratie, facilitaire- en financiële zaken, onderwijs. 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 domeinverantwoordelijke en/of stafmedewerkers zijn 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 Privacy Officer stellen zij het beleid voor toegang(autorisaties) vast.
- Samen met Privacy Officer en de ICT-beheer zien zij erop 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 de Privacy Officer en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

I-coaches en medewerkers met ICT in hun takenpakket
De Privacy Officer coördineert en controleert samen met de i-coaches softwarepakketten, toegangsrechten voorlichting en bewustwording.

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met infographics, 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 (G)MR)

Directeur
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering van de directeur. Iedere directeur heeft op uitvoerend niveau de taak om:
- ervoor 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 zelfeen 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 directeur kan in zijn taak ondersteund worden door de Privacy Officer .

IBP- team
De leden van hetIBP-team zijn benoemd door het CvB en handelen in diens opdracht.
Het IBP-team van Stichting Optimus Onderwijs heeft in samenwerking met de Privacy Officer de volgende opdracht:
- Het signaleren en registreren van datalekken die gemeld worden bij de AP. Het coördineren van de maatregelen en het toezien op de oplossing van problemen die tot het datalek hebben geleid en het bieden van ondersteuning daarbij;
- Bij een calamiteit kan het IBP-team terstond bij elkaar worden geroepen op initiatief van de Privacy Officer en het CvB. Het doel hiervan is om te zorgen voor adequate oplossingen en het waarborgen van de privacy. Onder calamiteiten worden verstaan:
    - Datalek;
    - Grote verstoringen van het netwerk (bijvoorbeeld DDoS aanval);
    - Natuurrampen (brand, overstroming, storm, etc.).

Het IBP-team bij Stichting Optimus Onderwijs behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor deoplossing van een incident.