

Informatie beveiliging en privacy (IBP) beleid

Bron

Sjabloon Kennisnet

Bewerkt door:

Stichting kom Leren

Stichting MosaLira

Versie	Status	Datum	Auteur	Omschrijving
1.0	Concept	13-11-2023	Rutger Bronsveld Jeroen van Can	Eerste opzet voor een beleid dat vanuit het Team ICT dat voor beide stichtingen opstelt staat is geschreven.
1.1	Definitief	12-3-2024	Rutger Bronsveld Jeroen van Can	Tekstuele aanpassingen doorgevoerd naar aanleiding van bespreking van het beleidsdocument.

Vastgesteld door Stichting kom Leren:

Versie	Datum	Naam	Functie
1.0	15-1-2024	Inge Ambaum - Jordens	College van bestuur
1.0	13-3-2024	Bert-Jan van Overeem	Voorzitter GMR, namens GMR

Vastgesteld door Stichting MosaLira:

Versie	Datum	Naam	Functie
1.0	12-3-2024	Jean-Pierre Giesen	College van bestuur
1.0	26-4-2024	Maurice Lambriex	Voorzitter GMR, namens GMR

STRATEGIE SCHOOLBESTUREN.....	4
VISIE.....	4
HET BELANG VAN INFORMATIEBEVEILIGING EN PRIVACY.....	4
TOELICHTING INFORMATIEBEVEILIGING EN PRIVACY	4
TOELICHTING INFORMATIEBEVEILIGING	4
TOELICHTING PRIVACY.....	4
VERVLECHTING INFORMATIEBEVEILIGING EN PRIVACY.....	5
DOEL EN REIKWIJDTE	5
DOEL.....	5
REIKWIJDTE	5
BELEID – HOE DOEN WE DAT?.....	6
UITWERKING VAN HET BELEID – WAT DOEN WE?	7
RELEVANTE WET- EN REGELGEVING	7
BASISREGELS BIJ HET OMGAAN MET PERSOONSGEGEVENS.....	7
ONDERSTEUNENDE RICHTLIJNEN EN PROCEDURES.....	8
VOORLICHTING EN BEWUSTZIJN.....	8
CLASSIFICATIE EN RISICOANALYSE	8
INCIDENTEN EN DATALEKKEN	8
PLANNING EN CONTROLE	8
NALEVING EN SANCTIES.....	9
LOGGING EN MONITORING.....	9
ORGANISATIE - WIE DOET WAT?	10
ROLLEN EN VERANTWOORDELIJKHEDEN	10
BIJLAGE 1: ONDERSTEUNENDE RICHTLIJNEN EN PROCEDURES.....	12
BIJLAGE 2: ORGANISATIE; WIE DOET WAT	13
RICHTINGGEVEND	13
STUREND.....	13
UITVOEREND.....	14

Strategie Schoolbesturen

Per januari 2023 is er een intensieve samenwerking tussen Stichting Kom Leren en Stichting MosaLira op het gebied van ICT & IBP. Beide stichtingen kiezen ervoor om Informatiebeveiliging en Privacy (IBP) goed te organiseren en duurzaam te borgen. Dit ligt vast in hun strategische koersplannen 2024-2028.¹ De gegevens van iedereen die betrokken is bij de stichtingen moeten passend beschermd worden tegen bedreigingen van buiten. Door de krachten te bundelen op deze aandachtsgebieden kunnen de stichtingen een weerbaarheid bieden die vanuit de praktijk wordt gevraagd.

Visie

Beide stichtingen willen een veilige en professionele leer- en werkomgeving aanbieden en daarbij is het noodzakelijk dat de door Stichting Kom Leren en MosaLira verzamelde, verwerkte en gepubliceerde informatie te allen tijde beschikbaar, correct en beschermd is. Dit vraagt om een strategisch samenhangende aanpak van Informatiebeveiliging en Privacy, die aantoonbaar aan de eisen voldoet, om blijvend een veilige en toekomstbestendige leer- en werkomgeving beschikbaar te stellen. Ten aanzien van deze aanpak volgen beide stichtingen de richtlijnen van het Normenkader IBP.

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 & gecombineerd 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.

Toelichting informatiebeveiliging en privacy

Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden.

Informatiebeveiliging richt zich op de volgende aspecten:

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

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

¹ - We zetten in op cybeveiligheid en borgen daarmee de continuïteit van het primaire proces. Hierbij monitoren en volgen we wet- en regelgeving. De veiligheid van de gegevens van onze collega's en leerlingen is prioriteit.

- We scholen, informeren en maken onze collega's bewust van hun rol op het gebied van cybersecurity en privacy.

persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:

Het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.

Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijke voorwaarde is voor privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Informatiebeveiliging en privacy staan naast elkaar en zijn van elkaar afhankelijk, en worden daarom samengevoegd tot één proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis om informatiebeveiliging en privacy binnen de onderwijsstichtingen kom Leren en MosaLira 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 De onderwijsstichtingen kom Leren & MosaLira 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 De onderwijsstichtingen kom Leren en MosaLira voldoen aan relevante wet- en regelgeving.


Reikwijdte

- Het IBP-beleid binnen De onderwijsstichtingen kom Leren en MosaLira geldt voor alle medewerkers, leerlingen, ouders/verzorgers, vrijwilligers, stagiairs, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices van waar geautomatiseerde toegang tot het schoolnetwerk verkregen kan worden.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen De onderwijsstichtingen kom Leren en MosaLira waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, vrijwilligers, stagiairs, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan De onderwijsstichtingen kom Leren en MosaLira persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van De onderwijsstichtingen kom Leren en MosaLira. 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. (Bijv. 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 De onderwijsstichtingen kom Leren en MosaLira 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 De onderwijsstichtingen kom Leren en MosaLira raakvlakken met:
 - *Algemeen veiligheids- en toegangsbeveiligingsbeleid*; met als aandachtspunten bedrijfs-hulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongeval-len.
 - *Personeels- en organisatiebeleid*; met als aandachtspunten in- en uitstroom van medewer-kers, functiewisselingen, functiescheiding en vertrouwensfuncties.
 - *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leer-middelen.
 - *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers.

Beleid – Hoe doen we dat?

De onderwijsstichtingen kom Leren & MosaLira hanteren de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken: 

1. De besturen van De onderwijsstichtingen kom Leren en MosaLira nemen de verantwoordelijk-heid om ervoor te zorgen dat informatiebeveiliging en privacy borging geregeld wordt. Het be-stuur is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur van de stichting de verwerkingsverantwoordelijke.
2. De onderwijsstichtingen kom Leren en MosaLira voldoen aan alle relevante wet- en regelge-ving.
3. Bij de onderwijsstichtingen kom Leren en MosaLira 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 onderwijsstichtingen kom Leren en MosaLira 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. De onderwijsstichtingen kom Leren en MosaLira zal alle betrokkenen helder en actief informe-ren over de verwerkingen van de hun persoonsgegevens, die zowel direct als indirect zijn ver-kregen. Ook worden alle betrokkenen gewezen op hun rechten met betrekking tot informatie, inzage, verbetering, het wissen van gegevens, beperking van verwerking, verzet, dataportabili-teit en profilering.
5. De onderwijsstichtingen kom Leren en MosaLira leggen alle verwerkingen van persoonsgege-vens vast in een verwerkingsregister en zullen deze up-to-date houden. De onderwijsstichtingen kom Leren en MosaLira voldoen hiermee aan de documentatieplicht.
6. Binnen De onderwijsstichtingen kom Leren en MosaLira is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdra-gen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van papieren documenten.
7. De onderwijsstichtingen kom Leren en MosaLira zijn als rechtspersoon eigenaar van de infor-matie die onder hun verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leer-lingen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.
8. De onderwijsstichtingen kom Leren en MosaLira classificeren informatie en informatiesys-temen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.
9. De onderwijsstichtingen kom Leren en MosaLira sluiten met alle leveranciers van digitale on-derwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.
10. De onderwijsstichtingen kom Leren en MosaLira verwachten 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. De onderwijsstichtingen kom Leren en MosaLira hebben hiervoor gedragscodes geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij De onderwijsstichtingen kom Leren en MosaLira een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
12. De onderwijsstichtingen kom Leren en MosaLira kijken 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. De onderwijsstichtingen kom Leren en MosaLira nemen passende technische & organisatorische (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 onderwijsstichtingen kom Leren en MosaLira zullen alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel 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
- AVG
- Wet bescherming persoonsgegevens (Wbp; tot 25 mei 2018)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 (2015) is leidend voor de te nemen beveiligingsmaatregelen. Voor digitale uitwisseling van persoonsgegevens zal ook de norm NTA 7516 worden geraadpleegd/gevolgd.

De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken.

Basisregels bij het omgaan met persoonsgegevens

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

1. **Doelbepaling en doelbinding:** persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag:** verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.
3. **Dataminimalisatie:** bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding staan tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (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 verwerkingsregister.

Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. Daarom wordt het bewustzijn van de individuele medewerkers periodiek 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 (externe) Functionaris Gegevensbescherming (FG), en de Privacy- en Security Officer.

Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen beveiligingsmaatregelen is afhankelijk van de classificatie. De classificatie van informatie is afhankelijk van de gegevens in het informatiesysteem en wordt bepaald op basis van risicoanalyses. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de betrouwbaarheidsaspecten die van belang zijn.

Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe (ict)projecten wordt rekening gehouden met informatiebeveiliging en privacy.

Incidenten en datalekken

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

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

Periodiek wordt ook middels de bestuursrapportage (aan GMR en RvT) gerapporteerd over o.a. incidenten.

Planning en controle

Dit IBP-beleid wordt minimaal elke twee jaar, na instemming GMR, 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 kennen de onderwijsstichtingen kom Leren en MosaLira 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.

Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een organisatiebrede 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 kunnen de onderwijsstichtingen kom Leren en MosaLira de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

Logging en monitoring

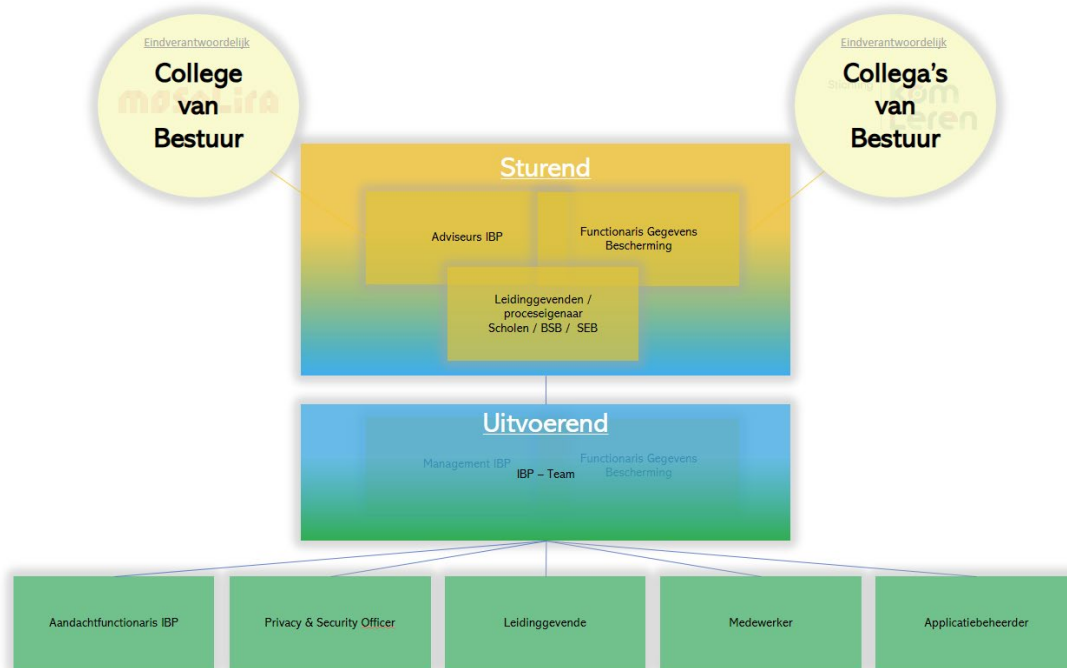
Logging en monitoring door de ICT-afdeling zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in-uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

Organisatie - Wie doet wat?

Rollen en verantwoordelijkheden

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij de onderwijsstichtingen kom Leren en MosaLira.

Hieronder een grafische weergave van de rollen. De verdere uitwerking van de rollen en taken staan beschreven in bijlage 2.



Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	CvB	<ul style="list-style-type: none"> Eindverantwoordelijk IBP-beleidsvorming, -vastlegging en het uitdragen ervan 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)	Adviseurs IBP Security officer & privacy officer	<ul style="list-style-type: none"> Inhoudelijk verantwoordelijk voor IBP IBP-planning en controle Adviseert CvB 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 Classificatie / risicoanalyse in samenwerking met betrokken domeinen 	Processen, richtlijnen en procedures IBP, waaronder: <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 media reglement Gedragscode ict en internetgebruik Gedragscode medewerkers en leerlingen

	Functionaris voor Gegevensbescherming	<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-incident afhandeling • Inrichten meldpunt datalekken
	Directeuren	<ul style="list-style-type: none"> • Toegangsbeleid zowel fysiek als digitaal vaststellen • Samen met functioneel beheer en ICT beheer er 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 gebruikers regelmatig beoordelen en controleren. 	<ul style="list-style-type: none"> • Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst); input verwerkingsregister • 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
Uitvoerend (operationeel)	Security officer Privacy officer	<ul style="list-style-type: none"> • Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • Communicatie naar alle betrokkenen; er voor 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. 	<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
	Functioneel en/of applicatie beheerder	<ul style="list-style-type: none"> • 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.; 	
	Medewerker	<ul style="list-style-type: none"> • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur. 	
	Dagelijkse leiding / leidinggevende / directie		
	Aandachtsfunctionaris IBP		

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. In het uitvoeringsdocument is een planning opgenomen aangaande actualisatie van de stukken.

Documenten:

Procedure toestemming gebruik beeldmateriaal
Procedure voor verwijderen van gegevens
Communicatie rechten betrokkenen
Procesbeschrijving rechten betrokkenen
Privacyreglement
Autorisatiematrix
Afspraken gebruik sociale media
Procedure rondom training medewerkers
Cameratoezicht
Wachtwoordbeleid
Responsible disclosure
Gedragcode ict en internetgebruik
Acceptable use policy
Procedure rondom uitwisselen gegevens

Aandachtspunten:

(toestemmingsbrief)
(bewaartermijnen)
(communicatie richting betrokkenen)
(proces rondom aanvragen van betrokkenen)

(wie mogen gegevens inzien, bewerken enz.)

(bewustzijn creëren)

(verantwoord gebruik bedrijfsmiddelen)
(passend onderwijs, leerplicht enz)

Verplicht vanuit de AVG:

Procesbeschrijving melden datalekken
Registratie beveiligingsincidenten
Verwerkingsregister
Verwerkersovereenkomsten
Gegevensbeschermingseffectbeoordeling
Risicoanalyse
Functionaris voor Gegevensbescherming

(privacy bijlage beschikbaar stellen)
(DPIA)

(communicatie hierover richting medewerkers)

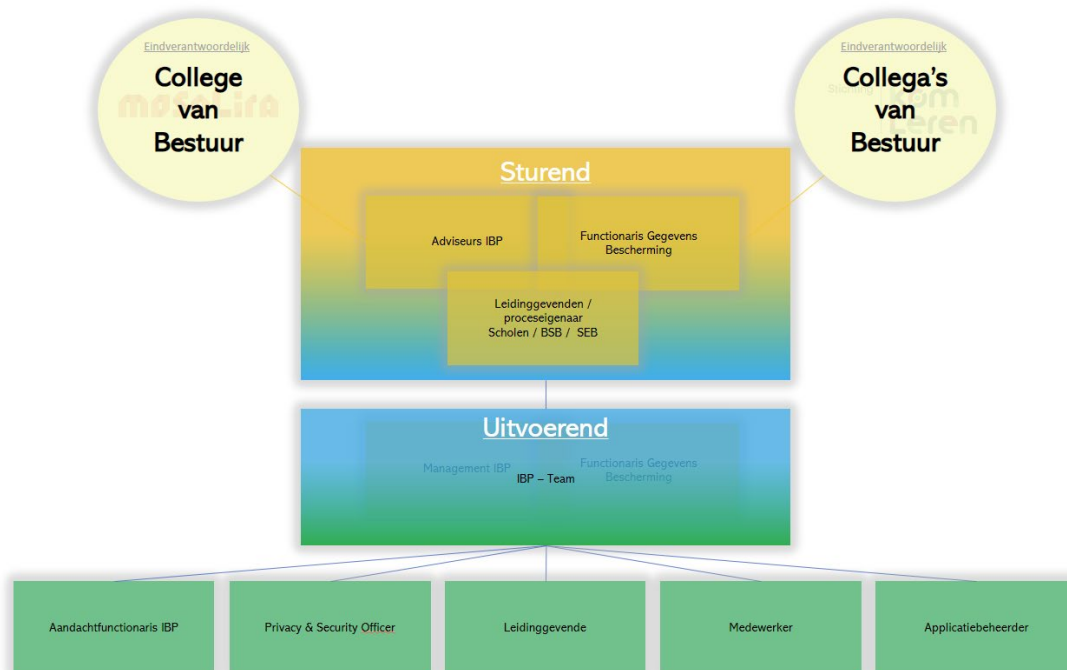
Bijlage 2: Organisatie; wie doet wat

Deze bijlage beschrijft hoe IBP op drie niveaus wordt georganiseerd.

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

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij de onderwijsstichtingen kom Leren en MosaLira voor elk niveau een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

Beschreven wordt welke rollen, welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.



Richtinggevend

College van bestuur

- Het College van Bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.
- De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd.
- De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de adviseurs IBP.

Sturend

Adviseurs IBP

Adviseurs IBP (Security officer en privacy officer) is een rol op sturend niveau. Geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau. De adviseur IBP zal:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen de onderwijsstichtingen kom Leren & MosaLira
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen de onderwijsstichtingen kom Leren & MosaLira coördineren

De adviseurs IBP definiëren het informatiebeveiligingsbeleid, gebaseerd op een risicomanagement-benadering en rekening houdend met het informatiebeveiligingsdreigingsbeeld, trends en organisatiebehoefte. Richt de informatiebeveiligingsorganisatie in, bepaalt de daarvoor benodigde middelen en de inzet hiervan op concrete beveiligingsmaatregelen. Initieert en coördineert de implementatie van informatiebeveiliging voor de gehele organisatie en houdt daar toezicht op. Zorgt voor een geschikt niveau van informatiebeveiliging en informatiebeveiligingsgedrag in de organisatie, gebaseerd op de behoeften en de risicobereidheid van de organisatie. Wordt door interne en externe stakeholders beschouwd als de deskundige op het gebied van informatiebeveiliging.

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) houdt binnen de onderwijsstichtingen kom Leren & MosaLira 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.

Schoolverantwoordelijke en/of Proceseigenaar

Primair is voor de aangelegenheden op school de directeur verantwoordelijk, dit al dan niet ondersteund door een eigen collega op school (aandachtfunctionaris IBP). Op de scholen bepalen zij op welke wijze IBP conform de geldende regels wordt vormgegeven.

Binnen de besturen zijn er verschillende domeinen/ processen, zoals ICT, Personeel, Administratie, Facilitaire- en Financiële zaken, Onderwijs et cetera. Hiervoor zijn proces-eigenaren aanwezig.

Deze proceseigenaar is 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 proces-eigenaren de volgende specifieke taken:

- Samen met de Directeuren stellen zij het beleid voor toegang (autorisaties) vast.
- Samen met functioneel beheer en ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
- Samen met functioneel beheer en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

Uitvoerend

IBP-team

Een IBP-team, bestaande uit het Management IBP & de FG wordt organisatie breed zowel **preventief** als **curatief** benoemd voor informatiebeveiliging en privacy incidenten. De leden van het IBP-team zijn benoemd door de eindverantwoordelijke en handelen in diens opdracht.

Het IBP-team van kom Leren & MosaLira heeft de volgende opdracht:

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

Bij een calamiteit kan het IBP-team terstond bij elkaar worden geroepen op initiatief van de adviseurs IBP, de FG of leidinggevende/proceseigenaar, in opdracht van De onderwijsstichtingen kom Leren & MosaLira. Het doel hiervan is om de continuïteit van de informatievoorziening en de privacy te waarborgen. Onder calamiteiten worden verstaan:

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

Het IBP-team bij De onderwijsstichtingen kom Leren & MosaLira behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident.

De werkzaamheden van het IBP-team bij De onderwijsstichtingen kom Leren & MosaLira is gedocumenteerd en door de eindverantwoordelijke bekrachtigd.

Security Officer (SO)

De Security Officer vormt een technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers.

Privacy Officer (PO)

De Privacy Officer vormt een inhoudelijk aanspreekpunt als het gaat over privacy voor het management en de medewerkers.

Functioneel beheerder of Applicatiebeheerder

Ieder softwarepakket of (web-)applicatie heeft een beheerder. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden. De functioneel beheerder wordt vanuit de domeinverantwoordelijke / proceseigenaar voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

Aandachtsfunctionaris IBP (rol)

Deze rol kan aan een medewerker in een school zijn toegewezen. Zo niet dan is de leidinggevende op de school primair de aangewezen persoon voor de taken bij deze rol.

De rol van aandacht-functionaris wordt ingevuld op onderstaande wijze:

- Samen met de leidinggevende op school het onderwerp periodiek bespreekbaar maken.
- Signalerende taak als 'oren & ogen' op het vlak van IBP voor het Management IBP. Risico's signaleren en bespreekbaar maken.
- Ondersteuning op de scholen bij het verhogen, en op peil houden, van het bewustzijn van risico's op het gebied van IBP.

Medewerker, vrijwilligers & Stagiaires

Alle medewerkers, vrijwilliger & Stagiaires hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. richtlijnen en codes voor het personeel. 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 security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR).

Leidinggevende

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft op uitvoerend niveau de taak om:

- Er voor te zorgen dat zijn medewerkers op de hoogte zijn van het IBP-beleid.
- Toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft.
- Periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.
- Als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

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