



stichting primair onderwijs

Condor

INFORMATIEBEVEILIGING EN
PRIVACY
Beleidsplan

Bron

Kennisnet

Bewerkt door:

Harold Swinkels en Willian Verwijst

Vastgesteld door SPO Condor:

Versie	Datum	Naam	Functie
1.0	09/11/2018	Marthijn Manders	Bestuurder

Aangepast door privacy- coördinatoren

Versie	Datum	Omschrijving
1.1	20/11/2020	<ul style="list-style-type: none">• Lay-out en spelling/grammatica• Expliciet benoemen van de 4 grondslagen:<ul style="list-style-type: none">- Uitvoeren of voorbereiden van de overeenkomst.- Wettelijke grondslag- Gerechvaardigd belang- Toestemming• Uitwerking van de grondslag verwerking persoonsgegevens van werknemers• Uitwerking van bewaartermijnen

Inhoud

1	Het belang van informatiebeveiliging en privacy	3
2	Toelichting informatiebeveiliging en privacy	3
2.1	Toelichting informatiebeveiliging	3
2.2	Toelichting privacy	3
2.3	Vervlechting informatiebeveiliging en privacy	3
3	Doel en reikwijdte	4
3.1	Doel	4
3.2	Reikwijdte	4
4	Beleid – Hoe doen we dat?	4
5	Uitwerking van het beleid – Wat doen we?	7
5.1	Relevante wet- en regelgeving	7
5.2	Basisregels bij het omgaan met persoonsgegevens	7
5.3	Ondersteunende richtlijnen en procedures	8
5.4	Voorlichting en bewustzijn	8
5.5	Classificatie en risicoanalyse	8
5.6	Incidenten en datalekken	8
5.7	Planning en controle	9
5.8	Naleving en sancties	9
5.9	Logging en monitoring	9
6	Organisatie - Wie doet wat?	10
6.1	Rollen en verantwoordelijkheden	10
7	Bijlage 1: Ondersteunende richtlijnen en procedures	12
8	Bijlage 2: Organisatie; wie doet wat	13
8.1	Richtinggevend	13
8.2	Sturend	13
8.3	Uitvoerend	14

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 o.a. 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 imagooverlies.

2.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:

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

2.3 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 op informatiebeveiliging en privacy binnen SPO Condor te regelen 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 SPO Condor 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 SPO Condor voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het IBP-beleid binnen SPO Condor geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers, vrijwilligers en externe relaties (inhuur / outsourcing). Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- Het IBP-beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen SPO Condor waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan SPO Condor persoonsgegevens verwerkt.
- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van SPO Condor Hieronder valt tevens de gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd en de niet-gecontroleerde informatie waarop de school kan worden aangesproken. (b.v. uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media.)
- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van SPO Condor 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 SPO Condor raakvlakken met:
 - *Algemeen veiligheids- en toegangsbeveiligingsbeleid*; met als aandachtspunten bedrijfs-hulpverlening, 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

4 Beleid – Hoe doen we dat?

SPO Condor hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het schoolbestuur van SPO Condor 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. SPO Condor voldoet aan alle relevante wet- en regelgeving.
3. Bij SPO Condor is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de volgende grondslagen:
 - Uitvoeren of voorbereiden van de overeenkomst.
 - Wettelijke grondslag
 - Gerechtigd belang
 - Toestemming
4. Grondslag verwerking persoonsgegevens
Verwerking van persoonsgegevens gebeurt alleen als aan een van de onderstaande voorwaarden is voldaan:
 - a) De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan het SPO Condor is opgedragen.
 - b) De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op SPO Condor rust.
 - c) De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (bijvoorbeeld de arbeidsovereenkomst) of om op verzoek van de betrokkene vóór de afsluiting van een overeenkomst maatregelen te nemen.
 - d) De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van SPO Condor of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen. In het kader van deze grondslag zal dus een belangenafweging moeten plaatsvinden.
 - e) De verwerking is noodzakelijk om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen (levensbelang).
 - f) De betrokkene heeft ondubbelzinnige toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden. D.w.z. toestemming is expliciet, voordat de verwerking plaatsvindt, gevraagd en gecommuniceerd.
5. Een goede balans tussen het belang van SPO Condor 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.
6. SPO Condor 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.
7. SPO Condor legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. SPO Condor voldoet hiermee aan de documentatieplicht.
8. Binnen SPO Condor is het veilig en betrouwbaar omgaan met informatie de verantwoordelijk-

heid 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.

9. SPO Condor 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.
10. SPO Condor classificeert informatie en informatiesystemen. 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.
11. SPO Condor sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.
12. SPO Condor 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 imagooverlies. SPO Condor heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
13. Informatiebeveiliging en privacy is bij SPO Condor een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
14. SPO Condor 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.
15. SPO Condor 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.

SPO Condor zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen

5 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.

5.1 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
- 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.

5.2 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 manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag:** verwerking van persoonsgegevens is gebaseerd op een van de zes wettelijke grondslagen.
3. **Dataminimalisatie:** bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt (subsidiar). Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk. Hierbij worden de van toepassing zijnde (wettelijke) bewaar- en vernietigingstermijnen in acht genomen.
In bijlage B is een overzicht opgenomen met de diverse categorieën van persoonsgegevens en de daarbij behorende bewaartermijnen en wettelijke grondslag.
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.

5.3 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.

5.4 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 voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de privacy coördinatoren, de FG, en de directeuren met het bestuur als eindverantwoordelijke. Iedere medewerker ontvangt (bij indiensttreding) een privacyreglement en ondertekent een geheimhoudingsverklaring.

5.5 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.

Data Protection Impact Assessment (DPIA)

Voor sommige risicovolle gegevensverwerkingen is een DPIA verplicht. SPO Condor 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 privacycoördinator.

5.6 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 (beveiligings)incidenten kunnen worden gemeld op de Sharepoint-omgeving van SPO Condor.

(Algemeen ->AVG)

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

5.7 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

Daarnaast kent SPO Condor 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.

5.8 Naleving en sancties

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

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

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan SPO Condor de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.9 Logging en monitoring

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

6 Organisatie - Wie doet wat?

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

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	Bestuur: Marthijn Manders	<ul style="list-style-type: none"> Eindverantwoordelijk IBP-beleidsvorming, -vastlegging en het uitdragen ervan Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens Evalueren toepassing en werking IBP-beleid op basis van rapportages Organisatie IBP inrichten 	<ul style="list-style-type: none"> Informatiebeveiligings- en privacy beleid Baseline / basismaatregelen Reglement FG vaststellen Privacyreglement vaststellen
Sturend (tactisch)	Privacy coördinatoren: Harold Swinkels Willian Verwijst	<ul style="list-style-type: none"> Inhoudelijk verantwoordelijk voor IBP IBP-planning en controle Adviseert bestuur en directie over IBP Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse <ul style="list-style-type: none"> Hanteren IBP normen en wijze van toetsen Evalueren IBP-beleid en maatregelen Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen 	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: Stijn Sarneel en/of Privacy-coördinatoren: Harold Swinkels Willian Verwijst	<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

	<p>Domeinverantwoordelijke / Proceseigenaren Waaronder o.a.:</p> <p>Heutink-ICT Directies van scholen Stafmedewerker Financiën Administratie Projectgroep ICT</p>	<ul style="list-style-type: none"> • Classificatie / risicoanalyse in samenwerking met de Privacy-coördinatoren • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door bestuur • 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 dataregister • Classificatie- en risicoanalyse documenten. <p>Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder:</p> <ul style="list-style-type: none"> • Toegangsmatrix diverse informatiesystemen en netwerk
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Uitvoerend (operationeel)</p>	<p>Privacycoördinatoren</p> <p>Bovenschools ICT-coördinator ICT-coördinatoren</p> <p>Medewerker</p> <p>Directies Privacy-coördinatoren</p>	<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. • 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

7 Bijlage 1: Ondersteunende richtlijnen en procedures

Deze bijlage bevat een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen.

Documenten:	Aandachtspunten:
Toestemming gebruik beeldmateriaal	(toestemmingsbrief)
Procedure voor verwijderen van gegevens	(bewaartermijnen)
Privacy verklaringen	(communicatie richting betrokkenen)
Procedure rechten van betrokkenen	(proces rondom aanvragen van betrokkenen)
Privacyreglement	
Autorisatiematrix enz.)	(wie mogen gegevens inzien, bewerken)
Sociale media protocol	
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.)
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)
Reglement Functionaris Gegevensbescherming	
Overzicht bewaartermijnen	

8 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 SPO Condor 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.

8.1 Richtinggevend

Eindverantwoordelijke

Het bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.

De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd.

De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de privacy-coördinator.

8.2 Sturend

Privacy-coördinator

Privacy-coördinator is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (het bestuur) en stuurt de mensen aan op uitvoerend niveau. De privacy-coördinator moet:

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

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) houdt binnen SPO Condor 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 de privacy-coördinator. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

Domeinverantwoordelijke / proceseigenaar

Binnen SPO Condor zijn er verschillende domeinen/processen, zoals ICT, personeel, 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 privacy-coördinator 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.

8.3 Uitvoerend

Bovenschools ICT-coördinator

De Bovenschools ICT-coördinator vormt een technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers.

Functioneel beheerder: ICT-coördinator van de school

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 projectgroep ICT voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit.

Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in het schoolveiligheidsplan. 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 privacy-coördinator.

Leidinggevendens hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

9 Bijlage 3: Bewaartermijnen

Hieronder een overzicht opgenomen met diverse categorieën van persoonsgegevens en de daarbij behorende bewaartermijnen en wettelijke grondslag.

Welke gegevens	Wettelijke basis	Uitleg	
1. Specifieke gevallen	specifieke wet	Specifieke bewaar- c.q. vernietigingstermijn terug te vinden in wet en regelgeving. Deze specifieke termijn wordt nagekomen. In de tabel in deze handreiking is een opsomming van specifieke bewaartermijnen te vinden (zie bijlage: lijst met termijnen in onderwijswetten).	
2. Europese subsidie (stimuleringsregeling)	ESF	Tot 10 jaar na vertrek van de betreffende leerlingen/medewerkers moet informatie bewaard worden.	
3. Financiële en fiscale en bekostigingsbescheiden	Artikel 172 lid 3 Wet PO Artikel 130a lid 3 Wet VO	7 jaar	
4. Alle gegevens in de leerling administratie PO / VO	Artikel 9 lid 1 (juncto artikel 6 lid 1) bekostigingsbesluit WPO Artikel 6 bekostigingsbesluit VO	Tot 5 jaar na uitschrijving betreffende leerling blijft diens informatie bewaard in de leerling administratie	
5. Persoonsgegevens betreffende de gezondheid van leerlingen	Artikel 18a lid 6 (juncto lid 13) Wet PO 17a lid 14 Wet VO	3 jaar na afloop van: (a.) de beoordeling of een leerling is aangewezen op het leerwegondersteunend onderwijs of van het toelaatbaar verklaren van leerlingen tot het praktijkonderwijs of het voortgezet speciaal onderwijs (b.) de advisering over de ondersteuningsbehoefte van de leerling aan het bevoegd gezag van de school, (c.) de toewijzing van ondersteuningsmiddelen of voorzieningen aan de school.	
6. Digitaal leermateriaal	Persoonsgegevens: niet langer bewaren dan noodzakelijk	Po	Gegevens huidige schooljaar, plus gegevens voorgaande schooljaar bewaren
		Onderbouw vo	
		Bovenbouw vo	Gegevens huidige schooljaar, plus de twee voorgaande schooljaren bewaren
7. Alle andere gevallen	Gegevens tot personen herleidbaar	Vernietigen 2 jaar na uitschrijven of beëindigen relatie	

	Toestemming om na uitschrijven gegevens te bewaren met specifiek doel	Bewaren toegestaan op basis van toestemming (bijv. alumni)
	Niet tot persoon herleidbaar	Vrij te kiezen