

Informatiebeveiligings- en privacy beleid

IBP

Stichting de Korre



Aangeboden aan DB	Besproken in DB	Aangeboden aan GMR	Besproken in GMR
	1-4-2019		15-4-2019
	Goedgekeurd d.d. 1-4-2019		Goedgekeurd d.d. 17 juni 2019

INHOUDSOPGAVE

INHOUDSOPGAVE	1
1. Inleiding	2
Toelichting informatiebeveiliging	2
Toelichting privacy	2
Vervlechting informatiebeveiliging en privacy	2
2. Doel en reikwijdte	3
Doel	3
Reikwijdte	3
3. Uitgangspunten	4
Algemene beleidsuitgangspunten	4
Uitgangspunten privacy	4
4. Wet- en regelgeving	5
5. Organisatie	5
Richtinggevend	5
Sturend	5
Uitvoerend	6
6. Controle en rapportage	7
Voorlichting en bewustzijn	7
Classificatie en risicoanalyse	7
Incidenten en datalekken	7
Controle, naleving en sancties	7
BIJLAGE 1: TABEL IBP ROLLEN EN TAKEN	8
BIJLAGE 2: GLOBALE TIJDSINVESTERING IBP	10
BIJLAGE 3: CHECKLIST AANPAK IBP	11

1. INLEIDING

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

Toelichting informatiebeveiliging

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

Deze aspecten zijn:

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

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

Toelichting privacy

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

Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijk onderdeel is van privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar, en zijn van elkaar afhankelijk. Het onderwerp informatiebeveiliging en privacy wordt afgekort tot IBP. Dit beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen De Korre.

2. DOEL EN REIKWIJDTE

Doel

Dit beleid heeft als doelen:

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

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

Reikwijdte

- Het informatiebeveiligings- en het privacy beleid binnen De Korre geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van De Korre. Het beleid heeft zowel betrekking op gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites.
- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen De Korre waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op andere betrokkenen waarvan De Korre persoonsgegevens verwerkt.
- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van De Korre evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.
- IBP-beleid binnen De Korre heeft raakvlakken met:
 - Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen.
 - Personeels- en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties.
 - IT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen.
 - Medezeggenschap van leerlingen, hun ouders/verzorgers en medewerkers.
 - Beleid inzake aanschaf en gebruik van digitale leermiddelen.

3. UITGANGSPUNTEN

Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij De Korre zijn:

- Informatiebeveiliging en het privacy dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming (die 25 mei 2018 in werking treedt).
De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen. Waarbij een goede balans tussen het belang van De Korre om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is.
- Binnen De Korre is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van fysieke documenten.
- De organisatie is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen moeten goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.
- Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt bij De Korre geclassificeerd. De classificatie is het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risicoanalyse, waarbij gebruik gemaakt wordt van de classificatie. Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.
- De Korre sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) bewerkersovereenkomsten af als zij persoonsgegevens ontvangen van de school. Hierbij wordt gebruik gemaakt van de meest recente versie van het convenant 'Digitale leermiddelen privacy' (www.privacyconvenant.nl) en de bijbehorende model bewerkersovereenkomst. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis.
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagooverlies. De Korre heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.
- Informatiebeveiliging en privacy is bij De Korre een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij De Korre vanaf de start rekening gehouden met informatiebeveiliging en privacy.

Uitgangspunten privacy

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij De Korre zijn:

1. **Doelbepaling en doelbinding:** persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag:** verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie:** bij de verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te

bereiken; ze staan in verhouding staan tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.

4. **Transparantie:** de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun Persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit:** er zijn maatregelen getroffen om te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen. Bij alle registraties op basis van toestemming, zal De Korre aan de betrokkene een eenduidige zogenaamde Opt-out procedure worden aangeboden.

4. WET- EN REGELGEVING

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

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

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

5. ORGANISATIE

Dit hoofdstuk beschrijft hoe IBP in De Korre is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

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

Richtinggevend

Eindverantwoordelijke

Het college van bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de maatregelen vast op het gebied van informatiebeveiliging en privacy. De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages door het cvb geëvalueerd.

Sturend

Manager IBP

Manager IBP is een rol op sturend niveau. Deze geeft terugkoppeling en advies geeft aan de eindverantwoordelijke en stuurt de mensen aan op de uitvoerende laag. De manager IBP moet:

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

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) houdt binnen De Korre toezicht op de toepassing en naleving van de privacy-wetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. FG heeft regelmatig overleg met manager IBP. De FG is meestal ook contactpersoon en voor klachten en vragen van betrokkenen met een vertrouwelijk karakter.

De rol van FG kan bij een jurist of vertrouwenspersoon van de organisatie worden belegd. Het kan ook een privacy officer zijn, deze heeft geen wettelijke taken en bevoegdheden die een onafhankelijke positie garanderen.

Domeinverantwoordelijkheid/proceseigenaar

Binnen De Korre zijn er verschillende domeinen/processen, zoals de scholen, ict, personeel zaken en financiële zaken 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. Leidinggevendenden hebben een voorbeeldrol ten opzichte van hun medewerkers.

Uitvoerend

Security Officer

De Security Officer vormt een technisch aanspreekpunt voor incidenten en informatiebeveiliging.

Functioneel beheerder

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

Medewerkers

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in de vastgestelde documenten. 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 (G)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 manager IBP.

6. CONTROLE EN RAPPORTAGE

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

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

Daarnaast kent De Korre 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.

Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij De Korre het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de manager IBP met het College van Bestuur als eindverantwoordelijke.

Classificatie en risicoanalyse

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

Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij het hoofd IT.

De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken.

Controle, naleving en sancties

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

Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de Functionaris Gegevensbescherming (FG) een belangrijke rol. De FG wordt aangesteld door het college van bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

De FG werkt via een door het cvb vast te stellen reglement.

Mocht de naleving ernstig tekort schieten, dan kan De Korre de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Bij De Korre is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

BIJLAGE 1: TABEL IBP ROLLEN EN TAKEN

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 Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens Evalueren toepassing en werking IBP-beleid op basis van rapportages Organisatie IBP inrichten 	<ul style="list-style-type: none"> Informatiebeveiligings- en privacy beleid Baseline / basismaatregelen Reglement FG vaststellen Privacyreglement vaststellen
Sturend (tactisch)	Manager IBP	<ul style="list-style-type: none"> Inhoudelijk verantwoordelijk voor IBP IBP-planning en controle Adviseert bestuur/CvB/directie over IBP Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse Hanteren IBP normen en wijze van toetsen Evalueren IBP-beleid en maatregelen Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen 	Processen, richtlijnen en procedures IBP, waaronder: <ul style="list-style-type: none"> Activiteitenkalender; protocol beveiligingsincidenten en datalekken; bewerkerovereenkomsten regelen; brief toestemming gebruik foto's en video; opstellen informatie documentatie richting leerlingen, ouders / verzorgers; security awareness activiteiten; sociale media reglement; gedragscode ict en internetgebruik; gedragscode medewerkers en leerlingen.
	Functionaris voor Gegevensbescherming	<ul style="list-style-type: none"> Toezicht op naleving privacy wetgeving Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens Afwikkeling klachten en incidenten 	<ul style="list-style-type: none"> Privacyreglement; procedure IBP-incident afhandeling; inrichten meldpunt datalekken.
	Domeinverantwoordelijke/ Proceseigenaren waaronder: directeuren en stafmedewerkers, financiën, P&O en administratie	<ul style="list-style-type: none"> Classificatie / risicoanalyse in samenwerking met Manager IBP Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door cvb <i>Samen met functioneel beheer en ICT beheer</i> er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. <i>Samen met functioneel beheer en ICT beheer</i> de toegangsrechten van gebruikers regelmatig beoordelen en controleren. 	<ul style="list-style-type: none"> inventariseren waar persoonsgegevens van de organisatie terecht komen (leveranciers lijst); classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: <ul style="list-style-type: none"> Toegangsmatrix diverse informatiesystemen en netwerk.

Uitvoerend (operationeel)	<p>Security officer</p> <p>Functioneel beheerder</p> <p>Medewerker</p> <p>Dagelijkse leiding / leidinggeven de / directie</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

BIJLAGE 2: GLOBALE TIJDSINVESTERING IBP

Globale tijdsinvestering IBP					
<i>Tijdsinvestering per medewerker per week</i>	<i>cvb</i>	<i>Manager IBP/Functionaris gegevensbeheer</i>	<i>ICT</i>	<i>Directeuren en hoofden van dienst</i>	<i>HR en administraties</i>
Tot juni 2018	2 uur	8 tot 16 uur	8 uur	4 uur	8 uur
Jaarlijks vanaf schooljaar 18-19	0,5 uur	4 uur	4 uur	2 uur	2 uur

BIJLAGE 3: CHECKLIST AANPAK IBP

Checklist aanpak IBP		
Onderwerp	Planning	Gereed
IBP-beleid is gemaakt, en vastgesteld door het cvb.		
Activiteiten kalender is gemaakt.		
Risicoanalyse is uitgevoerd.		
Op basis van de risicoanalyse zijn de belangrijkste te nemen maatregelen bepaald en vastgesteld.		
Er is een lijst met systemen en leveranciers, die persoonsgegevens verwerken.		
Basiskennis personeel over privacy is op orde.		
Protocol beveiligingsincidenten en datalekken is opgesteld.		
Er is een meldpunt datalekken en beveiligingsincidenten.		
Afspraken en procedures over privacy zijn geregeld.		
Privacyreglement is gemaakt en vastgesteld.		
Overzicht is gemaakt met welke leveranciers nog (model) bewerkersovereenkomsten moeten worden gesloten.		
Overzicht is gemaakt met welke leveranciers al een (model) bewerkersovereenkomsten is gesloten.		
Er wordt aan ouders/leerlingen voortaan om toestemming gevraagd om foto's en video's van leerlingen te gebruiken.		
Er wordt door de school en medewerkers bewust omgegaan met sociale media.		
Sociale-mediaprotocol of gedragsregels vastgesteld.		
Er is aandacht voor mediawijsheid of digitale geletterdheid van leerlingen.		
Er is een gedragscode ICT- en internetgebruik.		
Afspraken over passend onderwijs zijn gemaakt.		
Afspraken met/over externe hulpverleners zijn gemaakt en bekend bij de betrokken medewerkers.		
Er zijn afspraken over de uitwisseling van leerlingdossiers en -gegevens met andere scholen.		
De autorisaties en rollen van medewerkers zijn vastgesteld (bijv. m.b.v. een autorisatiematrix).		
De autorisaties en rollen van medewerkers zijn in de administratiesystemen ingevoerd en geregeld.		
Evaluatie van het IBP-beleid.		
Verbetervoorstellen IBP.		
Security awareness training is gegeven aan alle medewerkers.		
Relevante medewerkers zijn op de hoogte van de regels over het omgaan met leerling dossiers.		
Privacyreglement is gecommuniceerd en opgenomen op website en/of in schoolgids.		
Sociale-mediareglement is bekend gemaakt.		
Gedragscode ICT- en internetgebruik is bekend gemaakt.		
Leerlingen zijn geïnformeerd over IBP op school.		
Ouders worden actief benaderd en geïnformeerd over IBP op school.		
De (G)MR is (wordt regelmatig) geïnformeerd over IBP op school.		