Samenwerkende Vrijescholen Zuid-Holland

Informatiebeveiliging en privacybeleid

Oktober 2018

Stichting Samenwerkende Vrijescholen Zuid Holland

Vastgesteld door *Naam toevoegen.*

Versie	Datum	Naam	Functie
0.1	27-09-18	AVG-team	
0.2	11-10-18	AVG-team	
0.2		J.Gommers	bestuurder

Versie	Status	Datum	Auteur	Omschrijving
0.1	Concept	25-09-18		Voorzet van Reinier
0.2	Defcon	11-10-18		AVG team

Inhoud

Inleiding

De continuïteit van het onderwijs en de bedrijfsvoering op onze scholen is afhankelijk van informatie en (veelal geautomatiseerde) informatievoorziening. Omdat we met persoonsgegevens (van onszelf, leerlingen en anderen) werken, is privacywetgeving daarop van toepassing.
Het voorliggende document is samengesteld op basis van een concept van de Deventer Scholen. Zij hebben het concept opgesteld op basis van saMBO-ICT en Kennisnet en in samenwerking van de Deventer schoolbesturen voor het PO. Directe aanleiding hiertoe is de aanscherping van de Algemene Veroordeling Gegevensbescherming (AVG) per 25 mei 2018. *Dit document geldt voor het genoemde bestuur en alle aangesloten scholen/organisatieonderdelen.* Het document wordt minimaal elke twee jaar herzien om aan de geldende wetgeving te blijven voldoen. De GMR heeft in dit traject telkens instemmingsrecht.
Alle persoonsgebonden informatie willen wij zo zorgvuldig mogelijk bewaren en verwerken en zo beschermen tegen een vergissing, uitlekken, een aanval, de natuur (bijv. overstroming of brand), etc. Om dit structureel op te pakken is het noodzakelijk dat we duidelijk maken waar het om gaat, een doel stellen en de manier waarop we dit doel willen bereiken.

1. Uitleg en achtergronden

Informatiebeveiliging en privacy

Wij verstaan onder informatiebeveiliging het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten ‘beschikbaarheid’, ‘integriteit’ en ‘vertrouwelijkheid’ van de informatievoorziening te garanderen.De betekenis van deze aspecten is als volgt te omschrijven:

- **Beschikbaarheid**: informatie en aanverwante bedrijfsmiddelen zijn toegankelijk wanneer nodig;
- **Integriteit**: informatie en verwerkingsmethoden bevatten zo min mogelijk fouten;
- **Vertrouwelijkheid**: informatie is alleen toegankelijk voor diegenen die daartoe bevoegd zijn.

Privacy gaat om de bescherming van persoonsgegevens conform de huidige wet- en regelgeving. Door het goed toepassen van informatiebeveiliging kan aan deze wetgeving worden voldaan. Vooral het aspect vertrouwelijkheid is hiervoor van belang. Informatiebeveiliging is daarom integraal onderdeel van privacy. Om privacy goed te regelen is informatiebeveiliging nodig. Daarom zien we het als één onderwerp: informatiebeveiliging en privacy (IBP).

Doel en reikwijdte

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.
- Het voorkomen van financiële risico’s (claims, boetes).

Dit beleid is een leidraad voor iedereen die betrokken is bij IBP binnen onze organisatie. Het is van toepassing op onze eigen medewerkers, tijdelijk personeel en andere personen die een rol spelen in het bestuur en de school/scholen. Het is van toepassing op de hele organisatie van het bestuur, waaronder de fysieke locaties, systemen op interne en externe locaties en gegevensverzamelingen die gebruikt worden.
Het is nog zinvol om ook het onderliggende doel voor het gebruik van (digitale) gegevens te vermelden. Recent is digitalisering in het onderwijs in een versnelling geraakt en raakt het steeds meer verweven met

het onderwijsproces. Wat betreft het gebruik van data in het onderwijs gaan wij uit van vijf hoofddoelen[1] die voor elke school relevant zijn:[2]

- de ontwikkeling van leerlingen,
- het optimaal functioneren van medewerkers,
- een efficiënte bedrijfsvoering,
- heldere verantwoording en
- effectieve samenwerking met partijen buiten de school (binnen en buiten het bestuur).

Uitgangspunten

De belangrijkste beleidsuitgangspunten bij het bestuur zijn:

- Er is een balans tussen privacy, functionaliteit/werkbaarheid en veiligheid, waarbij er in ieder geval van uitgegaan wordt dat de informatiebeveiliging en de waarborg op de privacy voldoen aan alle relevante wet- en regelgeving.
- Veilig en betrouwbaar omgaan met informatie is de verantwoordelijkheid van iedereen.
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Iedere school en/ of bestuur heeft dit ook vastgelegd in een eigen integriteitscode en gedragscode.
- Het bestuur is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt.
- Het bestuur maakt met alle partijen waarmee persoonsgegevens worden uitgewisseld concrete afspraken over informatiebeveiliging en privacy.
- IBP is een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
- Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.

Verantwoordelijkheden

Het informatiebeveiligingsbeleid is gebaseerd op de volgende verantwoordelijkheden:

a. Informatiebeveiliging is de primaire verantwoordelijkheid van het bestuur op stichtingsniveau en van de schoolleider op schoolniveau. Zij dragen zorg voor een goede informatiebeveiliging. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan.
b. Informatiebeveiliging is ieders verantwoordelijkheid. De schoolleider communiceert met individuele personen, zoals intern begeleider, leraar, ouders en 'derden' (bijv. stagiaires, de schoonmaker, de cv-monteur) dat van hen verwacht wordt dat ze actief bijdragen aan de veiligheid van informatie, al dan niet opgeslagen in geautomatiseerde systemen. Dat gebeurt bij aanstelling, tijdens de gesprekkencyclus, bij het periodiek bespreken van de gedragscode, met periodieke bewustwordingscampagnes, bij het sluiten van contracten.
c. Uitgangspunt is dat evenwicht tussen vrijheid van handelen en veiligheid van informatie bewaard blijft. Dat evenwicht kan voor verschillende individuen of groepen binnen de school anders liggen.
d. Iedereen behoort de waarde van informatie te kennen en daarnaar te handelen. Deze waarde wordt bepaald door de schade als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid. 'Waardering' van informatie gebeurt aan de hand van de zgn. 'classificatie' (zie volgende paragraaf).
e. Het bestuurder 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

[1] Deze hoofddoelen zijn geformuleerd door Kennisnet.

[2] zie voor handvaten voor een nadere analyse van de inzet van ICT op school en de gegevensprocessen https://www.kennisnet.nl/fileadmin/kennisnet/publicatie/Omgaan_met_data_in_het_onderwijs.pdf.

wordt op basis van regelmatige rapportages geëvalueerd.

Vuistregels voor privacy

Het bestuur hanteert de vijf vuistregels voor privacy:

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 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.

Deze vuistregels zijn vertaald in een apart privacyreglement van de organisatie. Ook dit reglement wordt minimaal een keer per twee jaar herzien.

Wet- en regelgeving en overeenkomsten

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

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs;
- Wet goed onderwijs (inclusief code goed bestuur PO/VO);
- Wet bescherming persoonsgegevens;
- Algemene Verordening Gegevensbescherming (AVG);
- Archiefwet;
- Leerplichtwet;
- Auteurswet (o.a. alleen gebruiken van legale software)
- Wetboek van Strafrecht.

Hiernaast zijn de bepalingen van het convenant ‘Digitale onderwijsmiddelen en privacy 3.0’ (zie https://www.privacyconvenant.nl/het-convenant) leidend bij het maken van afspraken met leveranciers van digitale onderwijsmiddelen. Zonder ondertekening wordt er geen zaken gedaan met desbetreffende leverancier, indien er persoonsgegevens gebruikt worden. Het schoolbestuur sluit met leveranciers modelbewerkersovereenkomsten af, als dat niet op een ander niveau geregeld is.

2. Organisatie van gegevensverwerking en IBP

Classificatie en risicoanalyse

Bij ons 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. Door de informatie onder te verdelen in openbaar, intern of vertrouwelijk, wordt duidelijk voor welke groep van mensen deze informatie al dan niet beschikbaar dient te zijn en welke maatregelen genomen dienen te worden ter beveiliging van deze informatie.

Klasse	Basisprincipes	Maatregelen
Openbaar	Iedereen mag de gegevens inzien, bijvoorbeeld de website van de stichting en/of de scholen.	Geen
Intern	Iedereen die aan de school is verbonden als medewerker, stagiaire of ouder mag deze gegevens inzien. Toegang kan zowel binnen als buiten de school (remote) worden verleend. Een geselecteerde groep mag deze gegevens wijzigen o.g.v. hun specifieke toegekende rechten.	Toegang via generiek inloggen of informatie beschikbaar binnen de school.
Functie-specifiek	Alleen voor de betreffende functie nodig, toegangsrechten verleend. Gegevens mogen wel door anderen binnen de school gezien worden als dat nodig is voor het werk.	Toegang via inlog op naam.
Vertrouwelijk	Er is expliciet aangegeven wie welke rechten heeft t.a.v. de raadpleging van deze gegevens, bijvoorbeeld bijvoorbeeld melding veilig thuis van het kind, 1-op-1 gesprekken leraar – ouder(s) en leraar beoordelingen.	Toegang via inlog op naam, of informatie is gearchiveerd in een afgesloten ruimte.

Leerlinggegevens en gegevens ouders

Op school wordt gewerkt met een inschrijfformulier, waarvan de gegevens worden overgenomen in het leerlingadministratiesystemen (LAS) ParnasSys.[3] De gegevens van ouders zijn aan die van de leerling gekoppeld. Hierbij is het uitgangspunt leidend om alleen die gegevens op te nemen die voor de uitvoering van het ontwikkelings- en leerproces en voor het contact met ouders/verzorgers en andere instanties nodig zijn (zgn. dataminimalisatie). Enkele relevante gegevens kunnen ook worden overgezet naar andere (volg)systemen en digitale leermiddelen. Een deel van deze systemen is gekoppeld aan ParnasSys. Met alle leveranciers zijn verwerkersovereenkomsten afgesloten (zie deel 4). In principe worden alle leerlinggebonden gegevens in ParnasSys opgeslagen. Tussentijdse documenten met verdergaande persoonlijke informatie worden alleen op afgeschermde plekken opgeslagen (bijv. SharePoint van school of beperkt gedeelde mappen in Google for education). De mate van afscherming is afhankelijk van de gevoeligheid van de informatie (toetsgegevens versus melding huiselijk geweld).
Apparaten worden beveiligd door middel van :

- telefoon: toegang door middel van veilig wachtwoord en lock functie,
- laptop: toegang door middel van veilig wachtwoord en encryptie,

[3] Let wel op verschil tussen intake (belangstelling voor school) en daadwerkelijke inschrijving. Let ook in het algemeen erop of alle informatie direct digitaal moet worden opgeslagen.

- tablet: toegang door middel van veilig wachtwoord ,
- thuis computer: toegang door middel van veilig wachtwoord en encryptie.

Daarbij ook kinderen of derden **niet** onder jouw school- en/of privé-account laten werken.

Medewerkersgegevens

Medewerkersgegevens worden opgenomen in personeelsadministratiesystemen (Raet), in systemen voor de documentatie van bekwaamheidsontwikkeling, in communicatiesystemen en systemen om bijv. (anoniem) enquêtes uit te zetten. Overige gegevens van medewerkers die verder gaan dan NAW en formatieomvang worden op afgeschermde plekken opgeslagen, bijv. SharePoint-subsite of drive van Google for education van schoolleider of HR-medewerker.

- Gespreksverslagen
- Mail
- Enquêtes

Externe gegevens onder verantwoordelijkheid van SVZH zijn onder andere:

- Pensioengegevens (grondslag is contract, nl. CAO)
- Vervangingsfonds (grondslag is contract, nl. CAO)
- Belastingdienst (grondslag is wetgeving)
- UWV (grondslag is wetgeving)
- Participatiefonds (CAO)

Beperkte houdbaarheid

Leerlingen en medewerkers hebben het recht om te zijner tijd ‘vergeten te worden’. De bewaartermijn van gegevens wordt gehanteerd conform de geldende wetgeving. De gegevens worden in verschillende systemen automatisch gewist.
De overige gegevens worden handmatig verwijderd.

Bewustwording en borging

Beleid en maatregelen zijn niet voldoende om risico’s op het terrein van informatiebeveiliging uit te sluiten. Daarom wordt binnen de school het bewustzijn voortdurend aangescherpt, zodat kennis van risico’s wordt verhoogd en (veilig en verantwoord) gedrag wordt aangemoedigd. Bewustwording, evaluatie en borging hebben daarom een plek in de gedragscode die minimaal 1x per schooljaar in het team aan de orde komt. De specifieke invulling van informatiebeveiligingsbeleid per school wordt jaarlijks op inhoud, uitvoerbaarheid en implementatiestatus beoordeeld en, indien nodig, aangepast. Dit gebeurt door de schoolleider in samenwerking met team en MR.
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 ons 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, vrijwilligers, ouders, externen en stagiaires. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de schoolleider in samenwerking met de bestuurder.

Toegang

Op schoolniveau is de schoolleider verantwoordelijk voor het toekennen van toegang c.q. rechten tot het schoolgebouw (sleutel, alarmcode), educatieve software (login en wachtwoorden), digitale (administratie)programma’s, leerling- en/of leraar-dossiers (afsluitbare ruimte), computers en netwerkvoorzieningen. Leidraad voor toekennen van toegangsrechten is de classificatie van de toegankelijke informatie. Minimaal 1x per jaar en indien nodig vaker maakt de schoolleider de afweging of toegang generiek of individueel gewijzigd dient te worden.

Op schoolniveau is fysieke toegang tot het gebouw geregeld onder verantwoordelijkheid van de schoolleider. Voor fysieke data gelden dezelfde regels als voor digitale data. Dat wil zeggen dat vertrouwelijke documenten achter slot en grendel opgeborgen zijn, waarbij dezelfde functionarissen toegang hebben als tot de digitale informatie.

Clear desk en clear screen

Medewerkers zijn er zelf verantwoordelijk voor dat vertrouwelijke informatie niet inzichtelijk is voor derden.
De regel is dat:

1. Computers en laptops altijd worden geblokkeerd bij afwezigheid.
2. Vertrouwelijke fysieke documenten worden opgeborgen.

Back up

Indien van toepassing worden van alle bedrijfsbestanden worden centraal back ups gemaakt conform het volgende schema:

- dagelijks incremental
- bewaren van minimaal laatste 3 versies
- verwijderde bestanden

Verwijderen van back ups conform wettelijke bewaartermijn.

- Jaarlijks een full back up, na 3 jaar vernietiging

3. Controle

Naleving, controle en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces.
De functionaris gegevensbescherming is centraal ingehuurd bij OBT in samenwerking met een aantal andere scholen. Per school is een IBP verantwoordelijke vastgesteld, dat kan de schoolleider zijn. De taakverdeling is uitgewerkt in de betreffende bijlage.

Mocht de naleving ernstig tekort schieten, dan kan het bestuur de betrokkenen een sanctie opleggen, binnen de kaders van de CAO en/of de wettelijke mogelijkheden.

Medewerkers en andere aan school betrokkenen

Van belang hierbij is dat leidinggevenden medewerkers aanspreken in geval van het niet naleven van het vastgestelde beleid. Bij onze stichting wordt actief aandacht besteed aan IBP bij onder andere de aanstelling van nieuwe medewerkers, tijdens gesprekken, en in documentatie.
Met andere aan school verbonden personen (externen, vrijwilligers, stagiaires etc) worden geheimhoudingsverklaringen opgesteld, waarbij instructies worden gegeven.

Ouders

Daarnaast worden ouders op de hoogte gesteld van de interne regelgeving vanaf aanmelding van hun kind(eren). De eisen die gesteld worden aan de ouders worden gecommuniceerd door middel van het onder de aandacht brengen van de betreffende protocollen en richtlijnen.

Incidenten en meldplicht

Beveiligingsincidenten worden altijd gemeld bij de IBP-verantwoordelijke van de betreffende school, de schoolleider, de bestuurder en/of de FG (in deze volgorde). De afhandeling van deze incidenten volgt een

gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken. Afhankelijk van de impact treft de FG en zo nodig de bestuurder zelf adequate maatregelen. Wat betreft de ernst van de situatie is er verschil tussen een beveiligingsincident of een datalek. In geval van een beveiligingsincident is er in feite sprake van een gat in de beveiliging en is het zaak dit gat zo snel mogelijk te dichten. Dit begint al bij het beplakken van de computer met wachtwoorden.
Er is sprake van een datalek wanneer het er ook daadwerkelijk persoonsgegevens 'op straat' zijn komen te liggen en hiermee in handen zijn gekomen van personen of organisaties die deze gegevens niet zouden mogen hebben. Alle datalekken zijn beveiligingsincidenten, maar niet ieder beveiligingsincident is een datalek. Voorbeelden van datalekken:

- e-mail met persoonsgegevens verzonden naar verkeerd e-mailadres;
- laptop met persoonsgegevens gestolen / verloren;
- het verliezen van een USB stick met vertrouwelijke informatie;
- per abuis vertrouwelijke informatie publiceren in een publiek toegankelijke omgeving of nieuwsbrief, etc.

Controle en rapportage

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

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

Daarnaast kent het bestuur 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. Voor deze evaluatie stelt de FG jaarlijks een monitorrapportage op over de uitgevoerde controles en de incidenten.

Bijzondere afwegingen

Binnen ons werk kunnen wij te maken hebben met tegenstrijdige belangen en zelfs tegenstrijdige regelgeving. Zo kan bijv. het recht om vergeten te worden op gespannen voet staan met de behoefte voor latere eigen inzicht in gegevens. Het belangrijkste is om zich daarvan bewust te zijn en zo nodig een duidelijke afweging te maken. In alles staat het belang van het kind en zijn ontwikkeling centraal.
[Ruimte om zo nodig bijzondere afwegingen te beschrijven].

Bijlage 1: Verantwoordelijkheid en taken

Wie **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**
Bestuur	● 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	● Informatiebeveiligings- en privacy beleid ● Baseline / basismaatregelen ● Reglement vaststellen voor de Functionaris voor de Gegevensbescherming (privacy officer), belast met IBP ● Privacyreglement vaststellen
Schoolleider (is IBP-verantwoordelijke)	● Inhoudelijk verantwoordelijk voor IBP op schoolniveau ● Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door het bestuur ● IBP-planning en controle ● Adviseert bestuur 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 ● Beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	Processen, richtlijnen en procedures IBP, waaronder: ● Activiteitenkalender ● Protocol beveiligingsincidenten en datalekken ● Bewerkersovereenkomsten regelen ● Brief toestemming gebruik foto's en video ● Opstellen informatie documentatie richting leerlingen, ouders / verzorgers ● Security awareness activiteiten ● Sociale media reglement ● Gedragscode ict en internetgebruik ● Gedragscode medewerkers en leerlingen
Functionaris Gegevensbescherming (FG)	● Toezicht op naleving privacy wetgeving, nader beschreven in reglement (QuickScan enz.) ● Afwikkeling klachten en incidenten	● Monitoringsverslag IBP (jaarlijks) ● Procedure IBP-incident afhandeling ● Inrichten meldpunt datalekken
ICT'er/ adm. kantoor/Netwerk-beheerder	● Classificatie- en Risicoanalyse ism MT ● Toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. ● De toegangsrechten van gebruikers regelmatig beoordelen en controleren. ● Incidentafhandeling (registreren en evalueren). ● Technisch aanspreekpunt voor IBP-vragen. ● Beschikbaarheid en vertrouwelijkheid van netwerkapparatuur.	● Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) ● Classificatie- en risicoanalyse documenten. ● Toegangsmatrix diverse informatiesystemen en netwerk ● Inrichten netwerk ● Voorzien in beveiligingsmaatregelen zoals anti virus, firewall, anti-etc. ● Redundantie (disks en werkprocessen) ● Monitoren van functioneren van centrale netwerkapparatuur ● Monitoren van updates
Alle medewerkers	● Uitvoeren taken conform gegeven richtlijnen en procedures en implementeren IBP-maatregelen. ● Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. ● Communicatie over IBP naar de kinderen. ● Zelf op de hoogte zijn van het IBP-beleid en de consequenties ervan. ● Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. ● Informatiebeveiliging bespreken in werkoverleggen, beoordelingen etc.	Communiceren, informeren en toezien op naleving van o.a.: ● IBP in het algemeen ● Regels passend onderwijs ● Hoe omgaan met leerling dossiers ● Wie mogen wat zien ● Gedragscode ● Omgaan met sociale media ● Mediawijs en digitaal geletterd maken

Bijlage 2: Ondersteunende documenten

Deze bijlage bevat een verwijzing naar een aantal aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Een aantal zijn vanuit de Algemene Verordening Gegevensbescherming verplicht.

Processen die nog moeten worden uitgewerkt

- Beleidscyclus aanvullen met IBP-elementen (bijvoorbeeld dat in de schoolgids IBP-beleid opgenomen wordt en in het jaarverslag evaluatie IBP staat)
- Risico-analyse
- Wijzigingen wetgeving
- Inkoop IBP/ verwerkersovereenkomsten (controleren of verwerkersovereenkomst is afgeleid van PO-raad-model)
- Toegang verlenen, wijzigingen, bewaken en intrekken (logische toegangsbeveiliging)
- Back up en restore
- Datalogging en bewaking
- Verwijderen van data
- Beveiligingsincidenten (inclusief registratie)
- Melden van datalekken
- Procedure gegevensbeschermingseffectbeoordeling (DPIA)
- Procedure toestemming gebruik beeldmateriaal (toestemmingsbrief)
- Procesbeschrijving rechten betrokkenen (proces rondom aanvragen van betrokkenen)

In personeelshandboek/huishoudelijk reglement

Vanuit de standaard van Athena

Communicatie rechten betrokkenen (communicatie richting betrokkenen)
Privacyreglement
Autorisatiematrix (wie mogen gegevens inzien, bewerken enz.)
Afspraken gebruik sociale media
Procedure rondom training medewerkers (bewustzijn creëren)
Cameratoezicht
Wachtwoordbeleid
Responsible disclosure
Gedragscode ict en internetgebruik
Acceptable use policy (verantwoord gebruik bedrijfsmiddelen)
Procedure rondom uitwisselen gegevens (passend onderwijs, leerling dossiers, leerplicht enz)

Verplicht vanuit de AVG:

Dataregister om te voldoen aan de registratieplicht
Verwerkersovereenkomsten (privacy bijlage beschikbaar stellen)
Functionaris voor Gegevensbescherming (communicatie hierover richting medewerkers)