Informatiebeveiliging en privacybeleid

Januari 2018

Stichting Openbaar Primair Onderwijs Deventer

Andriessenplein 22a
7425 GX Deventer
Telefoon: 0570-782401
e-mail: openbaaronderwijs@opo-deventer.nl

Vastgesteld door *Naam toevoegen.*

Versie	Datum	Naam	Functie
1.0	31/1/18	Yvonne de Haas	Bestuurder

Versie	Status	Datum	Auteur	Omschrijving
0				saMBO-ICT en Kennisnet
0.1	concept	3 febr 2017	AE	Eerste opzet
0.2	Concept	20 nov 2017	TV/MT	Nieuwe omvattende structuur en vulling, Goedkeuring BOD dec-17
0.3	Concept	23 jan 2018	MT	Verwerking van opmerkingen van VOS-ABB jurist
0.4	Vastgesteld	30 januari 2018	BOD	
0.5	Vastgesteld	31 januari 2018	OPOD	

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 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 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 directeur 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 directeur 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

[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.

het gebied van informatiebeveiliging en privacy. De toepassing en werking van het IBP-beleid 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 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.

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 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’ (zie https://www.privacyconvenant.nl/het-convenant) leidend bij het maken van afspraken met leverancier 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. Een geselecteerde groep mag deze gegevens wijzigen.	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, bijvoorbeeld nieuwsbrief, klassikale gegevens. Een geselecteerde groep mag deze gegevens wijzigen o.g.v. hun specifieke toegekende rechten.	Toegang via generiek inloggen of informatie beschikbaar binnen de school.
Vertrouwelijk	Er is expliciet aangegeven wie welke rechten heeft t.a.v. de raadpleging en de verwerking van deze gegevens, bijvoorbeeld ontwikkelresultaten 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.

Welke (categorieën) persoonsgegevens in principe kunnen worden opgeslagen/verwerkt, is in bijlage 1 weergegeven.

Leerlinggegevens en gegevens ouders

Op school wordt gewerkt met een inschrijfformulier, waarvan de gegevens worden overgenomen in het leerlingadministratiesysteem (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 volgsystemen en digitale leermiddelen. Een deel van deze systemen is gekoppeld aan ParnasSys. Met alle leveranciers zijn bewerkersovereenkomsten 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 verder afgeschermde subsite van IB' er). De mate van afscherming is afhankelijk van de gevoeligheid van de informatie (toetsgegevens versus melding huiselijk geweld).

[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.

Medewerkersgegevens

Medewerkersgegevens worden opgenomen in personeelsadministratiesystemen, in systemen voor de documentatie van bekwaamheidsontwikkeling, in communicatiesystemen en systemen om bijv. (anoniem) enquêtes uit te zetten. Alle gegevens van medewerkers die verder gaan dan NAW en formatieomvang worden op afgeschermde plekken opgeslagen, bijv. OneDrive/SharePoint-subsite van directeur of HR-medewerker.

Beperkte houdbaarheid

Leerlingen en medewerkers hebben het recht om te zijner tijd 'vergeten te worden'. Bestuur en scholen geven de opslag van gegevens (digitaal en schriftelijk) zo vorm dat in principe na 5 jaar alle gegevens van leerlingen vernietigd worden.[4] I.v.m. tegenstrijdige wetgeving rondom toezicht en ter beperking van de administratieve last houdt dit bestuur het termijn van 5 jaar na uitschrijving aan voor de verwijdering van alle gegevens, behalve als ouders/verzorgers een eerdere vernietiging van een deel van de gegevens opeisen. Medewerkersgegevens worden na verlaten van de organisatie gearchiveerd en na 8 jaar vernietigd, behalve gegevens die pensioen-gerelateerd zijn. Een vernietiging moet veilig zijn (shredder resp. 'blauwe container').

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 directeur 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, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de directeur in samenwerking met de bestuurder.

Toegang

Op schoolniveau is de schooldirecteur eindverantwoordelijk 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 directeur de afweging of toegang generiek of individueel gewijzigd dient te worden.

Uitgangspunt voor de toegang is dat binnen school resp. bestuur ieder medewerker kan beschikken over de (ook privacygevoelig) informatie die relevant is voor de processen waarbij de medewerker betrokken is. Op een school is in principe het uitgangspunt dat het team gezamenlijk verantwoordelijk is voor de ontwikkeling van de kinderen. Hiervoor is het belangrijk dat de teamleden inzicht kunnen hebben

[4] ParnasSys heeft ingesteld dat behalve NAW- en loopbaangegevens alle leerlinggegevens worden vernietig 8 jaar na uitschrijving. Maar leerlinggegevens moeten dus al na 5 jaar vernietigd zijn. Scholen moeten vooral de tijdige verwijdering van losse digitale en papieren documenten (zoals toetsen) handig regelen (bijv. dozen op jaar) inclusief vergrendelde opslag.

gegevens van alle kinderen op school, maar in detail zo min mogelijk.[5] Invalleerkrachten krijgen zo beperkt mogelijk toegang tot leerlinggegevens (bijv. tijdelijk tot een bepaalde groep).

Informeren van betrokkene en toestemming

Het bestuur kiest voor een organisatiegerichte benadering van de toestemming voor gegevensgebruik. De organisatiegerichte benadering houdt in, dat niet voor elke gegevensverwerking apart toestemming vereist wordt. Bij specifieke redenen zoals een wettelijke verplichting, de uitvoering van de publiek-rechtelijke taak en gerechtvaardigd belang, is geen toestemming vereist voor gegevensverwerking (artikel 6 AVG). Veel gegevensverwerking is terug te voeren op de Wet op het primaire onderwijs en op wetten over arbeidsovereenkomsten en CAO. Om ook enige overige verwerking af te dekken geldt het volgende beleid: Bij in dienst komen moet een medewerker resp. bij inschrijving van een leerling zijn vertegen-woordiger(s) (ouder/verzorger) expliciet toestemming geven aan het interne opslag en gebruik van die gegevens die voor de uitvoering van het onderwijsproces en daaruit voortkomende processen relevant zijn (rechtsoverweging 32 AVG). De betrokkene wordt in algemene zin geïnformeerd over opslag en gebruik van gegevens, bijv. d.m.v. de schoolgids of een personeelshandboek. Voor zaken buiten het onderwijsproces wordt apart toestemming gevraagd, zoals gebruik van foto's en video's en omgang met sociale media. Minimaal 1x per jaar wordt erop gewezen dat de toestemming kan worden gewijzigd.

Zodra gegevens de organisatie verlaten (school/bestuur), dus verstrekt worden aan derden, bestaat er informatieplicht aan de betrokkene (welke gegevens op welke manier aan wie). Op basis van wet- en regelgeving kan deze plicht ook een instemmingsverplichting inhouden. Bij verstrekken van privacy-gevoelige gegevens aan derden wordt extra goed gelet op gegevensbeveiliging (bijv. per mail alleen versleuteld).[6]

3. Controle

Naleving, controle en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat leidinggevenden medewerkers aanspreken in geval van tekortkomingen. Bij onze stichting wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens gesprekken, en wordt beschreven in de gedragscode.

Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de hiermee belaste Functionaris voor de Gegevensbescherming (FG ofwel privacyofficer). Deze functionaris heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak en werkt volgens een door het bestuur ondertekend reglement. Voor de invulling van deze functie wil het bestuur samenwerken met andere besturen. De FG ziet alles voorbij komen en kan als een 'spin in het web' bijsturen waar nodig.

- Eén adres om te communiceren;
- Eén proces voor de duidelijkheid;
- Eén register voor het overzicht.

Voor de overige rollen in een goed IBP-proces zie bijlage 2.

[5] Voorbeeld voor een afweging: Om een incident met een leerling uit een andere groep adequaat te plaatsen en te documenteren, heeft een leerkracht inzicht nodig in eerdere documentatie over het gedrag van een leerling. Echter, dat hoeft niet in te houden dat de leerkracht bijv. ook de BSN ziet.

[6] Voor alle duidelijkheid: Voor onderwijsinstellingen is een uitzondering gemaakt op de meldplicht van gegevensverwerking bij het College Bescherming Persoonsgegevens (CBP).

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

Incidenten en meldplicht

Beveiligingsincidenten worden altijd gemeld bij de FG, belast met IBP. De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken. Dit proces is uitgewerkt in een apart document samen met de functieomschrijving van de FG. 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.

Recht op inzage en klachten

Een betrokkene resp. zijn vertegenwoordiger heeft altijd recht op inzage in gegevens die over hem/haar zijn verwerkt. De betrokkene kan zich hiervoor wenden aan een medewerker die toegang heeft tot de betreffende gegevens, bijv. de leerkracht. Een medewerker kan doorverwijzen, bijv. naar de directeur.

Wie klachten heeft m.b.t. informatiebeveiliging en privacy kan in eerste instantie terecht de directeur (school) of bestuurder (bestuur). Leidt dit niet tot tevredenheid, kan de Functionaris voor de Gegevens-bescherming worden benaderd. De FG zal de klacht zo veel mogelijk afwikkelen en zo nodig bemiddelen. En uiteindelijk kan men zich ook wenden tot het College bescherming persoonsgegevens.

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: Overzicht categorieën persoonsgegevens

De volgende (categorieën) persoonsgegevens kunnen worden verwerkt:

- naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens van de betrokkene;
- het persoonsgebonden nummer (BSN);
- nationaliteit;
- gegevens als bedoeld onder a, van de wettelijk vertegenwoordiger of verzorger van de leerling;
- gegevens betreffende de gezondheid of het welzijn van de leerling voor zover die noodzakelijk zijn voor de ondersteuning;
- gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor de school, het onderwijs of de te geven ondersteuning;
- gegevens betreffende de aard en het verloop van het onderwijs en ondersteuning, alsmede de behaalde leerresultaten;
- schoolgegevens (waaronder naam school, naam intern begeleider, klas/groep waarin de leerling zit, tijdstip van inschrijving bij deze school, naam van de indiener van de aanmelding bij het samenwerkingsverband, schoolloopbaan en rapportage vanuit primair en voortgezet onderwijs);
- aanleiding voor de aanmelding bij het samenwerkingsverband, relevante screenings- en onderzoeksgegevens en omschrijving van de problematiek die aan de orde is;
- activiteiten die door de school zijn ondernomen rond de betreffende leerling, alsmede de resultaten hiervan;
- bestaande of (relevante) afgesloten hulpverleningscontacten en de namen van contactpersonen;
- relevante persoonsgegevens die door externe partijen worden verstrekt met betrekking tot de aangemelde problematiek van de betreffende leerling;
- relevante financiële gegevens over bijvoorbeeld schoolgeld;
- etc.

Bijlage 2: 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 (FG ofwel privacy officer), belast met IBP • Incidentenproces uitwerken en communiceren • Bewerkersovereenkomsten regelen • Voorbeelden vaststellen m.b.t. foto's en video, sociale media, gedragscodes. • Toestemming vragen gegevensverwerking medewerkers
Schooldirecteur	• Inhoudelijk verantwoordelijk voor IBP • 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 (overige voor school) • 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 • Toestemming vragen gegevensverwerking leerlingen aan ouders/verzorgers • Minimaal 1x per jaar borging afspraken, mogelijkheid om toestemming aan te passen en heroverweging toegang tot gegevens
Functionaris Gegevensbescherming (FG)	• Toezicht op naleving privacy wetgeving, nader beschreven in reglement (QuickScan enz.) • Afwikkeling klachten en incidenten	• Monitoringverslag IBP (jaarlijks) • procedure IBP-incident afhandeling • Inrichten meldpunt datalekken

ICT' er/ adm. kantoor	Classificatie- en Risicoanalyse ism MT • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door het bestuur • 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.	• Inventariseren waar persoonsgegevens van de school terechtkomen (lijst leveranciers) • Classificatie- en risicoanalyse toepassen op soorten documenten • Toegangsmatrix diverse informatiesystemen en netwerk

Alle mede-werkers	• 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. • Betrokkene/vertegenwoordiger informeren als gegevens aan derden worden verstrekt	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerlingdossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken