Informatiebeveiligings- en privacybeleid

Beleidskader ontwikkelen en vaststellen nieuw beleid			
		Versienr:	21122021
Auteur / Eigenaar:	UB		
	Directies	**Datum:**	Ter kennisgeving 21122021
	TZH	**Datum:**	Ter kennisgeving 21122021
	MR	**Datum:**	instemming op:
Start implementatie	Dec. 2021	**Datum:**	In concept

Bron: Kennisnet

Inhoudsopgave

1 Het belang van informatiebeveiliging en privacy

1.1 Belang

Veilig omgaan met persoonsgegevens is een groot goed in het onderwijs. Het betreft immers altijd gegevens over een kwetsbare doelgroep en daarnaast is het onderwijs een sector waar altijd het vergrootglas op ligt. Het belang van de borging van privacy en de implementatie van informatiebeveiliging is dan ook groot, nog los van de wettelijke verplichtingen die op de onderwijssector rust. Het onderwijs wordt daarnaast in steeds grotere mate afhankelijk van ICT-systemen en toepassingen. Dit brengt nieuwe afhankelijkheden, kwetsbaarheden en risico's met zich mee. Dit beleid draagt eraan bij deze risico's te mitigeren tot een aanvaardbaar niveau en biedt een kapstok voor alle organisatorische en technische maatregelen om informatie te beschermen en te waarborgen.

Beschikbare en betrouwbare informatie is van essentieel belang voor de continuïteit van het onderwijs. De organisatie en haar informatievoorziening wordt blootgesteld aan een groot aantal potentiële risico's en bedreigingen, al dan niet opzettelijk van aard. Het proces van privacy borging begint met het definiëren van een beleid op dit punt.

1.2 Doel

Dit beleid heeft tot doel de doelstellingen en uitgangspunten met betrekking tot informatiebeveiliging binnen de organisatie vast te stellen en vast te leggen. Hiermee vormt het beleid de leidraad voor alle betrokkenen bij informatiebeveiliging en privacy, en dient het als spiegel bij de invoering maatregelen binnen de organisatie. Te bestrijden risico's, geaccepteerde risico's en genomen beheersmaatregelen moeten altijd terug te leiden zijn op de uitgangspunten in dit beleid en mogen hier nooit strijdig mee zijn.

Het stelsel van maatregelen heeft tot doel een *blijvend niveau van beveiliging* te realiseren. Door een zorgvuldige borging wordt bereikt dat het gewenste niveau van beveiliging ook op langere termijn blijft gehandhaafd. Hierbij is de organisatie zich ervan bewust dat:

- 100% veiligheid een illusie is. Wel wordt er gestreefd naar een optimaal niveau van beveiliging waarbij altijd op basis van geïdentificeerde risico's passende maatregelen zullen worden genomen om risico's zoveel als mogelijk uit te sluiten of te mitigeren.
- Informatiebeveiliging is gericht op het realiseren van een *optimaal niveau van beveiliging.* Dit optimum wordt bereikt door een zorgvuldige afweging van kosten, functionaliteit en baten.

1.3 Reikwijdte

De reikwijdte van dit beleid wordt hieronder uiteengezet.

- Dit beleid is van toepassing op bestuursniveau en het bestuurskantoor en ook alle onderliggende schoollocaties.

- Dit beleid geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing). Onder dit beleid valt ook alle apparatuur van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.

- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen de organisatie waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op overige betrokkenen waarvan de organisatie persoonsgegevens verwerkt.

- Het beleid geldt voor die toepassingen en applicaties, die vallen onder de verantwoordelijkheid van de organisatie. 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 beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van de organisatie 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 of fysieke locatie zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

2 Informatiebeveiliging en privacy

2.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan:

Het samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening, de gebruikte informatiesystemen en de opgeslagen gegevens.

Informatiebeveiliging in dit beleid richt zich in ieder geval op, maar beperkt zich niet enkel tot de volgende hoofdaspecten:

- Beschikbaarheid (continuïteit): de informatie en informatiesystemen moet op de gewenste momenten beschikbaar zijn;
- Integriteit, de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken;
- Vertrouwelijkheid, de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd/geautoriseerd is.

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

Opgemerkt wordt dat informatiebeveiliging een *samenhangend stelsel* van maatregelen omvat. Dit betekent dat de verschillende maatregelen die tezamen de informatiebeveiliging vormen niet los van elkaar worden getroffen, maar in onderlinge relatie met elkaar staan. Het is belang om te vermelden dat informatiebeveiliging gaat over alle typen gegevens die van belang zijn voor de organisatie, dit in tegenstelling tot privacy.

2.2 Toelichting privacy

Privacy gaat altijd over persoonsgegevens. Volgens de AVG zijn persoonsgegevens:

Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is.

Dergelijke gegevens dienen beschermd te worden conform geldende wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan, waaronder:
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.
De wijze waarop en de voorwaarden waaronder persoonsgegevens mogen worden verwerkt worden uiteengezet in dit beleid.

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 om informatiebeveiliging en privacy binnen Stichting Vrijeschool Almere te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3 Basisprincipes bij het omgaan met persoonsgegevens

De algemene verordening gegevensbescherming kent enkele basisprincipes die gelden voor elk type verwerking van persoonsgegevens. De organisatie committeert zich om gegevens altijd volgens deze principes te verwerken. Deze principes zijn als volgt samen te vatten:

1. **Doelbepaling**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld.

2. **Doelbinding**: Persoonsgegevens worden niet verder verwerkt op een manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

3. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes grondslagen uit de AVG.

4. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot het minimum dat nodig is om het vastgestelde doel te bereiken. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn.

5. **Transparantie**: de organisatie legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens. Deze informatievoorziening vindt ongevraagd en voorafgaande aan verwerking plaats. Daarnaast worden betrokkenen actief gewezen op de rechten die ze hebben.

6. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

7. **Bewaarbeperking**: Gegevens worden niet langer bewaard dan noodzakelijk voor het bepaalde doel of zo lang als wettelijke verplichtingen voorschrijven.

8. **Integriteit en vertrouwelijkheid**: Er worden organistorische en technische maatregelen getroffen om te waarborgen dat de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens intact blijft.

4 Uitgangspunten

In dit hoofdstuk worden de beleidsuitgangspunten, die de organisatie hanteert bij de uitwerking van dit beleid toegelicht. Deze geven de kaders om de doelstellingen rondom informatiebeveiliging en privacy te bereiken. Afwijking van deze uitgangspunten kan alleen met voorafgaande uitdrukkelijke toestemming van het bestuur.

1. Het bestuur van Stichting Vrijeschool Almere 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. Stichting Vrijeschool Almere voldoet aan alle relevante wet- en regelgeving. In het bijzonder geldt hier de algemene verordening persoonsgegevens. (Zie verder bijlage 1)

3. Stichting Vrijeschool Almere legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden.

4. Bij Stichting Vrijeschool Almere is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Deze staan vermeld in het verwerkingsregister.

5. Bij alle verwerkingen die gebeuren op basis van de grondslag toestemming geldt dat deze toestemming altijd voorafgaande aan de verwerking zal worden gevraagd. Hierbij wordt de betrokkene in staat gesteld om vrijwillig, specifiek en ondubbelzinnig toestemming te verlenen of te weigeren. De toestemming zal altijd aantoonbaar zijn. Een betrokkene wordt daarnaast altijd in staat gesteld zijn gegeven toestemming weer in te trekken.

6. Stichting Vrijeschool Almere zal alle betrokkenen helder en actief informeren over de verwerkingen van de hun persoonsgegevens. 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. (Zie verder hoofdstuk 8)

7. Binnen Stichting Vrijeschool Almere 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 papieren documenten.

8. Stichting Vrijeschool Almere sluit met alle partijen die namens haar persoonsgegevens verwerken verwerkersovereenkomsten af.

9. Stichting Vrijeschool Almere verwacht van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties dat zij zich ‘fatsoenlijk’ gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Stichting Vrijeschool Almere heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

10. Informatiebeveiliging en privacy is bij de organisatie een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is. Het doel hierbij is een continue verbetering van informatiebeveiliging en privacy. (Zie verder hoofdstuk 6)

11. De organisatie 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. Hierbij worden de begrippen privacy by design, en privacy by default toegepast. Indien de (nieuwe) verwerking een potentieel hoog risico voor persoonsgegevns oplevert zal de organisatie een DPIA uitvoeren. (Zie verder paragraaf 6.2)

12. De organisatie neemt passende technische en organisatorische (beveiligings-)maatregelen om persoonsgegevens en overige data te beschermen tegen inbreuk op de betrouwbaarheid, integriteit of de vertrouwelijkheid. (Zie verder bijlage 2)

13. De organisatie zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen. (Zie verder hoofdstuk 7)

14. De organisatie maakt personeel en (voor zover van toepassing) overige betrokkenen continue bewust van risico's en werkt aan blijvende bewustwording.

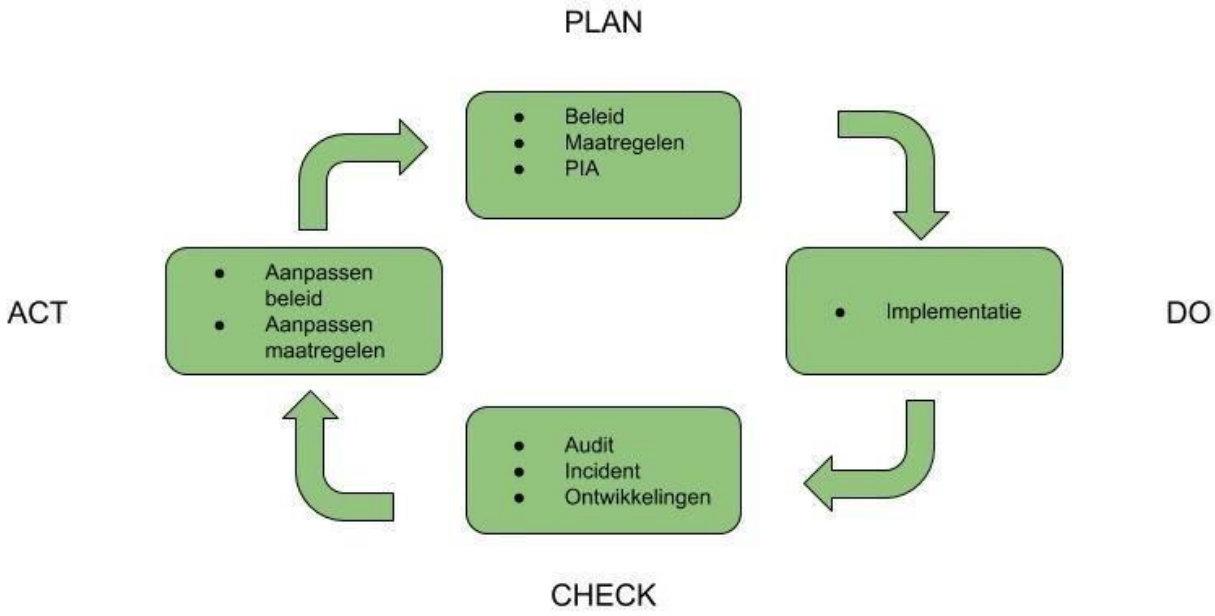
15. De organisatie stelt een functionaris gegevensbescherming aan die toetst of de organisatie aan de verplichtingen uit de AVG voldoet en blijft voldoen. (Zie verder hoofdstuk 9)

16. De organisatie bepaalt voor de verwerkingen die zij uitvoert welke bewaar en/of vernietigingstermijnen van toepassing zijn. Deze bewaartermijnen zullen worden vastgelegd en worden geïmplementeerd.

5 Het proces van informatiebeveiliging

5.1 Cyclisch proces

De continue borging van informatiebeveiliging valt of staat met een cyclus van controle en aanpassing. Het proces voor informatiebeveiliging en privacy omvat dan ook een continu en cyclisch proces. Dit betekent dat op basis van de uitkomsten van evaluaties en controles of door nieuwe ontwikkelingen de noodzaak aanwezig kan zijn het beleid aan te passen, extra maatregelen te treffen of de implementatie hiervan aan te passen. Hier geeft de Deming cirkel houvast zoals hieronder schematisch weergegeven.



5.2 PIA

Indien de organisatie nieuwe verwerkingen start of in huidige verwerkingen significante wijzigingen aanbrengt zal de organisatie de afweging maken of een PIA verplicht is. Hierbij zullen de risico's in kaart worden gebracht. Op basis van de risico's zullen beheersmaatregelen worden gespecificeerd en geïmplementeerd. Deze maatregelen dienen onderdeel te worden van het beheerde beleid.

5.3 Privacy by design en privacy by default

Bij het ontwikkelen en inrichten van nieuwe applicaties of processen zullen de begrippen *Privacy by design* en *privacy by default* worden toegepast. Deze begrippen houden in dat bij het ontwerpen al rekening moet worden gehouden met het borgen van de privacy. Dat kan door in het ontwerp al (technische) maatregelen te treffen (*by design*) of instellingen zo te maken dat privacy de standaard en geen keuze is (*by default*). Deze principes vallen in de praktijk ook vaak samen met het treffen van beheersmaatregelen op basis van een uitgevoerde PIA.

6 Incidenten en datalekken

De organisatie stelt een protocol op voor het melden van incidenten. Hiermee geeft zij invulling aan de meldplicht datalekken. Binnen de organisatie wordt onderscheid gemaakt in:

- **Beveiligingsincident**; een beveiligingsincident is een gebeurtenis die er voor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- **Datalek**; een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.

De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Tevens zal worden vastgelegd wie verantwoordelijk is voor de afhandeling van incidenten en het melden van datalekken bij de Autoriteit Persoonsgegevens en eventueel de betrokkenen. Alle beveiligingsincidenten worden vastgelegd in een incidentenregister.

De organisatie hecht er grote waarde aan dat van incidenten zal worden geleerd. Daarom zal er periodiek een evaluatie zijn van het incidentenregister. Hierbij zal gekeken worden naar (terugkerende) incidenten en trends. Op basis hiervan kunnen extra maatregelen worden genomen of bestaande maatregelen worden aangepast.

De organisatie zal bij het aangaan van verwerkersovereenkomsten ook altijd afspraken maken over de termijn en verantwoordelijkheid voor het melden van incidenten.

7 Rechten van betrokkenen

De organisatie neemt de rechten die betrokkenen hebben serieus en zal de organisatie en beveiliging van informatie dusdanig inrichten dat aan deze rechten gehoor kan worden gegeven. De primaire betrokkenen van een onderwijsinstelling zijn:

- De eigen medewerkers
- De leerlingen
- De ouders/verzorgers van leerlingen

De organisatie neemt maatregelen om de wettelijke rechten van deze betrokkenen te waarborgen. Deze rechten zijn:

1. Het recht op informatie. Het recht om (vooraf) geïnformeerd te worden over wat er aan gegevens wordt vastgelegd en met welk doel.
2. Het recht op inzage. Dat is het recht van mensen om de persoonsgegevens die worden verwerkt in te zien.
3. Het recht op rectificatie. Het recht om de persoonsgegevens die worden verwerkt te wijzigen.
4. Het recht op vergetelheid. Het recht om 'vergeten' te worden.
5. Het recht op beperking van een verwerking. Het recht om minder gegevens te laten verwerken.
6. Het recht op dataportabiliteit. Het recht om persoonsgegevens over te (laten) dragen.
7. Het recht op verzet (bezwaar). Het recht om bezwaar te maken tegen een verwerking.
8. Het recht op een menselijke blik bij (geautomatiseerde) besluiten. Bij profilering en geautomatiseerde besluitvorming kan een betrokkenen een menselijke blik eisen.

Betrokkenen zullen altijd actief op hun rechten worden gewezen door het vooraf informeren over deze rechten. De organisatie zal dit doen door het opstellen van een privacyverklaring toegespitst op de specifieke doelgroep.

De organisatie bepaald wie verantwoordelijk is voor het ontvangen en afhandelen van verzoeken van betrokkenen. Hierbij dienen de wettelijke voorwaarden in acht te worden genomen. Vuistregel hierbij is dat als een betrokkene een beroep doet op een van zijn rechten, de organisatie dat verzoek binnen één maand (kosteloos) moet afhandelen. Als dat niet lukt, mag deze maand (meerdere malen) verlengd worden tot maximaal drie maanden.

De organisatie richt verwerkingen dusdanig in dat het (technisch) mogelijk is om gehoor te geven aan deze rechten. Zo zullen systemen niet worden opgebouwd of ingericht op een wijze die inbreuk maakt op één of meer van deze rechten. Bijvoorbeeld doordat inzage in gegevens niet mogelijk is zonder het lekken van gegevens van derden of doordat gegevens niet kunnen worden verwijderd zonder tevens gegevens te verwijderen waarop een bewaartermijn rust die nog niet is verstreken.

8 Functionaris Gegevensbescherming

Op de organisatie rust de wettelijke verplichting om een Functionaris Gegevensbescherming (FG) aan te stellen. De organisatie draagt daarom zorg voor het aanstellen van een FG Hiervoor is in 2021 aangesteld: M. van der Stok.
Deze FG adviseert het bestuur over privacy en houdt toezicht daarop, handelt vragen en klachten over privacy af, ontwikkelt (mede) regelingen rondom privacy en geeft advies over technologie en beveiliging.

De FG heeft de bevoegdheid om in systemen te kijken, verwerkingen te toetsen en gedrag te controleren. De FG heeft geen formele sanctiebevoegdheden.

De FG zal tijdig en adequaat worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens binnen de organisatie. De FG is daarnaast het eerste aanspreekpunt voor de betrokkenen indien zij vragen of klachten hebben over privacy of hun Privacy rechten. Ook intern is de FG het eerste aanspreekpunt voor zaken rondom privacy.

9 Rollen en verantwoordelijkheden

Om informatiebeveiliging en privacy binnen de organisatie handen en voeten te geven is het van belang de verantwoordelijkheden hieromtrent eenduidig toe te kennen en de rollen te verdelen. Binnen de organisatie zijn de rollen en verantwoordelijkheden toegekend die in onderstaand schema worden toegelicht.

Niveau	Rollen	Verantwoordelijkheid / taken
Richtinggevend strategisch	Voorbeelden: Bestuur CvB Directeur	• Eindverantwoordelijk • Beleidsvorming, vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens. • Evalueren toepassing en werking van het beleid op basis van rapportages. • Organisatie van privacy en informatiebeveiliging inrichten.
Sturend tactisch	Voorbeelden: Verantwoorde-lijke Informatiebeveiliging informatiemana-ger privacy officer	• Inhoudelijk verantwoordelijk voor uitwerking beleid en uitwerking ervan naar specifiek (onderliggend) beleid. • Planning en controle van informatiebeveiliging. • Adviseren bestuur/CvB/directie over informatiebeveiliging. • Evalueren van het beleid en hierover rapporteren. • Schrijven, implementeren en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen.
	Functionaris voor Gegevensbescherming en/of Privacy officer	• 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.
	ICT	• Digitaal toegangsbeleid vaststellen en laten goedkeuren door bestuur/CvB/directie. • Borgen en er op 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. • Bepalen en implementeren van technische beveiligingsmaatregelen. • Afhandeling van technische beveiligingsincidenten. (i.c.m. de FG)

	Facilitair	• Fysiek toegangsbeleid vaststellen en laten goedkeuren door bestuur/CvB/directie. • Faciliteren van toegang en fysieke beveiliging.
	Financiën en administratie	Beheer voeren op bewaartermijnen van de administratie. Inrichten van de administratieve processen conform het vastgestelde beleid. (Laten) tekenen van verwerkersovereenkomsten en het beheer hierop.
	HRM	Beheer voeren op bewaartermijnen van de personeelsdossiers. Informeren en bewust maken van nieuw personeel.
	Leidinggevenden	Uitdragen van een voorbeeldfunctie. Controle op naleving van vastgesteld beleid. Zorgdragen voor continue bewustzijn.
- Uitvoerend operatio neel)	Overige medewerkers	Naleving van het vastgestelde beleid. Collega's aanspreken op ongewenst gedrag. Het actief en tijdig melden van incidenten.

Bijlage 1: Toepasselijke wet- en regelgeving

Binnen het onderwijs is veel wet en regelgeving van toepassing. Diverse wetten stellen specifieke eisen, rechten en kaders aan informatiebeveiliging of privacy. Deze wet en regelgeving bepalen dan ook mede de inhoud van dit beleid. Hieronder wordt de belangrijkste wet en regelgeving toegelicht.

Algemene Verordening Gegevensbescherming
De organisatie heeft de vereisten met betrekking tot persoonsgegevens op basis van de basisprincipes uit de wet geïmplementeerd via het beleid.

Wet op het primair onderwijs
Deze wet stelt o.a. eisen aan welke gegevens van leerlingen en ouders dienen te worden verwerkt. Aangezien het hier wettelijke verplichtingen betreft vormt deze wet een belangrijke grondslag voor gegevensverwerking binnen het onderwijs.

Wet passend onderwijs
Organisaties binnen het onderwijs hebben (bijzondere) persoonsgegevens van leerlingen nodig om de juiste begeleiding en eventuele doorverwijzing naar het speciaal onderwijs te faciliteren.

Wet onderwijstoezicht
De Wet op het onderwijstoezicht regelt de manier waarop in Nederland toezicht wordt gehouden op de kwaliteit van het onderwijs. Deze wet heeft raakvlakken met het zorgvuldig registreren en bewaren van gegevens.

Archiefwet
De organisatie houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d.

Leerplichtwet
De organisatie houdt zich aan de wettelijke vereisten die vanuit de Leerplichtwet aan haar worden gesteld. Hierbij geldt vooral de verplichting om inzicht te kunnen geven in aan/afwezigheid van leerlingen. De wijze waarop dergelijke gegevens worden gedeeld is onderhavig aan de eisen uit de AVG.

Wetboek van Strafrecht
In het Wetboek van Strafrecht zijn de laatste decennia een aantal specifieke bepalingen opgenomen over de strafrechtelijke probleemgebieden in relatie tot het computergebruik. De wet schrijft voor dat “enige beveiliging” vereist is alvorens er sprake kan zijn van het eventueel strafrechtelijk vervolgen van delicten jegens de onderwijsinstelling en het eventueel vrijwaren van bestuurders van de instelling. Naleving van dit informatiebeveiligingsbeleid en implementatie van de basismaatregelen binnen de organisatie moet leiden tot een niveau van beveiliging dat als voldoende mag worden gezien in het kader van het Wetboek van Strafrecht.

Bijlage 2: Minimale organisatorische en technische maatregelen

Verplichte documentatie
De organisatie werkt dit beleid minimaal verder uit in de volgende procedures en documenten.

1. Verwerkingsregister
2. Protocol beveiligingsincidenten en datalekken
3. Register datalekken
4. Privacy verklaringen

Organisatorische uitwerking van het beleid
De organisatie stelt de implementatie van de volgende organisatorische maatregelen verplicht.

1. Voorlichting en bewustzijn
De mens is de belangrijkste factor bij het borgen van privacy. 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 regelmatig terugkerende bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Daarnaast wordt tijdens functioneringsgesprekken en teamvergaderingen aandacht besteed aan privacy.

2. Goed sleutelbeheer en sleutelplan tot fysieke gebouwen en objecten.
De toegang tot gebouwen van de organisatie alsmede toegang tot kasten e.d. wordt gedaan op basis van een sleutelplan. Er is iemand verantwoordelijk voor het beheer van sleutels en de uitgifte en inname ervan. Er is nooit sprake van zwervende onbeheerde sleutels of open sleutelkastjes. Vast onderdeel hiervan is dat standaard de deuren van schoolgebouwen altijd gesloten zijn.

3. Geheimhoudingsverklaring
Al het personeel in dienst van de organisatie alsmede ingeschakelde vrijwilligers dienen een geheimhoudingsverklaring te tekenen.

4. Gedragscode
De organisatie stelt een bedrijfsbrede gedragscode op. Hierin zal aandacht worden besteed aan de omgang met (bedrijfs)apparatuur, informatie, social media, etc. Disciplinaire maatregelen zullen tevens onderdeel uit maken van de gedragscode.

5. Standaard indeling klassenmap
Er wordt (per school) een standaard indeling van de klassenmap bepaald. Buiten deze gegevens dient er geen informatie aanwezig te zijn in de mappen.

6. Bewaartermijnen
Voor alle domeinen worden voor de diverse categorieën van persoonsgegevens bewaartermijnen bepaald. Dit zal op zijn minst gebeuren voor leerling dossiers en personeelsdossiers.

7. Toestemming
Bij de aanmelding van een leerling zal standaard toestemming worden gevraagd voor de verwerkingen van beeld en fotomateriaal. Deze toestemming zal onderdeel uitmaken van het aanmeldingsformulier waarvoor een (dwingend) format ter beschikking zal worden gesteld.

8. Screening personeel
Er wordt beleid opgesteld voor het screenen van nieuw personeel. Hiervan worden minimaal onderdeel gemaakt de VOG, referenties en een diplomacheck.

9. Monitoring dienstverlening
Uitbestede (ICT) dienstverlening wordt periodiek gemonitord, beoordeeld en/of ge-audit aan de hand van de overeenkomsten en/of SLA's.

Technische uitwerking van het beleid
De organisatie stelt de implementatie van de volgende technische maatregelen verplicht.

1. Rechten leerlingvolgsysteem
Voor het leerlingvolgsysteem zal een autorisatiematrix worden opgesteld. Hierbij wordt op basis van functie en noodzaak toegang verleend tot leerling dossiers. Uitgangpunt hierbij is dat medewerkers alleen toegang krijgen tot dossier van leerlingen die zij actief begeleiden of onderwijzen. Beheerdersrechten zullen altijd tot een minimum worden beperkt.

2. Twee factor authenticatie
Bij het gebruik van het leerlingvolgsysteem zal altijd toegang worden verkregen op basis van 2 factor authenticatie.

3. Rechten informatiesystemen
Voor overige informatiesystemen zal een autorisatiematrix worden opgesteld. De rechten tot informatie zal hierin worden bepaald op basis van de functie of rol van een persoon. Tevens zal er iemand verantwoordelijk worden gemaakt voor het periodiek beoordelen van rechten en de intrekking hiervan (uiterlijk) op de laatste dag van het dienstverband. Beheerdersrechten zullen altijd tot een minimum worden beperkt.

4. Beveiligd printen
Printen van persoonsgegevens zal altijd gebeuren op basis van een unieke identificatiecode.

5. Wachtwoordbeleid
Voor wachtwoorden geldt dat de lengte en complexiteit ervan in het leerlingvolgsysteem en overige informatiesystemen technisch zullen worden afgedwongen. Tevens zal het periodiek wijzigen van wachtwoorden worden afgedwongen. Het gebruik van groepsaccounts is hierbij verboden.

6. Automatische vergrendeling
Alle PC's en laptops zullen zo worden ingesteld dat het beeldscherm na 5 minuten inactiviteit automatisch wordt vergrendeld.

7. Logging en monitoring
Logging en monitoring door de IT-afdeling 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. Onderdeel hiervan zal tevens zijn dat er gekozen wordt voor één tijdstandaard waarop alle (IT) systemen opereren.

8. Uit gebruik nemen apparatuur
Apparatuur die niet langer gebruikt wordt (waar onder laptops, desktops, servers en overige gegevensdragers) zullen professioneel worden vernietigd en nooit bij het grof vuil worden geplaatst.

9. Malware
Op systemen waarop persoonsgegevens worden verwerkt zal altijd anti malware software aanwezig zijn. Hierbij wordt geen gebruik gemaakt van gratis pakketten.

10. back ups
Van informatiesystemen waarin zich persoonsgegevens bevinden wordt minimaal dagelijks een backup gemaakt. Waar noodzakelijk zal hier in verwerkersovereenkomsten aandacht aan worden besteed.