Privacyreglement

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. 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 ICTsystemen 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 leggen en vast te stellen. Hiermee vormt het beleid de leidraad voor alle betrokkenen bij informatiebeveiliging en privacy, en dient het als spiegel bij de invoering van 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 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 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. De stichting voldoet aan alle relevante wet- en regelgeving. In het bijzonder geldt hier de algemene verordening persoonsgegevens. (Zie verder bijlage 1)
3. De Stichting legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden.
4. Bij de Stichting 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. De Stichting 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 de Stichting 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. De stichting sluit met alle partijen die namens haar persoonsgegevens verwerken verwerkersovereenkomsten af.

9. De stichting 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. De stichting 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. Indien de (nieuwe) verwerking een potentieel hoog risico voor persoonsgegevens oplevert zal de organisatie een DPIA (Data Protection Impact Assessment) 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 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.

6 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.

7 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. 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.