Het Sticht

Stichting voor katholiek en algemeen bijzonder primair onderwijs

Informatiebeveiligings- en privacy beleid

januari 2018

INHOUD

BIJLAGEN

1.Inleiding

Informatie en ict zijn noodzakelijk in de ondersteuning van het onderwijs. Omdat we met persoonsgegevens (van onszelf, leerlingen en anderen) werken, is privacywetgeving daarop van toepassing.

De informatie en ICT van Het Sticht worden blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Alle informatie die we bewaren en verwerken kan worden bedreigd door een aanval, een vergissing, de natuur (bijv. overstroming of brand), et cetera. Het niet beschikbaar zijn van ICT, incorrecte administraties en het uitlekken van gegevens kan leiden tot inbreuken op het geven van onderwijs en het vertrouwen op onze scholen.

Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's die gepaard gaan met deze bedreigingen tot een aanvaardbaar niveau te reduceren. Om dit structureel op te pakken is het noodzakelijk dat we iedereen duidelijk maken waar het om gaat, een doel stellen en de manier waarop we dit doel willen bereiken. In dit beleidsdocument kunt u lezen op welke wijze Het Sticht hieraan invulling geeft.

De linken in bijlage 5 verwijzen naar documenten die relevant zijn m.b.t. het gevoerde privacybeleid en zijn derhalve aanvullend.

Met dit geformuleerde beleid werken we binnen de kaders van de nieuwe Europese Algemene Verordening Gegevensbescherming (AVG)

Zeist, januari 2018
CVB Het Sticht
K.Timmers

1.1 Informatiebeveiliging en privacy

Informatiebeveiliging is een proces voor het beschermen van Het Sticht tegen risico's en bedreigingen met betrekking tot informatie en ict. Het richt zich op drie aspecten:

- 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).

2.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.

Dit beleid is een leidraad voor iedereen die betrokken is bij IBP binnen Het Sticht. Het is van toepassing op onze eigen medewerkers, tijdelijk personeel en andere personen die een rol spelen in Het Sticht. Het is van toepassing op de hele organisatie van Het Sticht, waaronder de fysieke locaties, systemen op interne en externe locaties en gegevensverzamelingen die gebruikt worden.
Daarnaast kan het gezien worden als communicatieinstrument voor zowel interne als externe belanghebbenden.

Het informatiebeveiligings- en privacybeleid heeft raakvlak met andere beleidsgebieden, te weten:

- Algemeen veiligheids- en beveiligingsbeleid; met als aandachtsgebieden bedrijfshulpverlening, fysieke toegang en –beveiliging, crisismanagement, huisvesting en ongevallen;
- IT-beleid; met als aandachtsgebieden de aanschaf en het beheer van ict;
- Personeels- en organisatiebeleid; met als aandachtsgebieden in- en uitstroom van medewerkers, functiescheiding en vertrouwensfuncties;

Dit beleid maakt duidelijk waar de verantwoordelijkheden rondom informatiebeveiliging en privacy zijn belegd.

3.Uitgangspunten

De belangrijkste beleidsuitgangspunten bij Het Sticht zijn:

- Informatiebeveiliging en het privacybeleid dient te voldoen aan alle relevante wet- en regelgeving. Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveilingsnormen.
- 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 m.b.t. informatiebeveiliging en privacybeleid zorgvuldig omgaan met wet- en regelgeving; ieder met een eigen verantwoordelijkheid.
- Het Sticht is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt gebruikt.
- Het Sticht 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.
- Er is een balans tussen privacy, functionaliteit/werkbaarheid en veiligheid.

Het Sticht 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 worden 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.

3.1 Rechten

Algemeen doel van de verwerking
Wij gebruiken uw gegevens uitsluitend ten behoeve van ons onderwijs. Dat wil zeggen dat het doel van de verwerking altijd direct verband houdt met de opdracht die wij in het kader van ons onderwijs hebben. Als u gegevens met ons deelt en wij gebruiken deze gegevens om andere redenen dan genoemd in het overzicht, vragen wij u hiervoor expliciet toestemming. Uw gegevens worden niet met derden gedeeld, anders dan om aan boekhoudkundige en overige administratieve verplichtingen te kunnen voldoen. Deze derden zijn allemaal tot geheimhouding gehouden op grond van de overeenkomst tussen hen en ons of een eed of wettelijke verplichting.

Relevante begeleidingsinformatie wordt binnen de betreffende afdeling gedeeld met medewerkers die te maken hebben of kunnen krijgen met de leerling in het primaire proces. Denk hierin aan pleindiensten, escalaties, busdiensten, etc.

De persoonsgegevens die Het Sticht registreert over leerlingen, ouder/verzorgers en medewerkers, welke functionarissen daar toegang toe hebben, op welke wijze gegevens opgeslagen worden en welke bewaartermijnen worden gehanteerd, zijn respectievelijk beschreven in bijlagen 2, 3 en 4.

Het Sticht kent op basis van de wetgeving de volgende rechten toe:

Inzagerecht
U heeft altijd het recht om de gegevens die wij (laten) verwerken en die betrekking hebben op uw persoon of de persoon onder uw gezag of daartoe herleidbaar zijn, in te zien. U kunt een verzoek met die strekking doen aan onze contactpersoon voor privacy aken.

Rectificatierecht
U heeft altijd het recht om de gegevens die wij (laten) verwerken en die betrekking hebben op uw persoon of de persoon onder uw gezag, of daartoe herleidbaar zijn, te laten aanpassen. U kunt een verzoek met die strekking doen aan onze contactpersoon voor privacy-zaken. U ontvangt dan binnen 30 dagen een reactie op uw verzoek. Als uw verzoek wordt ingewilligd, sturen wij u op het bij ons bekende e-mailadres een bevestiging dat de gegevens zijn aangepast.

Recht op beperking van de verwerking
U heeft altijd het recht om de gegevens die wij (laten) verwerken die betrekking hebben op uw persoon of de persoon onder uw gezag, of daartoe herleidbaar zijn, te beperken. U kunt een verzoek met die strekking doen aan onze contactpersoon voor privacy-zaken. U ontvangt dan binnen 30 dagen een reactie op uw verzoek. Als uw verzoek wordt ingewilligd sturen wij u op het bij ons bekende emailadres een bevestiging dat de gegevens tot u de beperking opheft niet langer worden verwerkt.

Recht op overdraagbaarheid
U heeft altijd het recht om de gegevens die wij (laten) verwerken en die betrekking hebben op uw persoon of de persoon onder uw gezag, of daartoe herleidbaar zijn, door een andere partij te laten uitvoeren. U kunt een verzoek met die strekking doen aan onze contactpersoon voor privacy-zaken. U ontvangt dan binnen 30 dagen een reactie op uw verzoek. Als uw verzoek wordt ingewilligd, kunt u afschriften of kopieën van alle gegevens over u die wij

hebben verwerkt of in opdracht van ons door andere verwerkers of derden zijn verwerkt ophalen op afspraak. Naar alle waarschijnlijkheid kunnen wij in een dergelijk geval de dienstverlening niet langer voortzetten, omdat de veilige koppeling van databestanden dan niet langer kan worden gegarandeerd.

Recht van bezwaar en overige rechten
U heeft in voorkomende gevallen het recht bezwaar te maken tegen de verwerking van uw of de persoon onder uw gezag, persoonsgegevens door, of in opdracht van, Het Sticht. Als u bezwaar maakt, zullen wij onmiddellijk de gegevensverwerking staken in afwachting van de afhandeling van uw bezwaar. Is uw bezwaar gegrond dan zullen wij afschriften en/of kopieën van gegevens die wij (laten) verwerken aan u ter beschikking stellen en daarna de verwerking blijvend staken. U heeft bovendien het recht om niet aan geautomatiseerde individuele besluitvorming of profilering te worden onderworpen. Wij verwerken uw gegevens niet op zodanige wijze dat dit recht van toepassing is. Bent u van mening dat dit wel zo is, neemt u dan contact op met Het Sticht, door een mail te sturen naar info@hetsticht.nl

4.Wet- en regelgeving

Het Sticht 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 3.0’ leidend bij het maken van afspraken met leveranciers.

5.Taken, verantwoordelijkheden en bevoegdheden

Dit hoofdstuk beschrijft hoe de taken, verantwoordelijkheden en bevoegdheden met betrekking tot IBP binnen Het Sticht zijn belegd. We onderscheiden drie niveaus te weten:

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

5.1 Richtinggevend

Eindverantwoordelijke
Het College van Bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de maatregelen vast op het gebied van informatiebeveiliging en privacy. De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages (één keer per jaar) door hen geëvalueerd. De rapportage bevat o.a. een beschrijving van de actuele stand van zaken m.b.t. informatiebeveiliging en privacy en mogelijke incidenten. Binnen het CvB is de voorzitter van het CvB verantwoordelijk voor IBP. Over de rapportages wordt verantwoording afgelegd aan de RvT.

5.2 Sturend

Manager IBP

Deze geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen aan op de uitvoerende laag. De manager IBP moet:

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

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) houdt binnen Het Sticht toezicht op de toepassing en naleving van de privacy-wetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. Deze taken en bevoegdheden zijn vastgelegd in de functieomschrijving FG van Het Sticht. De FG zorgt voor het afhandelen van -vertrouwelijke- informatiebeveiligingsincidenten. De FG is ook contactpersoon voor vragen van betrokkenen met een vertrouwelijk karakter en staat geregistreerd bij de Autoriteit Persoonsgegevens.

Domeinverantwoordelijkheid/proceseigenaar

Binnen de school zijn er verschillende domeinen/processen, zoals ict, personeel, administratie et cetera. De directeur van de school is verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

5.3 Uitvoerend

Leidinggevenden

Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende op de scholen van Het Sticht heeft op uitvoerend niveau de taak om:

- ervoor te zorgen dat medewerkers op de hoogte zijn van het beveiligingsbeleid;
- toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle personeel gerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de manager IBP.
Leidinggevenden hebben een voorbeeldrol ten opzichte van hun medewerkers.

Medewerkers

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.
Aan medewerkers wordt gevraagd actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de MR)

Security Officer
De Security Officer vormt een technisch aanspreekpunt voor incidenten en informatiebeveiliging. De bovenschools coördinator ICT-zaken voert de taak van Security Officer bij Het Sticht uit.

6.Uitvoering

Email
De Stichting heeft passende technische en organisatorische maatregelen getroffen om misbruik, verlies e.d. van uw en onze gegevens zoveel mogelijk te voorkomen. Wij maken voor ons reguliere zakelijke e-mailverkeer uitsluitend gebruik van het Office 365 (werk)account in de beveiligde omgeving van Sharepoint. Externen hebben geen toegang tot ons domein. Relevante persoonsinformatie staat op beveiligde servers van Het Sticht. Alle betrokkenen gaan zorgvuldig om met de inloginformatie. Privacy gevoelige informatie wordt vertrouwelijk verstuurd.

Social media
Naast email zijn er nog andere social media beschikbaar. Denk aan Whatsapp, Facebook, Twitter en Instagram. Ook het gebruik van deze middelen vraagt om zorgvuldigheid van de medewerkers van Het Sticht wat betreft de privacy. Het Sticht hanteert daartoe een zgn. social mediaprotocol (opgenomen in het Sociaal Veiligheidsplan) waaraan een ieder zich committeert in relatie tot professionele activiteiten.

Leerlingvolgsysteem
We maken gebruik van de diensten van o.a. ParnasSys en CITO om de administratie rondom onze leerlingen en onderwijs vorm te geven. Met deze aanbieders hebben we een zgn. bewerkersovereenkomst afgesloten. Persoonsgegevens die u ten behoeve van onze dienstverlening ter beschikking stelt, worden met deze partij(en) gedeeld. Zij hebben toegang tot uw gegevens om ons (technische) ondersteuning te bieden. Zij zullen uw gegevens nooit gebruiken voor een ander doel. Op basis van de overeenkomst die wij met hen gesloten hebben, zijn ze verplicht om passende beveiligingsmaatrgelen te nemen.

Verwerkersovereenkomsten: leermiddelen en onderwijsdiensten
Om ons onderwijs vorm te geven maken we gebruik van leermiddelen en onderwijsdiensten zoals o.a. Malmberg, Noordhoff, Zwijssen, Rolf Groep, Dedicon, CITO, Apsit diensten, CED, schoolfotograaf enz. Ook met dergelijke aanbieders zijn/worden verwerkersovereenkomsten afgesloten. Persoonsgegevens die u ten behoeve van onze dienstverlening aan ons beschikbaar stelt , worden met deze partij(-en) gedeeld. Deze partijen hebben toegang tot uw gegevens om ons (technische) ondersteuning te bieden; zij zullen uw gegevens nooit gebruiken voor een ander doel. Op basis van de overeenkomst die wij met hen hebben gesloten zijn ze verplicht om passende beveiligingsmaatregelen te nemen. De verwerkersovereenkomsten worden centraal afgesloten en bewaard.

ECK-ID
Het ECK-ID staat voor Educatieve Contentketen Identity. Voor het gebruik van digitaal lesmateriaal werken de systemen van scholen en aanbieders van lesmateriaal met elkaar samen. Het ECK-ID verbindt gebruikers en licenties van digitaal lesma-

teriaal betrouwbaar en bestendig met elkaar op basis van zo min mogelijk persoonsgegevens. Hieraan hebben de leveranciers die het ECK-ID hanteren zich gecommitteerd via het Privacy convenant onderwijs 3.0. Het ECK-ID fungeert als unieke, maar anonieme sleutel in de geautomatiseerde processen tussen de school en lesmethodes bij uitgeverijen. Het ECK-ID wordt niet getoond in beeldschermen; het is een lange string van karakters die voor het menselijk oog bovendien geen betekenis heeft.
Het ECK-ID bevordert de privacybescherming van leerlingen in het PO. Met het ECK-ID wordt de basis gelegd om als school minder persoonsgegevens te verstrekken aan leveranciers, terwijl toch de leerling bestendig wordt verbonden aan de licenties die hij gebruikt. De privacybescherming neemt ook toe doordat het ECK-ID een versleuteld pseudoniem is van het persoonsgebonden nummer met een eigen wettelijke basis. Gegevens die de school verstrekt voor het gebruik van digitaal lesmateriaal worden uitsluitend voor dat doel gebruikt. Voor meer informatie zie: http://info.basispoort.nl/Privacy-AVG-GDPR/ECK-ID-Primair-Onderwijs

Archivering en bewaartermijnen
Gegevens worden niet langer bewaard dan de wettelijke kaders toestaan. Zie hiervoor bijlagen 2,3 en 4.

Overheid en onderwijs
Als onderwijsinstelling zijn wij verplicht om informatie te delen van Bron en DUO. Dit zijn de administratieve en bekostigingsvoorzieningen Van de het ministerie van OCW, die toezicht houden op financiering en leerplicht van alle leerplichtigen in Nederland. Wij delen enkel de verplichte zaken met hen. Deze overheidsinstellingen voldoen aan de privacywetgeving en stellen alles in het werk om de gegevens en systemen te beveiligen.

Toestemming van ouders/verzorgers/leerlingen
Voorafgaand aan het verwerken van persoonsgegevens vragen de scholen toestemming van de desbetreffende persoon of van ouders/verzorgers als de leerling jonger is dan 16 jaar. Bij nieuwe leerlingen vragen de scholen ouders toestemming bij de aanmelding. Mocht er geen toestemming worden verleend, dan heeft dit vergaande gevolgen voor het onderwijs en ondersteuning welke onze scholen kunnen bieden aan de leerling. Een toestemmingsverklaring kan te allen tijde worden ingetrokken.

Toestemming van medewerkers/stagiaires/vrijwilligers
Ook bij deze personen vragen wij toestemming tot verwerking van persoonsgegevens en om adresgegevens intern te mogen voor speciale gelegenheden. Denk hierbij o.a. een personeelslijst van de school. De toestemmingsverklaring kan te allen tijde worden ingetrokken.

Beeldmateriaal
Beeldmateriaal valt onder persoonsgegevens waarvoor uitdrukkelijk toestemming nodig is. Jaarlijks wordt op de scholen toestemming gevraagd betreffende de publicatie van foto's. Het moet daarbij duidelijk zijn waarvoor zij instemmen (specifiek doel). De wijze van toestemming vragen, wordt per school gerealiseerd.

Ook voor de schoolfotografie wordt specifiek toestemming gevraagd.

Concent
De administratie met betrekking tot onze medewerkers en financiën verwerken wij met behulp van het administratiekantoor Concent. Met deze aanbieder is een verwerkingsovereenkomst afgesloten. Persoonsgegevens van medewerkers worden met deze partij gedeeld. Concent heeft toegang tot deze gegevens om ons (technische) ondersteuning te bieden; zij zullen de gegevens nooit gebruiken voor andere doeleinden. Zij zijn verplicht passende veiligheidsmaatregelen te nemen.

MOO en Google
Om optimaal gebruik te kunnen maken van de Chromebooks, laten we onze leerlingen op de Chromebook inloggen via de omgeving Mijn Omgeving Online (MOO) van Heutink-ict, de bekende schoolomgeving voor onze schoolcomputers; deze is gekoppeld aan een leerlinggebonden Google-account waar een Google for Education-omgeving achter zit. De *Identity Provider* is in dit geval MOO, dus MOO bepaalt of een gebruiker wel of niet mag inloggen. Meer informatie over het privacy- en beveiligingsbeleid van Heutink-ict, is na te lezen op www.heutink-ict.nl/privacy.
Ook Google moet voldoen aan de AVG-wetgeving en wordt daar scherp op gemonitord. Verdere, uitgebreidere informatie over de producten van Google en de privacy en beveiliging hiervan, is na te lezen op www.google.com/edu/privacy.

Cameratoezicht
Om de veiligheid van onze leerlingen, medewerkers te vergroten, kan er op terreinen en bij gebouwen van Het Sticht gebruik worden gemaakt van cameratoezicht. Deze gegevens worden alleen geraadpleegd als zich een (vermoeden van) veiligheidsincident heeft voorgedaan. De beelden worden maximaal twee werkweken bewaard.

Bewustwording en voorlichting
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 belangrijke speler. Daarom wordt bij Het Sticht het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig, verantwoord gedrag wordt aangemoedigd. Verhoging van het veiligheidsbewustzijn is een verantwoordelijkheid van eenieder binnen Het Sticht. Onderdeel van het beleid zijn regelmatig terugkerende informatieve berichten voor medewerkers in Connect. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de Functionaris gegevensbescherming i.c.m. het College van Bestuur als eindverantwoordelijke.

Evaluatie beleid
Het Sticht evalueert in het kader van de risicoanalyse jaarlijks de vastgestelde protocollen Beveiligingsincidenten en datalekken en het Privacyreglement.

7.Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar geevalueerd, getoetst en bijgesteld. 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 Sticht een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een jaarlijks evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst en wordt vastgelegd.

Classificatie en risicoanalyse

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

Documentatieplicht

Omdat elke school regelmatig persoonsgegevens verwerkt, geldt voor alle scholen de documentatieplicht. Onder de documentatieplicht valt bijvoorbeeld het vullen van het dataregister. In de dataregisters wordt de registratie en verwerking van (persoons-)gegevens zichtbaar. Voor de Autoriteit Persoonsgegevens tevens van belang voor controle op de naleving van de AVG.

Incidenten en datalekken

Alle incidenten kunnen worden gemeld bij: datalekken@hetsticht.nl . De afhandeling van deze incidenten volgt een gestructureerd proces, die ook voorziet in de juiste stappen rondom de meldplicht datalekken. Dit proces is vastgelegd in de beleidsnotitie Beveilingsincidenten en datalekken.

Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij Het Sticht wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instellingsbrede gedragscode, met periodieke bewustwordingssessies, et cetera.
Voor de bevordering van de naleving van de AVG vervult de Functionaris gegevensbescherming een belangrijke rol. De aanstelling van deze functionaris geschiedt door het bestuur. De FG werkt aan de hand van een wettelijk omschreven taak en werkt onafhankelijk aan het toezicht.
Mocht de naleving ernstig tekort schieten, dan kan Het Sticht de betrokken verantwoordelijke medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden van de AVG.

Bijlage 1 IBP rollen en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend (strategisch)	CvB	• 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 FG vaststellen • Privacyreglement vaststellen
Sturend (tactisch)	Manager IBP	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert bestuur/CvB/directie over IBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse • Hanteren IBP normen en wijze van toetsen • Evalueren IBP-beleid en maatregelen • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze • Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen • **Classificatie / risicoanalyse** *(Informatiemanager / verantwoordelijke IBP / Security officer)* • Digitaal toegangsbeleid opstellen en laten goedkeuren door *bestuur/CvB/directie* • *Samen met functioneel beheer en ICT beheer* er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • *Samen met functioneel beheer en ICT* beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	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 • Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen Vanuit de Wiki
	Functionaris voor Gegevensbescherming / Privacy officer Externe vertrouwenspersonen Het Sticht	• Toezicht op naleving privacy wetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement, • procedure IBP-incident afhandeling • Inrichten meldpunt datalekken
Uitvoerend (operationeel)	Security officer Bovenschools ICT coördinator Functioneel beheerder (Schoolleider) Medewerker Dagelijkse leiding / leidinggevende / directie	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • Uitvoeren taken conform gegeven richtlijnen en procedures. • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • Communicatie naar alle betrokkenen; ervoor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur.	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 maken

Bijlage 2 Persoonsgegevens leerlingen

Leerling gegevens	Moment	Doel	Toegang	Opslag	Bewaard tijdens	Bewaartijd na
NAW gegevens	Instroom	Inschrijving Bron/DUO	Leerlingadministratie Diagnostiek Functioneel beheer Betrokken leerkrachten CVB	Leerlingvolgsystemen Dossier	Gehele schooltijd	5 jaar
Geboortedatum/plaats	idem	Inschrijving diplomering	idem	idem	idem	idem
Geboorteland	idem	Cumi financiering	idem	idem	idem	2 jaar
Namen ouders/verzorgers	idem	Inschrijving	idem	idem	idem	idem
Contactgegevens telefoon/emailadres	idem	Afstemming in primaire proces	idem	idem	idem	idem
Hulpverlening indien noodzakelijk voor primaire proces	idem	Voorwaarde voor bepaald aanbod	idem	idem	idem	verwijderd
Ouderlijk gezag	idem	Inschrijving Bron Verantwoording primair proces + afstemming	idem	idem	idem	2 jaar
BSN nummer	idem	Inschrijving Bron	Leerlingadministratie CVB	idem	idem	idem
Kopie identiteitsbewijs	idem	Cumi financiering Diploma	idem	idem	idem	maand
Onderwijskundig rapport schooldossier	idem	Vormgeven primair proces	Leerlingadministratie Diagnostiek Functioneel beheer Betrokken leerkrachten CVB	idem	idem	5 jaar
Verzuim vorige school/betrokkenheid leerplicht	idem	idem	idem	idem	idem	verwijderd
Betrokkenheid onderwijsconsulent	idem	idem	idem	idem	idem	idem
Diagnose/handelingsadviezen	idem	idem	idem	idem	idem	idem
Ondersteuningsbehoefte	idem	idem	idem	idem	idem	idem
Medicijngebruik onder schooltijd	idem	idem	idem	idem	zolang van toepassing	idem

Toelaatbaarheidsverklaring	idem	financiering	idem	idem	idem	3 jaar
Plan ontwikkelingsperspectief	Interne doorstroom	Verantwoording primair proces	idem	idem	idem	idem
Incidentenregistratie	idem	Vormgeven primaire proces	idem	idem	idem	verwijderd
Voortgang Cijfers Gespreksverslagen Portfolio Toetsen	idem	Vormgeven + verant-woording primair proces	idem	idem	idem	 2 jaar verwijderd verwijderd 2jaar
Verzuim	idem	Wet- en regelgeving	idem	idem	idem	5 jaar
Beeldmateriaal	idem	Bij toestemming Informeren primair pro-ces	openbaar	divers	idem	2 jaar
Onderwijskundig rapport	uitstroom	Vormgeven primair pro-ces	ontvangende school	Leerlingvolgsystemen dossier		2 jaar
Overige info	divers	divers	divers	divers	divers	divers

Samenvattend op **hoofdlijnen**:
* Alles wat is vastgelegd in het leerling administratiesysteem 5 jaar
* Alles wat betrekking heeft op financiën 7 jaar (let op subsidies)
* Overige gegevens 2 jaar en in het passend onderwijs 3 jaar.

Bijlage 3 Persoonsgegevens ouders/verzorgers

Gegevens ouders/verzorgers	Moment	Doel	Toegang	Opslag	Bewaartijd tijdens	Bewaartijd na
NAW gegevens	**Instroom**	**Inschrijving Bron/DUO**	Leerlingadministratie Diagnostiek Functioneel beheer Betrokken leerkrachten CVB	**Leerlingvolgsystemen** **Dossier**	**Gehele schooltijd**	**5 jaar**
Geboortedatum/plaats	idem	Inschrijving	idem	idem	idem	idem
Geboorteland	idem	Cumi financiering	idem	idem	idem	idem
Contactgegevens telefoon/emailadres	idem	Afstemming in primaire proces	idem	idem	idem	2 jaar
Kopie identiteitsbewijs bij cumi leerling	idem	Cumi financiering	idem	idem	idem	5 jaar

Bijlage 4 Persoonsgegevens medewerkers

Gegevens medewer-kers	Moment	Doel	Toegang	Opslag	Bewaard tijdens	Bewaard na
NAW gegevens	Instroom	Basisbenodigdheden	Afdeling HR	Concent Insite Dossier	Gehele contracttijd	5 jaar
Geboorteda-tum/plaats	idem	Belastingdienst Afdrachten	Afdeling HR Leidinggevende CVB	idem	idem	idem
Geboorteland	idem	Belastingdienst Afdrachten	idem	idem	idem	idem
Contactgegevens tele-foon/emailadres	idem	Basis benodigdheden	idem	idem	idem	2 jaar
Kopie identiteitsbe-wijs	idem	Wet- en regelgeving	Afdeling HR	idem	idem	5 jaar
Relevante diploma's	idem	idem	Afdeling HR Leidinggevende CVB	idem	idem	2 jaar
BSN nummer	idem	Belastingdienst Afdrachten	Afdeling HR	idem	idem	5 jaar
VOG	idem	Wet- en regelgeving	idem	idem	idem	2 jaar
Laatste loonstrook	idem	Inschaling	idem	idem	idem	verwijderd
Arbeidsverleden	idem	Inschaling Jubilea/gratificaties	idem	idem	idem	idem
Betaalgegevens	idem	Financiële afwikkeling werkzaamheden	Afdeling HR Afdeling financiën	idem	idem	5 jaar
Burgerlijke staat	idem	Pensioenopbouw	Afdeling HR	idem	idem	2 jaar
Loonheffingsformulie-ren	idem	Belastingdienst	Afdeling HR	idem	idem	idem
Nevenactiviteiten	idem	Belastingdienst	idem	idem	idem	idem
Loonbeslag	idem	Financiële afwikkeling werkzaamheden	Afdeling HR CVB	idem	idem	idem
Gesprekkencyclus	Doorstroom	Monitoren functioneren	Afdeling HR Leidinggevende CVB	idem	idem	verwijderd
Berisping/schorsing	idem	idem	idem	idem	2 jaar	idem

Functioneringstrajec-ten	idem	idem	idem	idem	2 jaar	idem
Klachten	idem	idem	idem	idem	2 jaar	idem
Verzuim	idem	idem	Idem + Arbo	idem	Gehele contracttijd	idem
Referentie op aan-vraag medewerker	Uitstroom		Leidinggevende	idem	idem	n.t.b.
Verslag exit gesprek	idem	Evaluatie werkgever-schap	Afdeling HR Leidinggevende CVB	idem	Bij vertrek	2 jaar

Bijlage 5 Verwijzingen

1. **Onderstaande documenten vindt u op https://www.hetsticht.nl/Privacy**

- **Privacyverklaring**
- **Privacyreglement**
- **Gedragsprotocol**
- **Protocol Beveiligingsincidenten en datalekken**
- **Sociaal veiligheidsplan**