Het Sticht

Stichting voor katholiek en algemeen bijzonder primair onderwijs

Informatiebeveiligings- en privacybeleid

“Stilstaan bij je handelen is vooruitgang”

Bron
Kennisnet

Bewerkt door:
Het Sticht

Versie		Datum	Auteur	Omschrijving
2022		Januari 2022	Kees Francino	Functionaris Gegevensbescherming

Vastgesteld door Het Sticht:

Versie	Datum	Naam	Functie
2	Januari 2022	Simone Scholten Marleen Remmers	Leden CvB

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. Sinds mei 2018 is de AVG [Algemene Verordening Gegevensbescherming] van kracht**.**

De informatie en ICT van Het Sticht worden blootgesteld aan een aantal bedreigingen, al dan niet opzettelijk van aard. Alle informatie die we bewaren en verwerken kan ongewenst toegankelijk worden door een aanval (bv. ransomware), 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, op privacy en het vertrouwen op onze scholen.

Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's tot een aanvaardbaar niveau te reduceren. Om dit structureel aan 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.

Met dit geformuleerde beleid werken we binnen de kaders van AVG. Deze 2e versie betreft een update van het 1e Beleidsplan IBP uitgave januari 2020.

Zeist, januari 2022

CvB Het Sticht

INHOUDSOPGAVE

1.Het belang van informatiebeveiliging en privacy

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT. Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van informatiebeveiliging en privacy [afgekort tot IBP] in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

2.Toelichting informatiebeveiliging en privacy

2.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het nemen en onderhouden van een hoeveelheid samenhangende maatregelen zodat de betrouwbaarheid van de informatievoorziening gegarandeerd kan worden. Informatiebeveiliging richt zich op de volgende aspecten:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

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

2.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens moeten beschermd worden volgens de huidige wet- en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens verwerkt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die een natuurlijke persoon direct of indirect kunnen identificeren. Onder verwerking wordt elke handeling met betrekking tot persoonsgegevens verstaan. De wet noemt als voorbeelden van verwerking:

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.

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 ook van elkaar afhankelijk en worden daarom samengevoegd tot één proces: IBP. Dit beleid, verder te benoemen als IBP-beleid, vormt de basis op informatiebeveiliging en privacy binnen Het Sticht, te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

3. Doel en reikwijdte

3.1 Doel

Informatiebeveiliging en privacy heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan Het Sticht persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

Het informatiebeveiligings- en privacy beleid [IBP-beleid] is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een juiste balans moet zijn tussen privacy, functionaliteit en veiligheid. Het uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene [o.a. medewerkers, leerlingen en hun ouders/verzorgers] wordt gerespecteerd en Het Sticht voldoet aan relevante wet- en regelgeving.

3.2 Reikwijdte

- Het IBP-beleid binnen Het Sticht geldt voor alle medewerkers, leerlingen, ouders/verzorgers, [geregistreerde] bezoekers en externe relaties [inhuur/outsourcing]. Onder dit beleid vallen ook alle devices vanwaar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.

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

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van Het Sticht. 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 overige social media.]

- Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van Het Sticht evenals daaraan ten grondslag liggende documenten die in een bestand zijn

opgenomen.
- Het IBP-beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Het IBP-beleid heeft binnen Het Sticht raakvlakken met:

- *Algemeen veiligheids- en toegangsbeveiligingsbeleid;* met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting
- *Personeels- en organisatiebeleid;* met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
- *IT-beleid*; met als aandachtspunten aanschaf, beheer en gebruik van ICT en [digitale] leermiddelen
- *Medezeggenschap* van leerlingen, hun ouders/verzorgers en medewerkers
- *Sociaal veiligheidsplan*

4. Beleid – Hoe doen we dat?

Het Sticht hanteert de volgende uitgangspunten om de gestelde doelen van informatiebeveiliging en privacy te bereiken:

1. Het bestuur van Het Sticht 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. Het Sticht voldoet aan alle relevante wet- en regelgeving.

3. Bij Het Sticht is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen. Een goede balans tussen het belang van Het Sticht om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot het gebruik van zijn/haar persoonsgegevens is essentieel. Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming herzien.

4. Het Sticht zal alle betrokkenen helder en actief informeren over de verwerkingen van hun persoonsgegevens, die zowel direct als indirect zijn verkregen. 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 hiervoor de Privacyverklaring en het Privacyreglement.

5. Het Sticht legt alle verwerkingen van persoonsgegevens vast in een dataregister en zal deze up-to-date houden. Het Sticht voldoet hiermee aan de documentatieplicht.

6. Binnen Het Sticht 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. Er wordt continu aandacht besteed aan bewustwording bij het dagelijks handelen.

7. Het Sticht is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom [auteursrecht] toebehoort aan derden. Medewerkers en leerlingen worden waar noodzakelijk goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. Het Sticht classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen maatregelen. Er is een balans tussen de risico's die we willen afdekken en de benodigde investeringen en de te nemen maatregelen.

9. Het Sticht sluit met alle leveranciers van digitale onderwijsmiddelen [zowel van educatieve als bedrijfsapplicaties] verwerkersovereenkomsten af als zij, in opdracht van de school, persoonsgegevens verwerken. Dit geldt ook voor andere organisaties indien er gegevens van leerlingen of medewerkers worden verstrekt.

10. Het Sticht 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. Het Sticht heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd.

11. Informatiebeveiliging en privacy is bij Het Sticht een continu proces, waarbij minimaal 4-jaarlijks wordt geëvalueerd en wordt gekeken of aanpassing gewenst is. Er blijft altijd een mogelijkheid om het beleid tussentijds aan te passen als de omstandigheden dat vragen.

12. Het Sticht 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. Dit gebeurt m.b.v. een Data Protection Impact Assessment [DPIA].

13. Het Sticht neemt passende technische [beveiligings-]maatregelen om persoonsgegevens en overige data te beschermen tegen de risico's, die de voortgang van het onderwijs, de privacy en de bedrijfsvoering kunnen verstoren.
    Als de infrastructuur elders wordt beheerd en/of gegevens elders worden verwerkt legt Het Sticht aanvullende afspraken vast – bv. in een verwerkersovereenkomst- over de technische maatregelen.

14. Het Sticht zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en eventueel aan de betrokkenen als de omstandigheden daarom vragen.

5. Uitwerking van het beleid – Wat doen we?

Dit hoofdstuk geeft een praktische invulling van bovenstaande beleidspunten en is daarmee de minimale invulling van het beleid.

5.1 Relevante wet- en regelgeving

De uitwerking van het beleid voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet goed onderwijs en goed bestuur PO/VO
- Wet onderwijstoezicht
- Wet bescherming persoonsgegevens [Wbp; tot 25 mei 2018]
- Algemene Verordening Gegevensbescherming [AVG; vanaf 25 mei 2018]
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

De internationale norm voor informatiebeveiliging NEN-ISO/IEC 27001 en 27002 [2015] is leidend voor de te nemen beveiligingsmaatregelen.
De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerken [verwerkersovereenkomsten].

5.2 Basisregels bij het omgaan met persoonsgegevens

Bij het verwerken van persoonsgegevens zijn de wettelijke beginselen inzake verwerking persoonsgegevens [art.5 AVG] leidend. Deze zijn samengevat in de vijf vuistregels met betrekking tot de omgang met persoonsgegevens te weten:

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 manier die onverenigbaar is met de doelen waarvoor ze zijn verkregen.

2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de zes 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 betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Tevens 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.

5.3 Ondersteunende richtlijnen en procedures

Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen geven invulling aan de uitwerking van het beleid. Bijlage 1 geeft een overzicht van de diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen. Daarnaast worden alle verwerkingen van persoonsgegevens vastgelegd en up-to-date gehouden in een dataregister.

5.4 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hier een belangrijke factor. 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 de regelmatig terugkerende bewustwordingsmomenten voor medewerkers, leerlingen en ouders. Verhoging van het IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de verantwoordelijke IBP, de FG, en de Security Officer met het bestuur als eindverantwoordelijke.

5.5 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Het niveau van de te nemen 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. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de betrouwbaarheidsaspecten die van belang zijn.
Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe [informatie-)], wordt vóóraf gekeken naar de impact van de ontwikkelingen en de beoogde verwerkingen op informatiebeveiliging en privacy, zodat passende maatregelen genomen kunnen worden. Vanaf de start van nieuwe [ICT-] projecten wordt rekening gehouden met informatiebeveiliging en privacy.

5.6 Incidenten en datalekken

Alle medewerkers, die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol. De afhandeling van deze incidenten volgt een gestructureerd proces, dat ook voorziet in de juiste stappen rondom de meldplicht datalekken. Alle [beveiligings-]incidenten worden vastgelegd in een incidentenregister. Alle [beveiligings-]incidenten moeten worden gemeld bij FG/SO via datalekken@hetsticht.nl

In het geval van dataverlies d.m.v. ransomware (gijzelsoftware) of hacking heeft Microsoft 365 de mogelijkheid om gegevens van 3 tot uiterlijk 6 maanden terug via back-ups weer te herstellen.

Periodiek zullen beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.7 Evaluatie en aansturing

Dit IBP-beleid wordt minimaal elke 4 jaar getoetst en indien noodzakelijk bijgesteld door het bestuur. Hierbij wordt rekening gehouden met:

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

5.8 Naleving en sancties

De naleving bestaat uit algemeen toezicht in de dagelijkse praktijk op de naleving van beleid en richtlijnen. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Er wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingssessies, et cetera.
Mocht de naleving van dit beleid ernstig tekortschieten, dan kan het CvB maatregelen overwegen door een sanctie op leggen binnen de kaders van de CAO en de wettelijke mogelijkheden.
Voor toezicht op de naleving van de AVG vervult de Functionaris Gegevensbescherming [FG] een belangrijke rol. De FG wordt aangesteld door de het CvB en heeft een onafhankelijke toezichthoudende taak. De FG werkt volgens de functieomschrijving en legt verantwoording af aan het CvB.

5.9 Logging en monitoring

Logging en monitoring door de IT-afdeling zorgt ervoor 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.

6. Organisatie – Wie doet wat

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Onderstaand overzicht geeft aan welke verantwoordelijkheden en taken bij welke rollen horen bij Het Sticht.

6.1 Rollen en verantwoordelijkheden

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richtinggevend [strategisch]	Bestuur CvB	• Eindverantwoordelijk • IBP-beleidsvorming, -vaststelling en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages en/of jaarverslagen • Organisatie IBP -laten- inrichten	• Informatiebeveiligings- en privacy beleid vaststellen • Functieomschrijving FG vaststellen • Privacyreglement vaststellen • Privacyverklaring vaststellen
Sturend [Richtinggevend]	Functionaris Gegevensbescherming [FG] en Security officer	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert bestuur/CvB/directie over IBP • Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse • Hanteren en naleven IBP-normen • 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	Processen, richtlijnen en procedures IBP, waaronder: • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Toestemming gebruik beeldmateriaal [gedelegeerd schooldirecties] • Opstellen informatie documentatie voor ouders / verzorgers, directies, CvB • Sociale media reglement • Gedragscode ict en internetgebruik • Gedragscode medewerkers en leerlingen
	Functionaris Gegevensbescherming [FG] en Security officer	• Toezicht op naleving privacy wetgeving • Voorlichting privacy en stimuleren bewustwording Stichtbreed • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement • Inrichten meldpunt datalekken • De FG organiseert een 2-jaarlijkse evaluatie van het IBP-beleid • De FG maakt minimaal 1 x per schooljaar een Jaaroverzicht t.b.v. CvB, Directieoverleg, GMR, RvT en de schoolteams

		• 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.	• Inventariseren waar persoonsgegevens van de school terechtkomen [overzicht verwerkersovereenkomsten]; input dataregister
Uitvoerend [operationeel]	Security officer Functionaris Gegevensbescherming 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 leerlingdossiers • Gedragscode • Omgaan met sociale media • Mediawijs maken • Jaarverslagen • Het juist hanteren van de bewaartermijnen

De verdere uitwerking van de rollen en taken staan beschreven in bijlage 2.

Bijlage 1 Ondersteunende richtlijnen|procedures|documenten

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

Documenten via website Het Sticht [na eventuele melding veilig te openen]

Beleidsplan IBP Het Sticht
Privacyverklaring
Privacyreglement
Gedragscode
Protocol Internet – Social media

Overig

- Dataregisters
- Protocol cameratoezicht + bijbehorend DPIA
- Overige uit te voeren DPIA's
- Protocol beveiligingsincidenten en datalekken
- Incidentenregistratie
- Overzicht bewaartermijnen
- Wachtwoordbeleid versie aug 2021
- Verwerkersovereenkomsten
- Beleidsplan AVG en studenten
- Beleidsplan Sociale veiligheid
- AVG-infoboekje Privacy op school
- Poster top 10 datalekken
- Top 10 bewustwording
- 25-handige tips
- Jaaroverzichten

Er wordt ook gebruik gemaakt van de -digitale- Documentenbibliotheek van het netwerk IBP [Kennisnet & Sivon*]. Leden van het netwerk kunnen daar kennis delen middels opgedane ervaringen met o.a. beleidsstukken, DPIA's en bewustwording: de 'kruisbestuiving'.

*Sivon: https://www.sivon.nl/over-ons/

*Kennisnet: https://www.kennisnet.nl/wie-wij-zijn/
https://aanpakibp.kennisnet.nl/

2 Organisatie; wie doet wat

Deze bijlage beschrijft hoe IBP op drie niveaus wordt georganiseerd.

- Richtinggevend [strategisch]
- Sturend [tactisch]
- Uitvoerend [operationeel]

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Het Sticht voor elk niveau een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.
Beschreven wordt welke rollen, welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen.

Richtinggevend

Eindverantwoordelijk

Het CvB is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast.
De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd.
De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan Security Officer en Functionaris gegevensbescherming.

Sturend | adviserend | monitoring

Functionaris Gegevensbescherming [FG]

Dit is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke (het CvB) en stuurt mede de mensen aan op uitvoerend niveau. Taken:

- 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

De functionaris voor gegevensbescherming (FG), houdt binnen Het Sticht toezicht op de toepassing en naleving van de AVG. De FG zorgt voor het verbeteren en stimuleren van bewustwording rondom IBP, het afhandelen van informatiebeveiligingsincidenten, adviseert over het regelen van privacy, onderhoudt zo nodig de contacten met de Autoriteit Persoonsgegevens (AP) en overlegt met / rapporteert aan de eindverantwoordelijke (CvB). De FG heeft regelmatig overleg met de Security officer. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

Uitvoerend

Security Officer [SO]

De Security Officer vormt een technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers.

Ieder softwarepakket of (web-)applicatie heeft een beheerder. Bij vragen over de software of applicatie is bekend wie daarvoor aangesproken kan worden. Bij Het Sticht is dat de Bovenschools ICT-coördinator tevens SO.

Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists, protocollen, richtlijnen en/of school ICT-coördinator.
Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door privacy bewust te zijn bij het dagelijks handelen, meldingen te maken van security incidenten en het doen van verbetervoorstellen.

Leidinggevende

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

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

De leidinggevende kan in zijn/haar taak ondersteund worden door de ICT-coördinator, FG en/of SO.