Informatiebeveiligings- en privacy beleid
Stichting Saenstroom

Opsteller: Jan Zonneveld
Expertise: Informatiemanagement

Revisiedatum: 1 november 2018

Vastgesteld door het bestuur van de Stichting Saenstroom op 25 juni 2018

1 Inleiding

Het onderwijsveld is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. Ook neemt de hoeveelheid informatie toe door ontwikkelingen als gepersonaliseerd leren met ICT. Deze afhankelijkheid van ICT en gegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het is van belang om adequate maatregelen te nemen op het gebied van informatiebeveiliging en privacy (IBP) 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. Dit document wordt zo nodig herzien naar aanleiding van ontwikkelingen, incidenten en wetgeving.

1.1 Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening te garanderen.

Deze aspecten zijn:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten juist, actueel 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 onacceptabele risico's bij de uitvoering van onderwijs en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

1.2 Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform huidige wet – en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die herleidbaar zijn tot een bepaald individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. 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.*

1.3 Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijk onderdeel is van privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar en zijn van elkaar afhankelijk. Het onderwerp informatiebeveiliging en privacy wordt afgekort tot IBP. Dit beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen de stichting Saenstroom.

2 Doel en reikwijdte

2.1 Doel

Dit beleid heeft als doelen:

- ***Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.***
- ***Het beschermen van de privacy van leerlingen en medewerkers waardoor het risico op beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden geminimaliseerd.***

Dit beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij er een goede balans moet zijn tussen privacy, functionaliteit en veiligheid. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene, met name van medewerkers en leerlingen, wordt gerespecteerd en Saenstroom voldoet aan relevante wet- en regelgeving.

2.2 Reikwijdte

- Het informatiebeveiligings- en het privacy beleid binnen Saenstroom geldt voor alle medewerkers, leerlingen, ouders/verzorgers, bestuur, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het netwerk verkregen kan worden.

- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van Saenstroom. Het beleid heeft zowel betrekking op gecontroleerde informatie, die door Saenstroom zelf is gegenereerd en wordt beheerd, als op informatie in externe systemen (bijvoorbeeld Magister en AFAS).

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

- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van Saenstroom 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 zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

- IBP-beleid binnen Saenstroom heeft raakvlakken met:
  - Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
  - 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
  - Beleid inzake aanschaf en gebruik van digitale leermiddelen

3 Uitgangspunten

3.1 Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij Saenstroom zijn:

- Informatiebeveiliging en het privacy beleid dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming (die 25 mei 2018 in werking is getreden).
  De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen. Waarbij een goede balans tussen het belang van Saenstroom om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is.

- Binnen Saenstroom 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 fysieke documenten.

- Saenstroom is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert Saenstroom informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen moeten goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.

- Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. De waarde van informatie wordt bij Saenstroom beoordeeld op privacygevoeligheid, bewaartermijnen en vernietigingsplicht. Deze beoordeling is het uitgangspunt voor de te nemen maatregelen. Vervolgens worden mogelijke risico's geïdentificeerd middels een risicoanalyse op basis van de beoordeling. Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.

- Saenstroom sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) bewerkersovereenkomsten af als zij persoonsgegevens ontvangen van Saenstroom. Hierbij wordt gebruik gemaakt van de meest recente versie van het convenant 'Digitale leermiddelen privacy' (www.privacyconvenant.nl) en de bijbehorende model bewerkersovereenkomst. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis.

- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht 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. Saenstroom heeft hiervoor de gedragscode internet en sociale media vastgesteld en geïmplementeerd.

- Informatiebeveiliging en privacy is bij Saenstroom een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing

gewenst is.

- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij Saenstroom vanaf de start rekening gehouden met informatiebeveiliging en privacy.

- Saenstroom zal het beleid uitvoeren volgens de pas toe of leg uit principe.

3.2 Uitgangspunten privacy

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij Saenstroom zijn:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding staan tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie**: Saenstroom 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 en volledig zijn.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

4 Wet- en regelgeving

Saenstroom voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs
- Code goed onderwijsbestuur VO
- Wet bescherming persoonsgegevens
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van het convenant ‘Digitale onderwijsmiddelen en privacy 2.0’ leidend bij het maken van afspraken met leveranciers.

5 Organisatie

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.
Dit hoofdstuk beschrijft hoe IBP binnen Saenstroom is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

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

Voor elk niveau wordt beschreven welke rollen welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen

5.1 Rollen (functies) rondom IBP

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Saenstroom een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

5.2 Richtinggevend

Eindverantwoordelijke

Het Bestuur 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.

5.3 Sturend

Hoofd bedrijfsvoering Service- en Adviescentrum OVO-Zaanstad (OVO service)

Met betrekking tot de onderstaande informatie is het van belang dat OVO service de organisatie is die dienstverlenend is voor Saenstroom op alle beleidsterreinen waar het onderwijs ondersteuning behoeft.

Hoofd bedrijfsvoering is inhoudelijk verantwoordelijk voor IBP en voor de planning en controle. Hij/zij geeft terugkoppeling en adviseert aan de eindverantwoordelijke.

Informatiemanager

Manager IBP is een rol binnen de afdeling bedrijfsvoering op sturend niveau. Deze rol is belegd bij de informatiemanager.

- Het beleid voorbereiden en vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen OVO Zaanstad en Saenstroom.

Privacy officer OVO service

De Privacy officer van OVO service houdt binnen OVO Zaanstad en Saenstroom toezicht op de toepassing en naleving van het beleid. De wettelijke taken en bevoegdheden van de privacy officer geven deze functionaris een onafhankelijke positie in de organisatie. De privacy officer zorgt voor het afhandelen van privacygevoelige informatiebeveiligingsincidenten. Privacy officer heeft regelmatig overleg met manager IBP. De Privacy officer is meestal ook de contactpersoon voor klachten en vragen over privacy van betrokkenen. Deze rol is belegd bij het hoofd bedrijfsvoering van OVO-Zaanstad. Uitzondering geldt voor een datalek bij de klachtencommissie, in dat geval neemt de controller de rol van privacy officer over (functiescheiding).

De directeur van Saenstroom

Adviseert samen met manager IBP het Bestuur en is verantwoordelijk voor het organiseren van ICT- en informatiebeveiliging binnen Saenstroom.

Proceseigenaar

Binnen OVO service zijn er verschillende expertisegebieden, zoals ICT, personeel, administratie, facilitaire- en financiële zaken, onderwijskwaliteit. Voor elk van deze processen is de senior verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies. De manager IBP heeft hier een coordinerende rol.

Deze proceseigenaar is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen en applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben proceseigenaren de volgende specifieke taken:

- Het Bestuur stelt op voorstel van de seniors het beleid voor toegang vast.
- Samen met functioneel beheer en ICT-beheer zien zij erop toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
- Samen met functioneel beheer en ICT-beheer beoordelen zij regelmatig de toegangsrechten van gebruikers.

Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

5.4 Uitvoerend

Privacy officer Saenstroom

Zorgt voor de controle op naleving van de privacy wetgeving binnen de school. Stelt richtlijnen en kaders op. En doet aanbevelingen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens op de school. Zorgt voor de afwikkeling van klachten en incidenten over privacy en meldt deze direct aan de privacy officer van OVO Service.

Security Officer (Functioneel beheerder Informatiemanagement)

De security officer is een rol bij OVO service die belegd is bij de expertise Informatiemanagement. Deze is het technisch aanspreekpunt inzake informatiebeveiliging voor het management en de medewerkers. De security officer heeft kennis van alle technische beveiligings-maatregelen, zoals tokens en versleuteling van gegevens. Na een incident speelt hij een belangrijke rol bij het onderzoek naar de technische oorzaak en het voorkomen van herhaling.

Functioneel beheerder (beheerder van het softwarepakket)

De functioneel beheerder van een softwarepakket kent de richtlijnen, procedures en instructies en instrueert gebruikers met als doel het risico van een datalek te minimaliseren.

Medewerker

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het internetprotocol en privacyreglement. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Medewerkers worden geacht om actief betrokken te zijn bij informatiebeveiliging en privacy. 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 security officer)

Leidinggevende (Directeur/Hoofden)

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

- Een privacy officer voor de school aan te stellen. De privacy officer van de school heeft direct contact met de privacy officer van OVO service. De privacy officers samen vormen een samenwerkingsgroep waarin kennis wordt gedeeld;
- Ervoor te zorgen dat zijn 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.

6 Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt jaarlijks getoetst en zo nodig bijgesteld door de manager IBP. 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

Informatiebeveiliging en privacy van Saenstroom maakt deel uit van de jaarlijkse planning en control cyclus. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst.

Voor alle overlegmomenten geldt dat deze zoveel mogelijk ingepast worden in bestaande overlegvormen met hetzelfde karakter waarbij op:

- **Strategisch** niveau richtinggevend wordt gesproken over organisatie en compliance, alsmede over doelen, scope en ambitie op het gebied van IBP.
- **Tactisch** niveau wordt de strategie vertaald naar plannen, te hanteren normen,

evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering.
- **Operationeel** niveau de onderwerpen worden besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm wordt decentraal georganiseerd.

6.1 Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om alle risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij Saenstroom het bewustzijn van de individuele medewerkers regelmatig aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de manager IBP met het Bestuur als eindverantwoordelijke.

6.2 Classificatie en risicoanalyse

Bij Saenstroom heeft alle informatie waarde, daarom worden alle privacygevoelige gegevens zorgvuldig behandeld en beveiligd opgeslagen. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang zijn voor de informatievoorziening.

6.3 Incidenten en datalekken

De afhandeling van deze incidenten volgt het protocol, dat voorziet in de juiste stappen rondom de meldplicht datalekken.

6.4 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 medewerkers aanspreken in geval van tekortkomingen. Bij Saenstroom wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instellingsbrede gedragscode en met periodieke bewustwordingscampagnes.
Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de privacy officer een belangrijke rol. De privacy officer wordt aangesteld door het Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

7 Bijlage 1: Tabel IBP rollen en taken

Niveau	Wie Rollen	Hoe Verantwoordelijkheid / taken	Wat Realiseren / vastleggen
Richting-gevend **(strategisch)**	Bestuur Samen met hoofd bedrijfs-voering en secretaris CvB OVO	• Eindverantwoordelijk • IBP-beleid en basismaatregelen vaststellen • 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 • Basismaatregelen • Privacyreglement vaststellen
Sturend **(tactisch)**	Hoofd bedrijfs-voering	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert Bestuurdirectie over IBP	Processen, richtlijnen en procedures IBP, waaronder: • Activiteitenkalender
	Secretaris CvB = Privacy officer	• Controle op naleving privacy wetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten over privacy.	• Privacyreglement • Procedure IBP-incident afhandeling • Inrichten meldpunt datalekken
	Manager IBP (Informatie-manager)	• 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 in / Security officer)	• Protocol beveiligingsincidenten en datalekken • Brief toestemming gebruik foto's en video • Opstellen informatie documentatie richting leerlingen, ouders/ verzorgers • Security awareness activiteiten • Sociale media reglement • Gedragscode ICT en internetgebruik • Privacyreglement medewerkers en leerlingen

		• Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door *bestuur/directie* • *Samen met functioneel beheer en ICT-beheer* erop 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.	• Inventariseren waar persoonsgegevens van Saenstroom terechtkomen (leveranciers lijst) • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk • Bewerkersovereenkomsten regelen

Niveau	**Wie** **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren / vastleggen**
Uitvoerend (operationeel)	Privacy officer van de school	• Controle op naleving privacy wetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten over privacy	
	Security officer	• Incidentafhandeling technisch (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten.	
	Medewerker	• Uitvoeren taken conform gegeven richtlijnen en procedures.	
	Dagelijkse leiding/ leidinggevende/ directie	• Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden.	
	Directie en stafhoofden	• 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