Informatiebeveiligings- en privacy beleid (IBP)

SOOG

Stichting Openbaar Onderwijs
Oost Groningen

DOCUMENTBEHEER	
Document naam:	Informatiebeveiligings- en privacy beleid (IBP)
Versiedatum:	Definitief 2024
CvB:	Goedgekeurd d.d.: maart 2024
FG:	[ ] nee review (n.v.t.) [x] ja review [x] akkoord van FG d.d.: januari 2024
MT:	[x] Ter info ontvangen d.d.: maart 2024 [ ] Advies gegeven d.d.: [ ] n.v.t.
GMR:	[ ] Ter info ontvangen d.d.: [ ] Instemming gegeven d.d.: 25 april 2024 [ ] Advies gegeven d.d.: [ ] n.v.t.
RvT:	[ ] Ter info ontvangen d.d.: [ ] Instemming gegeven d.d.: [ ] Advies gegeven d.d.: [x] n.v.t.
CvB:	Vastgesteld d.d.: juli 2024

Inhoud

Inleiding

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.

Het IBP-beleid heeft de volgende doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van alle betrokkenen waarvan SOOOG 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 SOOOG voldoet aan relevante wet- en regelgeving.

In dit document wordt aandacht besteed aan informatiebeveiliging, privacy, de reikwijdte en uitvoering van het IBP-beleid. Daarnaast wordt het beleid en de uitwerking hiervan toegelicht. Als laatste worden de verschillende rollen en verantwoordelijkheden met betrekking tot IBP binnen SOOOG toegelicht.

1. Informatiebeveiliging en privacy

In dit hoofdstuk wordt uitgelegd wat informatiebeveiliging en privacy inhoudt. Er wordt aandacht besteed aan wat de verschillen zijn en in hoeverre beide onderwerpen zich verhouden tot het IBP-proces.

1.1. 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.

1.2. 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.'

1.3. 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 op informatiebeveiliging en privacy binnen SOOOG te regelen en vormt de kapstok voor de onderliggende afspraken en procedures.

2. Normenkader

Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs

Het beschermen van persoonlijke gegevens is in het onderwijs van cruciaal belang. Het onderwijs heeft tenslotte te maken met een minderjarige doelgroep. Leerlingen, maar ook ouders en medewerkers vertrouwen hun gegevens toe aan onderwijsinstellingen. Doordachte gegevensverwerking én goede gegevensbeveiliging vallen onder de verantwoordelijkheid van schoolbesturen en hun medewerkers. Het Normenkader Informatiebeveiliging en Privacy voor het Funderend Onderwijs (IBP FO) is bedoeld om schoolbestuurders, schoolleiders en IBP'ers te helpen met het versterken van hun informatiebeveiliging en verbeteren van de bescherming van persoonsgegevens.

Opzet van het normenkader IBP FO

Het Normenkader IBP FO bestaat momenteel uit 69 normen voor informatiebeveiliging. Later worden daar normen voor privacy aan toegevoegd. Deze normen geven een schoolbestuur inzicht in de maatregelen die nodig zijn voor een zo goed mogelijke bescherming tegen digitale dreigingen als datalekken en cyberaanvallen. Het normenkader bestaat uit een aantal onderdelen:

Beschrijving van de normen: elke norm is voorzien van een korte toelichting, onder de noemer 'Waarom doen we dit?' Zo maken we duidelijk waarop schoolbesturen moeten letten op het gebied van informatiebeveiliging en privacy om de continuïteit, kwaliteit en veiligheid van hun onderwijs te borgen.

Toetsingskader: het toetsingskader bevat diverse punten die met elkaar het minimumniveau vormen waar we als gehele sector en dus ook als individuele schoolorganisaties naartoe werken. Dit niveau is de ondergrens, hier moet elke schoolorganisatie in 2027 aan voldoen.

Voorbeeldmaatregelen: voorgestelde activiteiten en toepassingen waarmee je als schoolbestuur aan het minimumniveau van de norm kunt voldoen.

3. Reikwijdte IBP-beleid

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

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

Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van SOOOG. 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. (bijvoorbeeld uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites en of social media.)

Het IBP-beleid geldt voor de geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens, die plaatsvindt onder de verantwoordelijkheid van

SOOOG evenals op de 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.

IBP-beleid heeft binnen SOOOG 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.

4. IBP-beleid – hoe doen we dat?

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

1. Het schoolbestuur van SOOOG neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. Het bestuur kan hierop worden aangesproken en legt hier verantwoording over af. In termen van de wet- en regelgeving is het bestuur de verwerkingsverantwoordelijke.

2. SOOOG voldoet aan alle relevante wet- en regelgeving rondom informatiebeveiliging en privacy.

3. Bij SOOOG 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 SOOOG 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 te allen tijde hun toestemming herzien.

4. SOOOG zal alle betrokkenen helder en actief informeren over de verwerkingen van de 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.

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

6. Binnen SOOOG 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.

7. SOOOG 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 goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. SOOOG 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. SOOOG 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. SOOOG 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. SOOOG heeft hiervoor een gedragscode geformuleerd, vastgesteld en geïmplementeerd. Deze gedragscode is te vinden op de website van SOOOG.

11. Informatiebeveiliging en privacy is bij SOOOG een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.

12. SOOOG 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.

13. SOOOG 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 SOOOG aanvullende afspraken vast over de technische maatregelen.

14. SOOOG zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens, en eventueel aan de betrokkenen.

5. IBP-beleid en uitwerking

In dit hoofdstuk wordt de praktische invulling van het IBP-beleid beschreven.

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.

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:

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. Deze grondslagen zijn:
    1. Er is toestemming van de persoon om wie het gaat.
    2. Het is noodzakelijk om gegevens te verwerken om een overeenkomst uit te voeren.
    3. Het is noodzakelijk om gegevens te verwerken omdat dit wettelijk verplicht is.
    4. Het is noodzakelijk om gegevens te verwerken om vitale belangen te beschermen.
    5. Het is noodzakelijk om gegevens te verwerken om een taak van algemeen belang of openbaar gezag uit te oefenen.
    6. Het is noodzakelijk om gegevens te verwerken om het gerechtvaardigde belang te behartigen.
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 (subsidiar). 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 zowel gevraagd als 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 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 bewustwordingscampagnes voor medewerkers, leerlingen en gasten. Verhoging van de IBP-bewustzijn is een gezamenlijke verantwoordelijkheid van de privacy officer, de functionaris gegevensbescherming en de ICT'er met het college van 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)systemen, 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

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. Beveiligingsincidenten kunnen worden gemeld bij privacy@sooog.nl of via deze link. Periodiek zullen de beveiligingsincidenten besproken worden en waar nodig aanvullende passende beleidsmaatregelen genomen worden.

5.7. Planning en controle

Het IBP-beleid van SOOOG wordt periodiek getoetst en 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.

Daarnaast hanteert SOOOG een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarbij de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving et cetera meegenomen.

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, tijdens functioneringsgesprekken met medewerkers, met een gedragscode die voor heel SOOOG geldt, met periodieke bewustwordingscampagnes, etc.

Voor toezicht op de naleving van de AVG vervult de functionaris voor gegevensbescherming een belangrijke rol. De functionaris voor gegevensbescherming wordt aangesteld door SOOOG, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De functionaris voor gegevensbescherming werkt via een door SOOOG vastgesteld reglement.

Mocht de naleving van dit beleid ernstig tekort schieten, dan kan SOOOG de betrokken en/of verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO Primair Onderwijs en de wettelijke mogelijkheden.

5.9. Logging en monitoring

Logging en monitoring door de ICT-afdeling van SOOOG 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. Rollen en verantwoordelijkheden

Dit hoofdstuk beschrijft de rollen en verantwoordelijkheden bij de uitvoering van het IBP-beleid. IBP wordt op drie niveaus georganiseerd:

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

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij SOOOG 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.

6.1. Richtinggevend

Eindverantwoordelijke

Het College van Bestuur van SOOOG 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 de privacy officer.

6.2. Sturend

Privacy officer

De privacy officer heeft een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan het College van Bestuur en stuurt mensen aan op uitvoerend niveau. De privacy officer moet:

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

Functionaris voor Gegevensbescherming

De functionaris voor gegevensbescherming (FG) houdt binnen SOOOG toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. 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 rapporteert aan de eindverantwoordelijke (het bestuur). De FG heeft regelmatig overleg met de privacy officer. De FG is ook de contactpersoon voor klachten en vragen van betrokkenen.

ICT-beheer

Adviseert het College van Bestuur samen met privacy officer en is verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen SOOOG.

Proceseigenaar

Binnen SOOOG zijn er verschillende domeinen/processen, zoals ICT, P&O, administratie, facilitaire- en financiële zaken, onderwijs, etc. Op elk van deze domeinen/processen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies. De verantwoordelijkheid van de bovenschoolse processen van SOOOG ligt bij de stafmedewerkers op het bestuursbureau.

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

- Samen met de eindverantwoordelijke stellen zij het beleid voor toegang (autorisaties) vast.
- Samen met functioneel beheer en ICT-beheer zien zij er op toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn en voor hun werkzaamheden toegang toe moeten hebben.
- Samen met functioneel beheer en ICT-beheer beoordelen zij periodiek de toegangsrechten van de gebruikers.

6.3. Uitvoerend

Privacy officer

De privacy officer vormt een technisch aanspreekpunt als het gaat over informatiebeveiliging voor het management en de medewerkers. Daarnaast is de privacy officer verantwoordelijk voor het bijhouden van het verwerkersregister.

ICT en IBP-team

De ICT'er is verantwoordelijk is voor de effectieve inrichting van processen rondom IT en informatiebeveiliging. Het IBP-team wordt organisatie breed zowel preventief als curatief benoemd voor informatiebeveiliging en privacy incidenten. Het IBP-team van SOOOG heeft de volgende opdracht:

- het signaleren en registreren van alle privacy verzoeken, beveiligingsincidenten en datalekken. Het coördineren van de maatregelen en het toezien op de oplossing van problemen die tot incidenten hebben geleid of waardoor de incidenten zijn veroorzaakt (of het bieden van ondersteuning daarbij).
- het geven van voorlichting en het doen van algemene aanbevelingen aan netwerkbeheerders, systeembeheerders, ontwikkelaars en eindgebruikers door het verspreiden van informatie.
- het leveren van managementrapportages en verbetervoorstellen aan de proceseigenaren over de beveiligingsincidenten en verzoeken tot uitoefening privacyrechten van de betrokkenen.

Bij een calamiteit kan het IBP-team terstond bij elkaar worden geroepen op initiatief van de privacy officer, in opdracht van SOOOG. Het doel hiervan is om de **continuïteit** van de informatievoorziening en de privacy te waarborgen. Onder calamiteiten worden verstaan:

- een datalek;
- grote verstoringen van het netwerk (bijvoorbeeld DDoS aanval);
- natuurrampen (brand, overstroming, storm, etc.).

Het IBP-team van SOOOG behandelt meldingen vertrouwelijk en verstrekt alleen informatie over beveiliging en privacy incidenten als dat noodzakelijk en relevant is voor de oplossing van een incident. De werkzaamheden van het IBP-team bij SOOOG zijn gedocumenteerd en door het College van Bestuur bekrachtigd.

De verdere uitwerking van de rollen en verantwoordelijkheden bij de uitvoering van het IBP-beleid binnen SOOOG staan beschreven in een tabel in bijlage 2.

Medewerker
Alle medewerkers van SOOOG hebben verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden. Deze verantwoordelijkheden zijn beschreven in o.a. het personeelshandboek en de gedragscode. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met protocollen, checklists en/of formulieren.

Medewerkers worden gevraagd om 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).

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

- er voor te zorgen dat zijn/haar medewerkers op de hoogte zijn van het IBP-beleid;
- 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/haar taak ondersteund worden door de privacy officer. Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

7. Netwerkbeheer

Het netwerkbeheer wordt door SOOOG bovenschools beheerd. Alle apparaten die door SOOOG medewerkers worden gebruikt staan vermeld in het beheerders-account en kunnen bij calamiteiten, bijvoorbeeld bij diefstal, worden uitgeschakeld.

Elke school heeft een eigen SharePoint omgeving. In deze omgeving zijn de rechten en rollen verdeeld over directie, lb-ers, leerkrachten en administratief medewerkers.

Iedere medewerker krijgt een eigen account met een wachtwoord. Het account dient met Multi-Factor Authenticatie (MFA) extra beveiligd te worden.

Met het programma datto kan de ICT'er, met goedkeuring van de medewerker, op afstand meekijken op het device van de medewerker.

Leerlingen hebben een eigen afgesloten omgeving op het netwerk. Zij loggen in met hun eigen gebruikersnaam, aangemaakt door de bovenschoolse ICT'er, en wachtwoord.

8. Verwerkersovereenkomsten

SOOOG werkt met diverse partijen samen. Indien deze externe partijen persoonsgebonden en dus privacy gevoelige informatie of data gebruiken en/of verwerken dan dient SOOOG met deze leveranciers een zogenaamde verwerkersovereenkomst aan te gaan. Deze overeenkomsten worden in de regel centraal aangegaan en door de voorzitter van het CvB namens SOOOG getekend. De verwerkersovereenkomsten die met deze externe partijen worden aangegaan worden door het bestuursbureau verzameld en gearchiveerd. Indien scholen eigenhandig verwerkersovereenkomsten hebben afgesloten dan dient hier per omgaande melding van te worden gemaakt bij het CvB zodat alsnog een centrale verwerkersovereenkomst kan worden afgesloten.

Bijlage 1: Ondersteunende richtlijnen en procedures

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

Documenten	**Aandachtspunten**
Procedure toestemming gebruik beeldmateriaal	(toestemmingsbrief)
Procedure voor verwijderen van gegevens	(bewaartermijnen)
Communicatie rechten betrokkenen	(communicatie richting betrokkenen)
Procesbeschrijving rechten betrokkenen	(proces rondom aanvragen van betrokkenen)
Privacyreglement	
Autorisatiematrix	(wie mogen gegevens inzien, bewerken, etc.)
Afspraken gebruik sociale media	
Procedure rondom training medewerkers	(bewustzijn creëren)
Cameratoezicht	
Wachtwoordbeleid	
Responsible disclosure	
Gedragscode ICT en internetgebruik	
Acceptable use policy	(verantwoord gebruik bedrijfsmiddelen)
Procedure rondom uitwisselen gegevens	(passend onderwijs, leerlingendossiers, leerplicht, etc.)
Verplicht vanuit de AVG	
Procesbeschrijving melden datalekken	
Registratie beveiligingsincidenten	
Dataregister om te voldoen aan de registratieplicht	
Verwerkersovereenkomsten	(privacy bijlage beschikbaar stellen)
Procedure gegevensbeschermingseffectbeoordeling	(DPIA)
Risicoanalyse	
Functionaris voor Gegevensbescherming	(communicatie hieronder richting medewerkers)

Bijlage 2: Rollen en verantwoordelijkheden

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 SOOOG.

Richtinggevend	**Eindverantwoordelijk**	
	Verwerkingsverantwoordelijke afhankelijk van de (school)organisatie: • College van Bestuur	• *Eindverantwoordelijk* • *IBP-beleidsvorming, -vastlegging en communiceren ervan* • *Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens* • *Organisatie IBP inrichten; toewijzen van de taken en rollen* • *Evalueren toepassing en werking IBP-beleid op basis van rapportages*
Sturend	**Uitwerken beleid & inhoudelijk verantwoordelijk**	
	• Privacy officer	• *Voorbereiden opstellen IBP-beleid, Classificatie/risicoanalyse* • *Inhoudelijk verantwoordelijk voor uitwerking van het IBP-beleid binnen SOOOG* • *Adviseert CvB over IBP* • *Uitwerken algemeen IBP-beleid naar specifiek beleid op een uniforme manier* • *Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering van het IBP-beleid te ondersteunen* • *Evalueren van het IBP-beleid en de maatregelen*
	• Functionaris voor gegevensbescherming	• *Toezicht houden op naleving privacy wetgeving* • *Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens* • *Voorlichting privacy geven en stimuleren van bewustwording* • *Afwikkeling IBP klachten en incidenten*
	• ICT-beheer	• *Adviseert CvB over IBP* • *Organiseert ICT en informatiebeveiliging binnen SOOOG*
	Proceseigenaren • ICT • P&O • Facilitair • Financiën • Administratie • Secretariaat • Huisvesting	• *Risicoanalyse in samenwerking met inhoudelijk verantwoordelijke* • *Toegangsbeleid zowel fysieke toegang als digitale toegang vaststellen en laten goedkeuren door de verwerkingsverantwoordelijke* • *Regelmatig de (netwerk)toegangsrechten van gebruikers beoordelen, controleren en vastleggen*

Uitvoerend	**Uitvoeren en naleven beleid**	
	• Privacy officer (IBP-team)	• *Incidentafhandeling (registreren en evalueren)* • *Technisch aanspreekpunt voor IBP-incidenten* • *Bijhouden van het verwerkersregister*
	• ICT'er • Leidinggevende, directie • Medewerkers	• *Verantwoordelijk voor de effectieve inrichting van processen rondom IT en informatiebeveiliging* • *Uitvoeren taken conform gegeven richtlijnen en procedures* • *Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden*
	Toezicht naleving en communicatie	
	• FG • Leidinggevende, directie • Privacy officer • ICT'er	• *Communicatie naar alle betrokkenen; er voor 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.*