SKOLO

Stichting Katholiek Onderwijs Losser Overdinkel

Beleidsplan
Informatiebeveiliging en privacy

Herziening 2025

Herziening september 2026

Status: Vastgesteld
Besproken in het DB: 13-10-2025
Positief advies GMR: 03-11-2025
Vastgesteld door directeur-bestuurder: 12-11-2025

Status herziening: Concept
Besproken in het DB: 08-09-2026
Positief advies GMR: 05-10-2026
Vastgesteld door directeur-bestuurder: 07-10-2026

Inhoudsopgave

1 Het belang van informatiebeveiliging en privacy 3
2 Toelichting informatiebeveiliging en privacy binnen SKOLO 3
3 Doel en reikwijdte 4

3.1 Doel 4
3.2 Reikwijdte 4

4 Beleid – Hoe doen we dat? 4
5 Uitwerking van het beleid – Wat doen we? 6

5.1 Ondersteunende richtlijnen en procedures 6
5.2 Voorlichting en bewustzijn 6
5.3 Rechten van betrokkenen 6
5.4 Classificatie en risicoanalyse 6
5.5 Incidenten en datalekken 7
5.6 Planning en controle 7
5.7 Naleving en sancties 7
5.8 Logging en monitoring 7

6 Organisatie - Wie doet wat? 8

6.1 Rollen en verantwoordelijkheden 8

Bijlage 1: Ondersteunende richtlijnen en procedures 10
Bijlage 2: Gegevens betrokken functionarissen 11
Bijlage 3: SKOLO-top 10 in omgang met privacy 12
Bijlage 4: Protocol datalekken 13
Bijlage 5: Taken en verantwoordelijkheden AVG/ IBP-coördinator 16
Bijlage 6: Taken en verantwoordelijkheden Privacy Officer (nog te ontwikkelen)

Noot:
Beleid is in september 2026 aangepast in verband met de benoeming van een nieuwe externe Functionaris Gegevensbescherming en het introduceren van een Privacy Officer in onze organisatie.

1 Het belang van informatiebeveiliging en privacy

Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. Het goed regelen van **informatiebeveiliging en privacy** (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering binnen SKOLO optimaal te kunnen waarborgen.

2 Toelichting informatiebeveiliging en privacy binnen SKOLO

Waarom verwerken wij gegevens?

Op onze scholen verwerken we persoonsgegevens van leerlingen, om onze verplichtingen als onderwijsinstelling te kunnen nakomen. Zo zijn er bijvoorbeeld gegevens nodig om kinderen aan te melden als leerling en om (leer)vorderingen bij te houden. Daarnaast hebben wij de wettelijke verplichting om bepaalde gegevens door te sturen naar andere partijen zoals DUO (ministerie van Onderwijs) en leerplichtambtenaren. Samengevat verwerken wij gegevens van kinderen om goed onderwijs te kunnen geven en om onze wettelijke verplichtingen te kunnen nakomen.

Gegevens die niet voldoen aan onze wettelijke en onderwijskundige taak zullen wij alleen met toestemming van ouders verwerken. Als voor het verwerken van gegevens toestemming wordt gevraagd, zoals voor het gebruik van beeldmateriaal, dan kunnen ouders de toestemming op elk moment intrekken of alsnog geven.

Welke gegevens verwerken wij?

Wij verwerken diverse soorten persoonsgegevens, waarvan wij de meeste gegevens rechtstreeks van ouder/verzorger hebben gekregen omdat deze voor de inschrijving op onze scholen zijn vereist. Je kunt hierbij denken aan contactgegevens, BSN, allergieën en informatie die nodig is in het kader van veiligheid. Daarnaast houden we leervorderingen van kinderen bij in ons schooladministratiesysteem ParnasSys, en in onderwijskundige programma's die wij gebruiken tijdens de lessen (vanwege het grote aantal onderwijskundige programma's, niet per programma nader benoemd).

Hoe gaan wij om met de gegevens van onze leerlingen?

Bij het verwerken van de gegevens gaan wij uit van de gegevens, die noodzakelijk zijn om onze rechten en plichten als onderwijsinstelling na te komen. In een aantal gevallen zijn wij, zoals eerder aangegeven, verplicht om gegevens van onze leerlingen te delen met andere organisaties. Dit zijn onder andere DUO, GGD/JGZ, leerplichtambtenaren, onderwijsinspectie, samenwerkingsverband en accountant. Wij kunnen commerciële derde partijen verzoeken om te ondersteunen bij het verwerken van de gegevens voor de eerdergenoemde doeleinden. Denk hierbij bijvoorbeeld aan digitaal lesmateriaal of een administratiesysteem, waarbij de gegevens niet op ons eigen netwerk worden opgeslagen, maar bij een andere organisatie. Dit gebeurt altijd in opdracht en onder verantwoordelijkheid van SKOLO. Met dergelijke organisaties sluiten we verwerkersovereenkomsten af, waarin onder andere is vastgelegd welke gegevens er verwerkt worden en hoe deze gegevens beveiligd worden.

Wij zullen de gegevens van leerlingen niet delen met commerciële derde partijen voor andere doeleinden. Ook zullen wij deze gegevens nooit verkopen of verhuren aan derde partijen. De persoonsgegevens worden zoveel mogelijk gecodeerd bewaard en alleen gebruikt door de medewerkers die dit nodig hebben voor de uitvoering van hun werk. Daarnaast bewaren wij de gegevens niet langer dan noodzakelijk. Wij hanteren hiervoor de wettelijke bewaartermijnen.

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 SKOLO persoonsgegevens verwerkt, waaronder leerlingen, hun ouders/verzorgers en medewerkers.
- Beveiligings- en privacy-incidenten voorkomen en de eventuele gevolgen hiervan beperken.

3.2 Reikwijdte

- Het IBP-beleid heeft betrekking op het verwerken van alle persoonsgegevens van betrokkenen waaronder binnen SKOLO in ieder geval alle medewerkers, leerlingen en ouders/verzorgers.

- Het beleid geldt voor die toepassingen, die vallen onder de verantwoordelijkheid van SKOLO. 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.

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

- IBP-beleid heeft binnen SKOLO raakvlakken met:
  - Veiligheidsbeleid; 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;
  - ICT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ICT en (digitale) leermiddelen;

4 Beleid – Hoe doen we dat?

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

1. De directeur-bestuurder van SKOLO neemt de verantwoordelijkheid om ervoor te zorgen dat informatiebeveiliging en privacy geregeld wordt. De directeur-bestuurder is hierop aan te spreken en legt hier verantwoording over af. In termen van de wet is het bestuur de verwerkingsverantwoordelijke.

2. SKOLO voldoet aan alle relevante wet- en regelgeving (onder andere de Algemene Verordening Gegevensbescherming).

3. Bij SKOLO is de verwerking van persoonsgegevens altijd gekoppeld aan een specifiek doel en gebaseerd op één van de wettelijke grondslagen (toestemming van gebruiker, vitaal belang, wettelijke verplichting, overeenkomst, algemeen belang, gerechtvaardigd belang). Bij verwerking van persoonsgegevens denken we aan alle gegevens die ten dienste staan van de ontwikkeling en het welbevinden van betrokkenen

(voor een overzicht zie ‘Register van verwerkingsactiviteiten’). Bij alle verwerkingen van persoonsgegevens op basis van toestemming kunnen betrokkenen ten alle tijden hun toestemming herzien.

4. SKOLO maakt voor alle betrokkenen het IBP-beleid inzichtelijk met daarin onder andere verwerkingen van de persoonsgegevens en de rechten van betrokkenen.

5. SKOLO legt alle verwerkingen van persoonsgegevens vast in een register van verwerkingsactiviteiten en zal deze up-to-date houden. SKOLO voldoet hiermee aan de documentatieplicht.

6. Binnen SKOLO 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. SKOLO is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Betrokkenen worden goed geïnformeerd over de regelgeving rondom het gebruik van informatie.

8. SKOLO classificeert informatie en informatiesystemen. De classificatie is het uitgangspunt voor de risicoanalyse en de te nemen passende technische en organisatorische maatregelen.

9. SKOLO 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. SKOLO verwacht van alle betrokken dat zij verantwoord omgaan met informatie en privacy. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies.

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

12. SKOLO 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. SKOLO 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.

14. SKOLO zal alle beveiligingsincidenten vastleggen en datalekken volgens een vast protocol afhandelen en melden bij de Autoriteit Persoonsgegevens en waar nodig aan betrokkenen melden.

5 Uitwerking van het beleid – Wat doen we?

5.1 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 register van verwerkingsactiviteiten.

5.2 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 medewerker door middel van voorlichting voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Een concrete uitwerking hiervan is de SKOLO-top 10 in omgang met privacy (zie bijlage 3). Verhoging van het IBP-bewustzijn is binnen SKOLO een gezamenlijke verantwoordelijkheid van het privacy-team, alle AVG/IBP-, en ICT-coördinatoren van de scholen, de externe Functionaris voor Gegevensbescherming, de netwerkbeheerder, en de directeur-bestuurder als eindverantwoordelijke.

5.3 Rechten van betrokkenen

Een belangrijk onderdeel van de privacywet AVG gaat over de rechten die betrokkenen, zoals ouders, leerlingen of medewerkers, hebben. Die rechten moeten betrokkenen zelf kunnen uitoefenen binnen bepaalde termijnen waarbij zij zelf een verzoek indienen om gegevens in te zien, te wijzigen, te laten verwijderen en/of over te dragen.

<u>Belangrijkste aandachtspunten omtrent de rechten van de betrokkenen:</u>

- De eerste verantwoordelijke om verzoeken van betrokkenen te behandelen is de directeur van de school. In uitzonderlijke gevallen kan het ook de Functionaris voor Gegevensbescherming zijn.
- Het verzoek van de betrokkene hoeft niet schriftelijk te zijn, dat mag ook digitaal of zelfs mondeling. Het verzoek wordt schriftelijk vastgelegd.
- De identiteit van de verzoeker moet duidelijk zijn, er moet vastgesteld kunnen worden dat het gaat om de wettelijk vertegenwoordigers (ouders moeten het gezag hebben over het kind).
- Een antwoord of weigering wordt altijd gemotiveerd in begrijpelijke taal.
- De betrokkene krijgt 4 weken na het indienen van zijn verzoek antwoord.
- Er wordt alleen inzage gegeven in de eigen gegevens.
- De betrokkene heeft het recht om alle gegevens in te zien.
- De enige uitzondering waarbij er geen inzage wordt gegeven is bij verdenking van misbruik of kindermishandeling.

5.4 Classificatie en risicoanalyse

Alle informatie heeft waarde, daarom worden alle gegevens en informatiesystemen waarop dit beleid van toepassing is, geclassificeerd. Er worden passende technische en organisatorische maatregelen getroffen waarbij rekening wordt gehouden met de kans en de impact van de privacy risico's in de diverse verwerkingen.

5.5 Incidenten en datalekken

Alle SKOLO-medewerkers die een beveiligingsincident of datalek vermoeden dienen dit te melden. Het melden van beveiligingsincidenten en datalekken is vastgelegd in een protocol (bijlage 4). 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 en datalekken moeten worden gemeld via meldpunt@skolo.nl. Binnen de wettelijke termijnen wordt passende actie ondernomen.

5.6 Planning en controle

SKOLO kent een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst. Tevens worden hier actuele ontwikkelingen op het gebied van techniek, wet- en regelgeving etcetera meegenomen. Het privacyteam is hiervoor verantwoordelijk.

5.7 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, AVG-coördinatoren en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen.
Voor toezicht op de naleving van de AVG vervult de Functionaris voor Gegevensbescherming (FG) een belangrijke rol. De FG is aangesteld door de het bestuur van SKOLO, en heeft een onafhankelijke toezichthoudende taak.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan SKOLO de betrokken verantwoordelijke medewerkers een sanctie opleggen binnen de kaders van de CAO en de wettelijke mogelijkheden.

5.8 Logging en monitoring

Logging (opslaan van gelogde data) en monitoring door de ICT-coördinator SKOLO en de netwerkbeheerder zorgt ervoor dat gebeurtenissen met betrekking tot geautomatiseerde systemen en toegang tot gegevens wordt vastgelegd. Hieronder vallen onder andere het in- en uitloggen van gebruikers en (poging) tot ongeautoriseerde toegang tot het netwerk.

6 Organisatie - Wie doet wat?

6.1 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 SKOLO.

Niveau	Wie Rollen	Hoe Verantwoordelijkheid/taken	Wat Realiseren/vastleggen
Richtinggevend (strategisch)	Directeur-bestuurder	• 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 • Basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen
Sturend (tactisch)	Privacy-team	• Inhoudelijk verantwoordelijk voor IBP • IBP-planning en controle • Adviseert directeur-bestuurder/DB 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	Processen, richtlijnen en procedures IBP: • Protocol beveiligingsincidenten en datalekken • Verwerkersovereenkomsten regelen • Toestemming gebruik beeldmateriaal via Social Schools. • Opstellen informatie documentatie richting leerlingen, ouders/verzorgers • Sociale mediaprotocol • Gedragscode ICT en internetgebruik • Gedragscode medewerkers en leerlingen • Activiteitenkalender
	Functionaris voor Gegevensbescherming	• Toezicht op naleving privacywetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen. • Afwikkeling klachten en incidenten	• Verantwoordingsrapportage • Afhandeling procedure IBP-incidenten of melding datalekken
	Privacy Officer	• Coördineren, adviseren en uitvoeren privacybeleid • Ondersteuning bij uitvoering • Aanspreekpunt binnen de organisatie en voor FG	• Bewaken van het interne proces • Beoordelen verwerkersovereenkomsten
	Domeinverantwoordelijke/ Proceseigenaren	• Classificatie/risicoanalyse • Toegangsbeleid	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) en het treffen van passende technische en organisatorische

	(ICT, P&O, beheer, financiën, administratie)		maatregelen; input register van verwerkingsactiviteiten • Classificatie- en risicoanalyse documenten • Autorisatiematrix diverse informatiesystemen en netwerk
Uitvoerend (operationeel)	ICT-coördinator SKOLO Functioneel en/of applicatie beheerder Medewerker Directeuren i.s.m. AVG/IPB-coördinatoren	• Incidentafhandeling • Technisch aanspreekpunt voor IBP-incidenten • Uitvoeren taken conform gegeven richtlijnen en procedures • Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden (SKOLO top 10 in omgang met privacy) • Communicatie naar alle betrokkenen (SKOLO-top 10 in omgang met privacy) • Toezien op de naleving van het IBP-beleid en treffen van passende technische en organisatorische maatregelen • Periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur	Communiceren, informeren en toezien op naleving van het IPB-beleid

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.

Aanvullende documenten (verplicht vanuit de AVG):

Document	Status	Vindplaats
Privacy Reglement	Klaar	SKOLO-website
Protocol Datalekken	Klaar	SKOLO-beleidsbibliotheek (SharePoint)
Infographic Protocol datalekken	Klaar	Bijlage 4
Register van Verwerkingsactiviteiten Registratie beveiligingsincidenten	Klaar navragen	SharePoint
Dataregister SKOLO	navragen	
Verwerkersovereenkomsten	Klaar	Map Organisatie/ Kennisnet
Bewaartermijnen	Concept	
Toestemming gebruik beeldmateriaal	Klaar	Via Social Schools
Inschrijfformulier proces vastleggen	Gepland	
Veiligheidsbeleid, personeels- en organisatiebeleid	Vastgesteld	SKOLO-beleidsbibliotheek (SharePoint)
Protocol Cameratoezicht	Nog te ontwikkelen	
Taakomschrijving AVG/IBP coördinator (15 uur Taakbeleid)	Vastgesteld	Bijlage 5
Privacy Officer Taakomschrijving	Concept	

Bijlage 2: Gegevens betrokken functionarissen

Bij SKOLO is een Functionaris Gegevensbescherming (FG) benoemd. Daarnaast heeft SKOLO een onafhankelijk adviseur en toezichthouder op het gebied van de bescherming van persoonsgegevens.

Functionaris gegevensbescherming:
Clemens Geenen info@peponderwijsadvies.nl

Privacy Officer:
Anouk Nordkamp meldpunt@skolo.nl

ICT-coördinator SKOLO
Léon Poorthuis lpoorthuis@skolo.nl

Privacyteam SKOLO
Anouk Nordkamp
Léon Poorthuis
Robert Everink
Susan Eulderink administratie@skolo.nl

Bijlage 3: SKOLO-top 10 in omgang met privacy

Bijlage 4: Protocol datalekken

Bijlage 5: Taken en verantwoordelijkheden AVG/IBP-coördinator

Stichting Katholiek Onderwijs Losser Overdinkel

Status: Vastgesteld met instemming GMR 06-10-2025

Taken en verantwoordelijkheden AVG/IBP-coördinator op schoolniveau

De rol van AVG/IBP-coördinator wordt op schoolniveau gedelegeerd door de directeur in overleg met het team. Voor deze taken worden er 15 uur opgenomen in het taakbeleid.

Van belang

- De Algemene Verordening Gegevensbescherming (AVG) verplicht scholen tot het treffen van passende technische en organisatorische maatregelen ter bescherming van persoonsgegevens.
- Volgens het SKOLO-managementstatuut zijn directeuren bevoegd tot het uitvoeren van gedelegeerde taken (art. 5.1) en mogen zij intern medewerkers mandateren.
- De AVG/IBP-coördinator ondersteunt de directeur bij de inrichting van het IBP-beleid en de naleving daarvan.

Taken- en verantwoordelijkheden AVG/IBP-coördinator

Bewustwording & Cultuur:

- Bevorderen van privacy bewustzijn onder medewerkers, leerlingen en ouders.
  Het hele jaar wordt er aandacht aanbesteed in onder meer tijdens de startvergadering op de scholen en in de SKOLO-nieuwsbrief Hartslag.
- Signaleren van risico's in gedrag en processen m.b.t. gegevensverwerking.

Procesinrichting & Borging:

- Adviseren van de schooldirecteur over IBP-beleid en protocollen.
- Verzamelen van het verwerkingsovereenkomsten op schoolniveau en deze delen met Susan Eulderink uit het privacy-team. Op SKOLO-niveau is er een verwerkingsregister en overzicht van alle verwerkersovereenkomsten.
- Bijhouden van datalekken en ondersteunen bij de afhandeling daarvan conform het protocol datalekken.

Toetsing & Advies:

- Signaleren van afwijkingen van het IBP-beleid en rapporteren aan de directeur.
- 'Beoordelen' van nieuwe projecten/processen op privacy-impact en dit bespreken met de directeur.

Samenwerking & Coördinatie:

- Fungeren als aanspreekpunt voor IBP-gerelateerde vragen op schoolniveau.
- Afstemmen met de bovenschoolse Functionaris Gegevensbescherming (FG).
- Indien nodig meedenken, aandragen en/of participeren actuele documentatie, beleid en formats in samenspraak en overleg met het privacy-team.

Monitoring & Rapportage:

- Rapporteren aan de schooldirecteur over de naleving van het IBP-beleid op schoolniveau.