STICHTING VOOR KATHOLIEK ONDERWIJS AALSMEER
Gerberastraat 2 bestuur@sko-aalsmeer.nl
1431 SG Aalsmeer

IBP-beleid

Informatiebeveiliging en privacy

Antoniusschool Kudelstaart
Jozefschool Aalsmeer
De Oosteinder Aalsmeer

Documentgeschiedenis

Revisies

Versie	Datum	Auteur	Review
1.0	23-05-2025	Jeroen de Bok	Ryan Bakker

Vaststelling

Naam	Functie	Versie	Datum
Ryan Bakker	Bestuurder	1.0	06-11-2025

Inhoudsopgave

1. Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. Lesmateriaal wordt digitaal aangeboden, toetsingsprogramma's worden digitaal en de resultaten en ontwikkelingen van leerlingen worden opgenomen in een digitaal leerlingvolgsysteem. Daarnaast wordt ook veel gebruikgemaakt van digitale communicatie tussen de school, leerlingen en ouders/verzorgers. Door deze ontwikkelingen neemt het risico op verstoring van het onderwijs, verlies of misbruik van gegevens en overmatige dataverzameling toe. Het is de verantwoordelijkheid van de **Stichting voor Katholiek Onderwijs Aalsmeer** (hierna SKOA) om dat te voorkomen en een veilige leeromgeving te bieden.

Dit beleid voor informatiebeveiliging en privacy (IBP-beleid) beschrijft hoe de SKOA met de beveiliging van informatie omgaan en hoe de verwerking van (persoons)gegevens wordt gewaarborgd en gehandhaafd. In het beleid worden de verschillende rollen en verantwoordelijkheden binnen de SKOA op het gebied van informatiebeveiliging en privacy (IBP) beschreven.

1.1. Onze intentie

De SKOA draagt de verantwoordelijkheid voor het creëren van een veilige werk- en leeromgeving. Dit houdt in dat de SKOA passende technische en organisatorische maatregelen neemt om informatie te beschermen en ongeoorloofde toegang, verlies of misbruik te voorkomen.

Het recht op privacy is een grondrecht. Iedereen heeft recht op privacy en bescherming van de persoonlijke levenssfeer. Dit geldt vanzelfsprekend ook voor leerlingen, ouders/verzorgers en medewerkers. De SKOA is verantwoordelijk voor het waarborgen van hun privacy. Dit betekent ook dat deze betrokkenen zeggenschap hebben over het gebruik van hun persoonsgegevens, zoals wettelijk bepaald.

Bij de SKOA staat het bieden van goed onderwijs voorop. Om dit te kunnen doen verwerkt de SKOA diverse persoonsgegevens van leerlingen, ouders/verzorgers en medewerkers. De SKOA vindt het belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. Het goed regelen van informatiebeveiliging en privacy in een beleid is noodzakelijk om de gevolgen van mogelijke informatiebeveiliging- en privacyrisico's tot een aanvaardbaar niveau terug te brengen en de voortgang van het onderwijs te kunnen waarborgen.

1.2. Doelstelling

Dit IBP-beleid is erop gericht de kwaliteit van de verwerking van (persoons)gegevens en de beveiliging van informatie en systemen te verhogen. Hierbij moet een juiste balans bestaan tussen veiligheid, privacy en functionaliteit. Het uitgangspunt is dat een veilige werk- en leeromgeving wordt gecreëerd, de persoonlijke levenssfeer van de betrokkenen wordt gerespecteerd en de SKOA voldoet aan relevante wet- en regelgeving. Dit gebeurt onder andere door bewustwording te vergroten over het belang van het zorgvuldig omgaan met informatie, systemen en persoonsgegevens.

De SKOA maakt gebruik van het '[Normenkader Informatiebeveiliging en Privacy voor het onderwijs]' om inzichtelijk te maken waar de organisatie nu staat en welke maatregelen genomen moeten worden om een veilige werkomgeving te creëren en te voldoen aan de AVG. Het doel is om in 2027 een gemiddeld volwassenheidsniveau van 3.0 te bereiken.

1.3. Reikwijdte

Dit beleid is van toepassing op alle leerlingen, medewerkers, bezoekers, ouders/verzorgers, derde partijen en andere gebruikers die toegang hebben tot of werken met de informatie van de SKOA. Het beleid heeft betrekking op de verwerking van alle soorten gegevens en informatie waaronder; persoonsgegevens, bedrijfsinformatie en technische gegevens. Het is van toepassing op alle gegevensverwerkingen die onder de AVG vallen.

Informatiebeveiliging en privacy maken integraal onderdeel uit van dit IBP-beleid. Informatiebeveiliging is een belangrijke voorwaarde voor privacy. Informatiebeveiliging omvat de beveiliging van **alle** informatie, terwijl privacy gaat over de verwerking van persoonsgegevens.

2. Juridisch kader

2.1. Wettelijke en reglementaire kaders

Het juridisch kader voor dit IBP-beleid wordt gevormd door de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG. Daarnaast kunnen uit andere wet- en regelgeving verplichtingen of instructies voortvloeien voor de verwerking van persoonsgegevens. Voor de SKOA is op dit gebied onder andere de volgende wetgeving van belang:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs en/of Wet op de expertisecentra
- Wet onderwijstoezicht
- Archiefwet en Archiefbesluit
- Leerplichtwet
- Wet medezeggenschap op scholen
- Arbeidsregelgeving en CAO
- Belastingwetgeving
- Telecommunicatiewet en e-privacy wetgeving

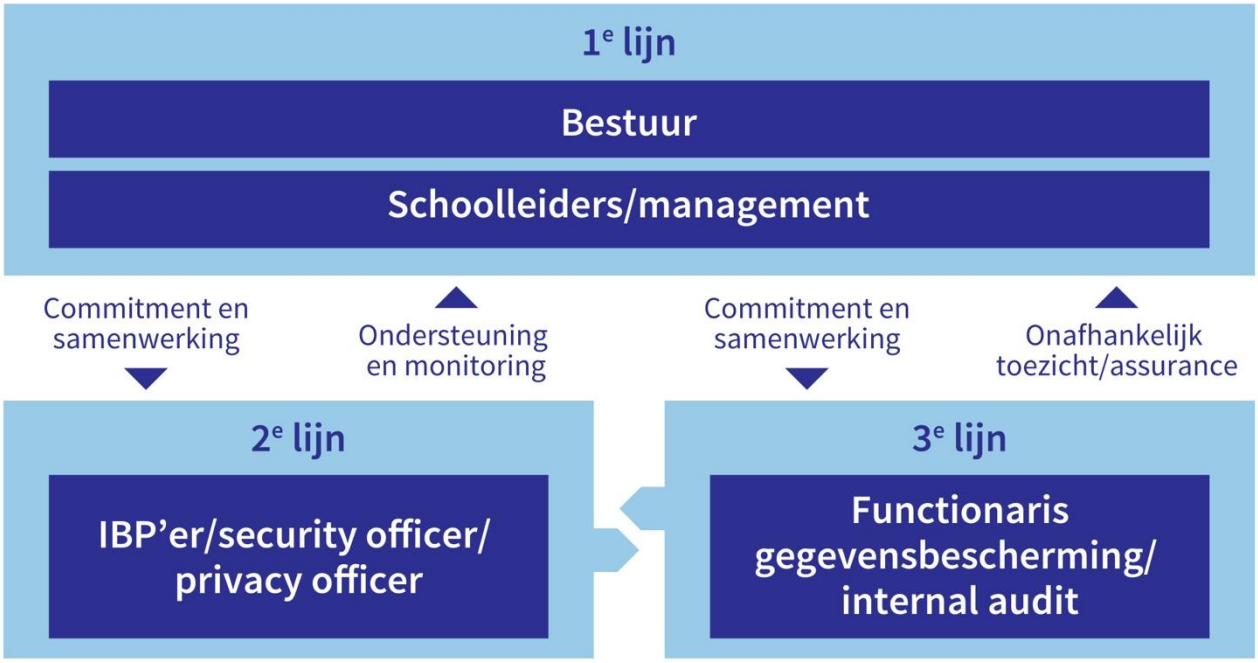
2.2. Normen en standaarden

Als onderwijssector hebben we afgesproken om toe te werken naar één normenkader om aan de minimale vereisten te voldoen voor digitaal veilig onderwijs. Dit is het ‘Normenkader Informatiebeveiliging en Privacy voor het onderwijs’. Dit normenkader beschrijft de regels, principes en standaarden op het gebied van informatiebeveiliging en privacy waaraan de SKOA moet voldoen voor een digitale veilige schoolomgeving.

3. Eigenaarschap en verantwoordelijkheden

Dit hoofdstuk beschrijft hoe de verschillende rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy samenhangen.

3.1. Three Lines model



Informatiebeveiliging en privacy bij de SKOA is ingericht volgens het Three Lines model (3L-model). Het 3L-model is een leidraad bij het inrichten van de governance van een organisatie.

Eerste lijn: eindverantwoordelijkheid bij het bestuur
Het 3L-model heeft als uitgangspunt dat de eerste lijn verantwoordelijk is voor processen, informatie en systemen van de organisatie, de risico's die hieruit voortvloeien en het treffen van de juiste maatregelen om de risico's te verkleinen. De eerste lijn bestaat uit het bestuur en schoolleiders.

Het bestuur is binnen de eerste lijn eindverantwoordelijk voor informatiebeveiliging en privacy, maar kan bepaalde verantwoordelijkheden beleggen bij andere functies binnen de organisatie.

Tweede lijn: adviseren en ondersteunen
Naast de eerste lijn moet er een rol zijn die de eerste lijn ondersteunt, adviseert, coördineert en die bewaakt of het management de verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. De tweede lijn bestaat uit ICT-medewerkers en ICT-coördinatoren.

Derde lijn: onafhankelijke controle
De derde lijn controleert of de eerste en tweede lijn soepel samenwerken en goed functioneren. De derde lijn is onafhankelijk, opereert los van de andere organisatieonderdelen en suggereert waar nodig verbeteringen. De functionaris gegevensbescherming (FG) valt binnen de derde lijn. De FG wordt aangesteld door het bestuur en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak.

3.2. Medezeggenschap

De SKOA betrekt de gemeenschappelijke medezeggenschapsraad (GMR) bij besluiten over regelingen en procedures ten aanzien van de bescherming van persoonsgegevens. Het schoolbestuur is eindverantwoordelijk voor het informeren van de GMR en voor het opstellen van instemmingsprocedures.

4. Beleidsthema’s informatiebeveiliging

In dit hoofdstuk zijn de beleidsthema’s op het gebied van informatiebeveiliging opgenomen.

4.1. Risicomanagement

Als instelling die zich inzet voor een veilige werk- en leeromgeving, erkent de SKOA het belang van het identificeren, analyseren en beheersen van potentiële risico's die de continuïteit van activiteiten en de reputatie van de SKOA kunnen beïnvloeden. Door risico's proactief aan te pakken, probeert de SKOA negatieve gevolgen te minimaliseren en bij te dragen aan de doelstellingen die de SKOA nastreeft.

4.2. Kennis en afhankelijkheid medewerkers

De SKOA is voor de beveiliging van informatie en de continuïteit van het onderwijs afhankelijk van de kennis en beschikbaarheid van medewerkers. De SKOA wil voorkomen dat er onvoldoende kennis aanwezig is bij medewerkers of dat kritieke kennis en vaardigheden onvoldoende aanwezig zijn binnen de organisatie. Taken van sleutelfiguren moeten daarom altijd overgenomen kunnen worden door andere medewerkers. Hiervoor hanteren wij de volgende maatregelen:

- Een back-upplan voor kritieke medewerkers.
- Voldoende training en certificering.
- Duidelijke documentatie.

4.3. Bedrijfscontinuïteit

De SKOA zorgt ervoor dat mogelijke verstoringen van het onderwijs zo snel mogelijk verholpen worden en dat de impact van verstoringen beperkt blijft. Door processen te analyseren worden de meest kritieke applicaties en medewerkers geïdentificeerd, en wordt bepaald welke terugvalopties nu aanwezig zijn. Hierna kunnen maatregelen geïmplementeerd worden om verstoringen zo veel mogelijk te voorkomen of de impact te beperken.

4.4. Back-up en herstel

Om de impact van verstoringen of dataverlies te beperken zorgt de SKOA voor back-ups van systemen en data. Back-ups worden regelmatig getest om te verifiëren of gegevens kunnen worden hersteld. De volgende uitgangspunten worden hierbij gehanteerd:

- De SKOA stelt dezelfde back-upeisen aan diensten van externe leveranciers als aan systemen die we zelf beheren.
- Bij voorkeur maakt de SKOA bij externe leveranciers gebruik van de back-upfaciliteit die ze zelf bij hun dienst aanbieden. Ontbreekt die of voldoet die niet, dan maakt de SKOA zelf back-ups van de informatie die de SKOA verwerkt in de dienst van deze leverancier.
- De SKOA evalueert jaarlijks de manier waarop de SKOA zelf back-ups maakt.

4.5. Fysieke beveiliging

Aangezien veel server- en patchkasten in openbare- en opslagruimtes staan zorgt de SKOA dat de patchkasten zijn afgesloten en alleen toegankelijk zijn met sleutels die zijn opgeborgen op een veilige plek. De opbergplek wordt beschreven in de documentatie.

4.6. Systeem- en data-eigenaarschap en configuratiebeheer

Om IT-processen te beheren is inzicht nodig in welke systemen worden gebruikt binnen de organisatie. Veel van de IBP-thema's in dit beleid zijn afhankelijk van dit inzicht. De rol van systeemeigenaar wordt gebruikt om bepaalde verantwoordelijkheden toe te kunnen wijzen die specifiek voor een systeem gelden. De rol van proceseigenaar wordt gebruikt om bepaalde verantwoordelijkheden toe te kunnen wijzen die te maken hebben met een specifiek proces. De SKOA maakt de keuze om eigenaarschap van data niet vast te leggen, maar zich te beperken tot het beleggen van eigenaarschap van systemen waar deze data in is vastgelegd. Voor het vastleggen van processen en het eigenaarschap van systemen en processen treft de SKOA de volgende maatregelen:

- De SKOA heeft een configuratiemanagementdatabase (CMDB) waarin alle systemen, het eigenaarschap en andere benodigde eigenschappen bijgehouden worden.
- Systeemeigenaarschap wordt bepaald vóór implementatie van nieuwe systemen. De eigenaren van systemen worden vastgelegd in het CMDB.
- Proceseigenaarschap wordt bepaald en vastgelegd binnen het verwerkingsregister.

4.7. Classificatie van systemen en data

Om risicogestuurd beslissingen te kunnen nemen is belangrijk om per systeem het benodigde niveau van beschikbaarheid, integriteit en vertrouwelijkheid (BIV) te bepalen. De classificatie is beperkt tot systeemniveau. De SKOA kiest ervoor om de classificatie niet per individueel dataobject toe te passen. De SKOA heeft voor elk systeem dat opgenomen is in de CMDB een BIV-classificatie uitgevoerd. Deze BIV-classificatie wordt gebruikt om te bepalen welke maatregelen er voor het betreffende systeem geïmplementeerd moeten worden.

4.8. Securitybaseline

Een securitybaseline voor IT-systemen is vastgesteld om het risico van ongeoorloofde toegang tot IT-middelen te beperken. De SKOA maakt gebruik van het certificeringsschema ROSA voor het bepalen van de securitybaseline voor IT-systemen in eigen beheer. De securitybaseline is formeel vastgelegd, wordt periodiek geactualiseerd en wordt goedgekeurd door het schoolbestuur. De toepassing van de securitybaseline voor IT-middelen wordt periodiek beoordeeld op naleving. Afwijkingen van de baselines zijn gedocumenteerd en goedgekeurd.

4.9. Bewustwording

Beleid en technische maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hierin ook een belangrijke factor. Daarom wordt het bewustzijn van medewerkers over de verantwoordelijkheden die ze hebben voortdurend aangescherpt, zodat de kennis van bestaande risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.

4.10. Incident- en probleemmanagement

Incidentmanagement is het proces voor het melden van incidenten binnen de organisatie. Sommige incidenten kunnen een datalek tot gevolg hebben. Incidenten binnen de organisatie zijn nooit helemaal uit te sluiten. Bij de SKOA is er een centraal punt waar incidenten gemeld kunnen worden. Hierna worden deze geclassificeerd en afgehandeld. Als ze regelmatig terugkomen kan er sprake zijn van een *known error* en worden hier extra stappen op ondernomen om het onderliggende probleem op te lossen.

4.11. Risicomanagement leveranciers

De SKOA besteedt een deel van de IT uit aan leveranciers, maar blijft eindverantwoordelijk voor beveiliging van informatie en persoonsgegevens. Om ervoor te zorgen dat ook leveranciers zich houden aan de technische maatregelen die volgen uit de securitybaseline zijn bepaalde stappen toegevoegd aan het leveranciersmanagementproces.

4.12. Identiteits- en toegangsbeheer

Met identiteits- en toegangsbeheer zorgt de SKOA ervoor dat iedereen binnen de organisatie alleen bij de gegevens kan waar deze vanuit zijn rol recht toe heeft. Dit om gevoelige informatie af te schermen, de privacy te waarborgen en om de gegevensset bij een datalek zo klein mogelijk te maken. Ook waarborgt de SKOA dat accounts gesloten worden als een persoon niet meer aan de SKOA verbonden is. De uitvoering hiervan is aan de tweede lijn maar de eerste lijn beslist welke rechten er uitgedeeld worden.

4.13. Vulnerabilitymanagement en pentesting

Vulnerabilitymanagement en pentesting vormen een essentieel onderdeel voor het verminderen van risico's, het voorkomen van ongeautoriseerde toegang tot IT-systemen en het beschermen van gegevens tegen mogelijke dreigingen. De SKOA houdt zichzelf op de hoogte van mogelijke vulnerability's en voert pentesten uit.

4.14. Patchmanagement

Met patchmanagement verhelp je kwetsbaarheden in systemen, applicaties en hardware. Het doel is om de beveiliging, stabiliteit en prestaties van IT-omgevingen te waarborgen door het tijdig testen en implementeren van patches. Om dit te bereiken worden patches zover mogelijk automatisch geforceerd binnen een korte periode, eindgebruikers kunnen de patches hierna niet meer uitstellen.

4.15. Logging

Loggegevens bieden inzicht in de activiteiten van systemen en spelen een sleutelrol bij het detecteren, onderzoeken en voorkomen van beveiligingsincidenten. Loggegvens worden waar technisch mogelijk vastgelegd en bewaard om periodiek nagelopen te worden.

4.16. Digitaal sleutelbeheer

De SKOA heeft geen eigen ontwikkelde software waar encryptie is toegepast en heeft dus geen digitale sleutels in beheer.

5. Uitgangspunten privacy

Het algemene uitgangspunt in dit IBP-beleid is dat persoonsgegevens in overeenstemming met de AVG en gerelateerde wet- en regelgeving op zorgvuldige wijze worden verwerkt. Om aan dit uitgangspunt te voldoen verwerkt de SKOA persoonsgegevens in overeenstemming met de privacyvuistregels die in verderop in dit hoofdstuk worden uiteengezet.

5.1. Persoonsgegevens

Persoonsgegevens zijn gegevens die direct of indirect over iemand gaan en dus naar een persoon te herleiden zijn, zoals een naam of e-mailadres. Naast gewone persoonsgegevens - denk aan contactgegevens en onderwijsnummers - onderscheidt de AVG bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens. Daarnaast bestaat een categorie ‘gevoelige’ persoonsgegevens die expliciet in de AVG is benoemd. Dit zijn persoonsgegevens die vanwege hun aard privacygevoelig zijn en daarom extra bescherming verdienen.

- **Bijzondere persoonsgegevens** zijn gegevens die te maken hebben met bijvoorbeeld ras of etnische afkomst, gezondheid, religie of seksueel gedrag. De verwerking van deze gegevens is verboden, tenzij een wettelijke uitzondering bestaat zoals toestemming van de betrokkene.
- **Strafrechtelijke gegevens** zijn gegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten. De verwerking van deze gegevens is ook verboden, tenzij hiervoor een wettelijke uitzondering geldt.
- **Gevoelige persoonsgegevens** zijn gegevens die een groter privacyrisico vormen dan gewone persoonsgegevens. Denk aan financiële gegevens, burgerservicenummers (BSN), beoordelingen of gegevens van kwetsbare leerlingen.

Nummers ter identificatie van een persoon, zoals het BSN, mogen alleen worden gebruikt voor specifieke doeleinden die in de wet zijn vastgelegd. Een onderwijsnummer (persoonsgebonden nummer) is gelijk aan het BSN.

5.2. Privacyvuistregels

Bij het verwerken van persoonsgegevens houdt de SKOA rekening met onderstaande vuistregels. Door deze basisprincipes te volgen zorgen we ervoor dat we kunnen voldoen aan de AVG.

De SKOA verwerkt persoonsgegevens rechtmatig en transparant
De SKOA verzamelt en gebruikt persoonsgegevens op een eerlijke en transparante manier. Persoonsgegevens worden alleen verwerkt als daarvoor een wettelijke grondslag bestaat in de AVG. De SKOA legt altijd duidelijk uit waarom de SKOA bepaalde gegevens nodig heeft, wat de SKOA ermee doet en hoe lang de SKOA deze gegevens bewaart. Daarom informeert de SKOA ouders, leerlingen en medewerkers tijdig over het gebruik van hun persoonsgegevens, via een transparante privacyverklaring. Dit gebeurt bijvoorbeeld op het moment van inschrijving van een leerling.

De SKOA verwerkt persoonsgegevens voor specifieke doeleinden
De SKOA verwerkt persoonsgegevens alleen wanneer vooraf de specifieke doeleinden voor de verwerking zijn bepaald. Deze doeleinden worden vastgelegd. Persoonsgegevens worden niet voor andere, niet-verenigbare, doelen verwerkt. De SKOA zal dus niet persoonsgegevens verzamelen omdat die wellicht ooit

van pas gaan komen. De SKOA doet dit alleen met vooraf bepaalde, duidelijke en gerechtvaardigde doelen, zoals het plannen van onderwijs en communiceren met leerlingen en ouders over de voortgang en schoolactiviteiten.

De SKOA verwerkt alleen noodzakelijke persoonsgegevens
De SKOA verzamelt alleen persoonsgegevens die noodzakelijk zijn voor het doel waarvoor ze worden verwerkt. De SKOA vraagt dus niet om meer gegevens dan de SKOA daadwerkelijk nodig heeft en hanteert hierbij het uitgangspunt 'zo min mogelijk'. De SKOA onderzoekt altijd of de SKOA met minder gegevens of enkel met anonieme gegevens kan werken. Zo vraagt de SKOA bij de inschrijving van een leerling alleen om de gegevens die relevant zijn voor het kunnen bieden van onderwijs en bewaart de SKOA geen overbodige gegevens die niet nodig zijn voor onze schoolactiviteiten.

De SKOA zorgt dat persoonsgegevens juist en actueel zijn
De SKOA treft maatregelen om ervoor te zorgen dat persoonsgegevens correct en actueel zijn. Onjuiste of achterhaalde gegevens worden geactualiseerd of verwijderd. Leerlingen en ouders kunnen op een laagdrempelige manier doorgeven dat persoonsgegevens incorrect zijn en/of gewijzigd moeten worden. Onze processen en systemen worden zo ingericht dat de juistheid van gegevens zoveel mogelijk wordt afgedwongen en gecontroleerd.

De SKOA bewaart persoonsgegevens niet langer dan nodig
De SKOA bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor ze zijn verzameld. Zodra gegevens niet meer nodig zijn, worden ze verwijderd of geanonimiseerd. De SKOA houdt zich hierbij aan vooraf vastgestelde bewaartermijnen. Zo wordt het leerlingendossier (inclusief rapporten en schoolprestaties) na uitschrijving van een leerling niet langer bewaard dan nodig is voor administratieve en onderwijsdoeleinden en dus zo spoedig mogelijk verwijderd, in ieder geval binnen 2 jaar na uitschrijving.

De SKOA zorgt voor een passende bescherming van persoonsgegevens
De SKOA kan de privacy van leerlingen, ouders en medewerkers alleen goed beschermen als de SKOA op een veilige manier met hun persoonsgegevens omgaat. De SKOA is daarom verantwoordelijk voor het treffen van passende technische en organisatorische beveiligingsmaatregelen. Die maatregelen moeten ervoor zorgen dat de persoonsgegevens op een passende wijze worden beveiligd en worden beschermd tegen verlies, vernietiging, beschadiging of onrechtmatige verwerking. Dit doet de SKOA bijvoorbeeld door het gebruik van veilige systemen voor de opslag van leerlinggegevens en het opleiden van personeel in het veilig omgaan met gevoelige gegevens.

De SKOA kan aantonen dat de SKOA voldoet aan de AVG
De SKOA is verantwoordelijk voor het naleven van bovengenoemde vuistregels en kan daarmee aantonen dat de SKOA voldoet aan de belangrijkste uitgangspunten van de AVG. Dit doet de SKOA bijvoorbeeld door het bijhouden van een verwerkingsregister en het uitvoeren van *Data Protection Impact Assesments* (DPIA's) voor gegevensverwerkingen met een hoog privacyrisico.

De SKOA kan zich ethisch verantwoorden

Bij het beoordelen van verwerkingen van persoonsgegevens houdt de SKOA niet alleen rekening met de vereisten uit de AVG (‘*mogen we dit?*’), maar nadrukkelijk ook met ethische aspecten (‘*willen we dit*?). Het gaat hierbij dus niet om de vraag of de SKOA iets ‘mag’ of ‘kan’, maar juist om de vraag of de SKOA iets zouden moeten ‘willen’ als school. Ethische aspecten spelen in het bijzonder een rol bij verwerkingen die privacyrisico’s kunnen opleveren, bijvoorbeeld bij het gebruik van meekijksoftware of schermcontroles. Dit moet ook worden bezien vanuit een ethisch afwegingskader. De SKOA stelt zich dan ook eerst de vraag of de SKOA het kan uitleggen aan leerlingen en ouders.

6. Beleidsthema's privacy

6.1. Verwerkingsregister

De SKOA heeft maatregelen getroffen om aantoonbaar te voldoen aan de eisen uit de AVG. Dit houdt onder meer in dat de SKOA kan aantonen dat de verwerking van persoonsgegevens voldoet aan de uitgangspunten uit de AVG. De SKOA geeft onder meer invulling aan haar verantwoordingsplicht door een overzicht bij te houden met informatie over de persoonsgegevens die zij verwerkt. Dit heet het verwerkingsregister. Dit register bevat bijvoorbeeld informatie over de leerlingenadministratie of het HR-systeem. Het bijhouden van het verwerkingsregister zorgt voor een goed overzicht van welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt. Het register stelt de SKOA in staat te voldoen aan haar verantwoordingsplicht.

Het verwerkingsregister bevat van afzonderlijke verwerkingsactiviteiten informatie over onder meer de doeleinden voor de verwerking, de toepasselijke grondslag onder de AVG, een beschrijving van de betrokkenen, een beschrijving van de persoonsgegevens, de toepasselijke bewaartermijnen en de ontvangers waarmee persoonsgegevens worden gedeeld.

Persoonsgegevens worden alleen verwerkt als een specifiek, vooraf bepaald doel is vastgesteld door de SKOA. Dit doel moet duidelijk en in begrijpelijke taal aan de betrokkenen worden uitgelegd. Persoonsgegevens mogen niet voor andere doeleinden worden gebruikt.

De SKOA moet voor iedere verwerking van persoonsgegevens een geldige reden hebben. De AVG noemt dit een grondslag. De SKOA verwerkt persoonsgegevens alleen op basis van de in de AVG genoemde grondslagen:

- de betrokkene heeft **toestemming** verleend, bijvoorbeeld voor het maken en delen van foto's of video's.
- de verwerking is noodzakelijk voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is, bijvoorbeeld het verwerken van salaris om de arbeidsovereenkomst met werknemers na te komen.
- de verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting,** bijvoorbeeld het delen van salarisinformatie met de Belastingdienst voor de uitvoering van de belastingwetgeving.
- de verwerking is noodzakelijk om **de vitale belangen** van de betrokkene te beschermen, bijvoorbeeld bij een levensbedreigende situatie waarbij het noodzakelijk is dat bepaalde gegevens van een leerling acuut aan hulpverleners moeten worden doorgeven.
- de verwerking is noodzakelijk om uitvoering te geven aan een **taak van algemeen belang**, hierbij gaat het om wettelijk vastgestelde taken en bevoegdheden**.** Zo heeft de SKOA de wettelijke taak om onderwijs te bieden.
- de verwerking is noodzakelijk voor de behartiging van een **gerechtvaardigd belang** van de SKOA of van een derde. Denk hierbij aan het verwerken van medewerkersgegevens voor het opstellen van managementrapportages ten behoeve van beleidsontwikkeling of het gebruik van bewakingscamera's op het schoolplein.

6.2. Informatieplicht

De SKOA verwerkt persoonsgegevens op een behoorlijke en transparantie manier. Dit is in begrijpelijke taal inzichtelijk voor de betrokkenen. De SKOA informeert leerlingen, ouders en medewerkers voorafgaand aan de gegevensverwerking op transparante wijze via een duidelijke privacyverklaring. Deze privacyverklaring wordt gepubliceerd op de website van de SKOA. Hiermee zorgt de SKOA ervoor dat betrokkenen weten welke persoonsgegevens worden verwerkt en voor welke doeleinden dit gebeurt. Ook zijn ze op de hoogte van de rechten die ze hebben.

6.3. Toestemming

Bij het gebruik van toestemming als grondslag gelden een aantal voorwaarden:

- Toestemming moet op een begrijpelijke en toegankelijke manier worden gevraagd, in duidelijke taal en niet verborgen in algemene voorwaarden of lange teksten.
- Toestemming moet vrijwillig worden gegeven en moet ook weer gemakkelijk ingetrokken kunnen worden.
- De SKOA moet kunnen aantonen dat toestemming is verkregen, bijvoorbeeld door logs of ondertekende formulieren.
- Voor kinderen onder de 16 jaar moet een wettelijke vertegenwoordiger toestemming geven. Dit geldt ook voor personen onder curatele, bewind of mentorschap. De SKOA verifieert of deze vertegenwoordiger daadwerkelijk toestemming heeft gegeven.

Leerlingen (of hun wettelijke vertegenwoordigers) worden in bepaalde situaties om toestemming gevraagd. Denk aan de situatie dat de SKOA foto's of video's van leerlingen maakt en publiceert. Dit mag alleen als de school vooraf toestemming heeft verkregen. Omdat een gezagsrelatie bestaat tussen de SKOA en haar leerlingen en medewerkers, moet goed worden beargumenteerd waarom toestemming in specifieke gevallen in vrijheid kan worden gegeven. De SKOA gaat daarom terughoudend om met het gebruik van deze grondslag.

6.4. Privacy by design en privacy by default

Privacy by design betekent dat de SKOA bij de ontwikkeling, het ontwerp, de selectie en het gebruik van toepassingen, diensten en producten zo vroeg mogelijk rekening houdt met privacyrisico's en passende waarborgen inbouwt om de privacy van betrokkenen te beschermen. Neemt de SKOA bijvoorbeeld een leerlingvolgsysteem in gebruik? Dan moet in een vroeg stadium al worden nagedacht over passende toegangsbeperkingen. Leraren horen alleen inzicht te krijgen in de noodzakelijke gegevens van hun eigen leerlingen. *Privacy by default* betekent dat de standaardinstellingen van een product, dienst of proces op de meest privacyvriendelijke instelling staan, tenzij er een reden is om hiervan af te wijken.

Hiermee zorgt de SKOA ervoor dat zo vroeg mogelijk rekening wordt gehouden met privacybeginselen en op die manier privacyrisico's tijdig worden gemitigeerd.

6.4.1. Dataminimalisatie

De SKOA verzamelt alleen gegevens die noodzakelijk zijn voor het doel dat voorafgaand aan de verwerking is vastgesteld. De verzamelde gegevens dienen toereikend, ter zake dienend en niet bovenmatig te zijn. Hiermee voorkomt de SKOA dat er te veel gegevens worden verwerkt. Bij de aanmelding van een leerling verzamelt de SKOA bijvoorbeeld alleen de informatie die nodig is om de leerling op de juiste manier in te

schrijven. Denk aan naam, geboortedatum, adres en contactgegevens van ouders/verzorgers. Extra informatie, zoals het beroep van de ouders, is niet relevant voor de inschrijving en hoort daarom niet te worden verzameld.

6.5. Bewaartermijnen

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor zij zijn verzameld. Na het verlopen van de toepasselijke bewaartermijnen zorgt de SKOA ervoor dat persoonsgegevens tijdig worden vernietigd (of geanonimiseerd). Hierdoor worden persoonsgegevens beter beschermd tegen onnodige verwerking en datalekken. Zo worden bijvoorbeeld overzichten van schoolprestaties en rapporten uiterlijk tot 2 jaar na uitschrijving van een leerling bewaard. Het schooladvies, NAW- gegevens en aanwezigheidsregistratie worden tot uiterlijk 5 jaar na uitschrijving van een leerling bewaard. Een overzicht met alle bewaartermijnen is te vinden bij Kennisnet.

6.6. Afhandelen van datalekken

Voorbeelden van datalekken zijn een gestolen laptop, een verloren usb-stick, of een e-mail met persoonsgegevens die naar de verkeerde persoon is verstuurd. Datalekken moeten direct worden gemeld via privacy@sko-aalsmeer.nl en geregistreerd in het interne register voor beveiligingsincidenten en datalekken. Risicovolle datalekken moeten worden gemeld aan de Autoriteit Persoonsgegevens en ook aan de betrokkenen als het datalek waarschijnlijk een hoog risico voor hen oplevert. Dit gebeurt als het nodig is in samenspraak met de functionaris gegevensbescherming.

6.7. Data Protection Impact Assessment

Voor elke nieuwe verwerking van persoonsgegevens, bijvoorbeeld een nieuw proces, technologie of applicatie, controleert de SKOA of de privacybeginselen uit de AVG worden nageleefd. Bij verwerkingen met een hoog privacyrisico wordt eerst een *Data Protection Impact Assessment* (DPIA) uitgevoerd. Een DPIA brengt in kaart hoe groot de kans is dat de privacy van betrokkenen wordt geschaad, waar de risico's liggen en welke gevolgen dit kan hebben. Op basis van de uitkomsten van de DPIA neemt de SKOA maatregelen om deze risico's te mitigeren.

6.8. Uitwisseling persoonsgegevens

Een verwerker is een partij die in opdracht van de SKOA persoonsgegevens verwerkt, zoals een leverancier van een leerlingadministratiesysteem. Als de SKOA een verwerker inschakelt om persoonsgegevens te verwerken, dan worden privacyafspraken vastgelegd in een verwerkersovereenkomst.

De bepalingen van de meest recente versie van het convenant ‘Digitale onderwijsmiddelen en privacy’ zijn leidend bij het maken van afspraken met leveranciers, die als verwerkers in opdracht van de school persoonsgegevens verwerken.

Persoonsgegevens kunnen ook beschikbaar worden gesteld aan partijen die niet als verwerkers worden aangemerkt, maar als ‘derden’. Deze derden verwerken persoonsgegevens niet in opdracht van een verwerkingsverantwoordelijke, maar voor hun eigen doel. Een verwerkersovereenkomst is daarom ook niet nodig, maar er moet wel een grondslag bestaan om de persoonsgegevens te delen. Denk aan de situatie waarin de SKOA gegevens over medewerkers deelt met de Belastingdienst ten behoeve van de loonaangifte. De Belastingdienst verwerkt deze gegevens voor haar eigen wettelijke doeleinden en handelt niet als verwerker.

6.9. Rechten van betrokkenen

Betrokkenen hebben op grond van de AVG recht op controle op de verwerking van hun persoonsgegevens. Een betrokkene kan onder andere gebruikmaken van het recht op inzage, rectificatie, verwijdering en bezwaar. Leerlingen, leraren en andere medewerkers kunnen een verzoek tot uitoefening van deze rechten indienen via sko-aalsmeer.nl. Ook hebben betrokkenen het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens.

7. Verantwoording IBP

7.1. Naleving AVG

Er vindt toezicht plaats door de SKOA op de naleving van de normen uit dit beleid. Van belang is dat bestuur, schoolleiders en ICT hun verantwoordelijkheid nemen en medewerkers aanspreken in geval van tekortkomingen. De SKOA besteedt in dit verband actief aandacht aan informatiebeveiliging en privacy bij de aanstelling van medewerkers, tijdens functioneringsgesprekken en via bewustwordingscampagnes.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan de SKOA de betrokken verantwoordelijke medewerkers maatregelen opleggen binnen de kaders van de CAO en toepasselijke wetgeving. Voor toezicht op de naleving van de AVG vervult de functionaris gegevensbescherming (FG) een belangrijke rol. De FG kan bijvoorbeeld informatie verzamelen over gegevensverwerkingen en beoordelen of deze aan de AVG voldoen. Ook kan de FG adviezen en aanbevelingen verschaffen aan de SKOA.

7.2. Rapportage

De SKOA heeft de verantwoordelijkheid om het IBP-beleid formeel goed te keuren en te monitoren of het IBP-beleid door de organisatie wordt toegepast. Jaarlijks wordt hierover gerapporteerd in het bestuursverslag.

7.3. Beleidsherziening

Het IBP-beleid wordt door ons eenmaal per twee jaar getoetst en indien nodig herzien. Bij een substantiële wijziging van het IBP-beleid of in geval van belangrijke ontwikkelingen of veranderingen in wet- en regelgeving, volgt er indien nodig een beleidswijziging.