

Oplegnotitie vaste Kamercommissie 1 april 2026 – inbreng Tijmen Smit, voorzitter College van Bestuur Kalsbeek College en bestuurder van het Nederlands Onderwijsinstituut (Neon)

Een onbeheerd device is een open achterdeur — niet alleen voor wie er ongevraagd kan binnendringen, maar ook om te kunnen vaststellen of de leerlingen zelf nog wel verantwoordelijk zijn voor hun schoolwerk.

Een schoolbestuur kan de verantwoordelijkheid voor goed gebruik van AI in het onderwijs pas waarmaken als de randvoorwaarden (beheerd device, sectorale AI-infrastructuur zoals een AI-hub) zijn geregeld.

1. Een schoolbestuur kan pas instaan voor kwalitatief goed en veilig gebruik van AI als het de devices beheert waarop leerlingen werken, dat is het primaire punt dat ik met deze notitie wil bepleiten. Een beheerd device is mogelijk de belangrijkste voorwaarde om meer veiligheidsgaranties te kunnen hebben en te kunnen bepalen wie nu en in de toekomst het huiswerk maakt. Nu is BYOD (Bring Your Own Device) nog het meest gangbaar in het VO. Om besturen hiervoor verantwoordelijk te maken vereist dit dat devices in de Wet Gratis Schoolboeken worden opgenomen.
2. Daarnaast is een sectorale AI-infrastructuur (AI-hub) bijvoorbeeld beheerd door Kennisnet als vervolgstap een aanbeveling waaronder een veilige educatieve laag voor AI in leerapps.

De beheerde devices is de sleutel, de no-regret maatregel die we vandaag nog moeten regelen – de AI-hub bouwen erop voort. Hieronder werk ik ze uit.

1) Beheerde devices

AI ontwikkelt zich razendsnel. Waar ChatGPT en vergelijkbare tools aanvankelijk alleen tekst genereerden op verzoek van de gebruiker, kunnen de nieuwste AI-tools zelfstandig handelingen verrichten op het device: een restaurant reserveren, een e-mail sturen, een formulier invullen, of een aankoop doen met de betaalgegevens die in de browser zijn opgeslagen. Dit is geen toekomstscenario – Alexander Klöpping demonstreerde dit met OpenClaw in februari bij Eva Jinek¹.

Voor het onderwijs betekent dit een fundamenteel nieuw risico. Een leerling die zo'n AI-tool installeert op zijn eigen laptop, brengt daarmee – bewust of onbewust – een tool mee die toegang kan krijgen tot schoolmails, leerlinggegevens in de browser, en gevoelige informatie in de digitale leeromgeving. De school kan niet meer instaan voor de integriteit van het onderwijsproces. Een AI kan immers het huiswerk maken alsof het de leerling zelf is. De school hier moeilijk zicht of greep op krijgen hebben wanneer ze de devices niet beheren. De ontwikkelingen gaan daarnaast snel. Wat gisteren nog een vergezicht was, is vandaag een reële mogelijkheid.

Met een door de school beheerd device, ingeschreven in een zogeheten Mobile Device Management systeem, heeft de school directe, praktische controle. Concreet betekent dit:

- Updates en beveiliging: de school kan beveiligingsupdates op afstand naar alle devices tegelijk sturen, buiten schooltijd, zodat alle leerlingen altijd met dezelfde, actuele en veilige software werken.
- AI-tools blokkeren of goedkeuren: alleen apps en websites die de school heeft goedgekeurd zijn toegankelijk. Een tool als een autonome AI-agent kan worden

¹ <https://www.youtube.com/watch?v=Z4v5cHTzLN8>

geblokkeerd, terwijl goedgekeurde, privacyveilige AI-tools juist beschikbaar worden gemaakt.

- Educatieve apps uitrollen: de school kan apps en leermiddelen centraal installeren op alle devices, zonder dat leerlingen of ouders daar iets voor hoeven te doen.
- Focusmodus aanzetten: tijdens een toets of opdracht kan de school het device vergrendelen op één applicatie. De leerling kan dan niet naar andere websites of apps.

Dit zijn geen uitzonderlijke maatregelen – ze zijn de standaard in elke professioneel beheerde bedrijfsomgeving, alleen in het onderwijs is het niet de standaard. Scholen kunnen de extra kosten voor een device vanuit de lumpsum niet dragen en dus is BYOD (Bring Your Own Device) de huidige standaard. Op een privé device van een leerling kan de school bovenstaande echter niet toepassen. Dat maakt het eigen device van de leerling een blinde vlek in het veiligheidsbeleid van de school.

Opname van devices draagt ook bij aan kansengelijkheid. Scholen die werken met BYOD zien in de praktijk grote verschillen: de ene leerling heeft een snelle, nieuwe laptop, de ander werkt op een verouderd, gedeeld apparaat thuis.

Elke leerling heeft hetzelfde werkende apparaat, met dezelfde software, dezelfde mogelijkheden. Een belangrijk voordeel: ook de toegang tot AI-tools wordt gelijk. Leerlingen wiens ouders een duur AI-abonnement betalen, hebben nu een voorsprong op leerlingen die dat niet hebben. De school kan dit nivelleren door een goedgekeurde, toegankelijke AI-tool voor iedereen beschikbaar te stellen via het beheerde device, zie hiervoor punten 2 en 3.

Het Normenkader Informatiebeveiliging en Privacy (IBP)², ontwikkeld door OCW, Kennisnet, SIVON en de sectorraden, bevat norm SM.03: scholen moeten Mobile Device Management (MDM) toepassen op alle devices die voor onderwijs worden gebruikt. Alle scholen moeten dit voor 2030 op orde hebben.

Deze eis uit het normenkader botst echter met de praktijk: MDM vereist schooleigen devices, je kunt dit namelijk niet afdwingen op privé devices, maar bij vaststelling van het Normenkader zijn er door de toenmalige minister geen structurele middelen beschikbaar gesteld om de devices en het beheer ervan te kunnen bekostigen. Het is daarmee een beleidsverplichting die onmogelijk is om waar te maken.

Oproep

- Grijp de evaluatie van de Wet Gratis Schoolboeken aan om devices structureel onder deze wet te brengen – zodat elk kind in het voortgezet onderwijs recht krijgt op een beheerd schooldevice.
- Dring bij de staatssecretaris aan om de bekostiging van devices op te nemen in het aangekondigde actieplan digitalisering.
- Voeg middelen voor dit doel toe aan de lumpsum, zodat scholen stappen kunnen zetten en onderzoek of dit collectief voor de sector te organiseren is, bijvoorbeeld door Kennisnet en SIVON.

^{2 2} <https://normenkaderibp.kennisnet.nl>

2) Een publieke digitale infrastructuur: AI-hub

Beheerde devices zijn noodzakelijk, maar we kunnen meer doen. Bescherm de publieke waarden in het onderwijs door regie te voeren over welke AI-toepassingen worden ontsloten binnen scholen. Met een publieke digitale infrastructuur in de vorm van een AI-hub kunnen we verantwoord gebruik van AI beter waarborgen. Hierbij kan gedacht worden aan:

a) Sectorale AI-infrastructuur

AI-tools zelf moeten veilig en “soeverein” zijn. De UvA AI Chat³ laat zien hoe dat kan: een eigen front-end op bestaande, door de UvA beheerde versies, van de grote taalmodellen, waarbij alle invoer binnen de eigen infrastructuur blijft, data worden geanonimiseerd en de instelling zelf de regie houdt.

Voor het funderend onderwijs is een vergelijkbare voorziening nodig, bijvoorbeeld beheerd door Kennisnet namens de hele sector: geen datadeling met commerciële buitenlandse partijen en afgestemd op de onderwijscontext. Individuele schoolbesturen in het funderend onderwijs hebben niet de slagkracht van de UvA, daarom moet dit sectoraal als voorziening worden georganiseerd.

Dit is geen luxe, maar een basisvoorziening – net als een leerlingadministratiesysteem. Kennisnet is de aangewezen partij, met structurele bekostiging vanuit de overheid.

b) Een veilige educatieve AI bescherming door EduGenAI

AI wordt steeds meer verweven binnen educatieve apps en leermiddelen (dus niet enkel als chatvenster). Die AI “weet” niet dat het in een schoolomgeving opereert, met minderjarige gebruikers en bijbehorende pedagogische en juridische kaders. EduGenAI, het platform van Npuls voor het vervolgonderwijs, biedt hier mogelijk een model voor.

Voor het funderend onderwijs kan Kennisnet een vergelijkbare functie vervullen of kunnen we gebruik maken van het platform van Npuls: een educatieve gateway die aanbieders van leerapps toegang biedt tot een veilige, gecertificeerde AI-infrastructuur. De AI in die apps krijgt daarmee een ‘educatieve context-laag’ mee: Het AI-model weet dat het in een schoolomgeving opereert, met welke leeftijdsgroep, en welke grenzen gelden. Zo hoeft de sector niet elk AI-component in elke app afzonderlijk te beoordelen, maar kan vertrouwen op één gedeelde, beheerde laag.

Oproep

- Onderzoek of en hoe een EduGenAI functionaliteit voor het funderend onderwijs kan bijdragen aan beter en veiliger gebruik van AI in die sector.
- Onderzoek en ontwikkel een AI-hub voor het funderend onderwijs, soortgelijk aan de UvA AI chatomgeving in beheer bij kennisnet als onderdeel van de basisvoorzieningen portefeuille (basisinfrastructuur)

Het is noodzakelijk dat deze middelen op korte termijn beschikbaar komen om zo de hele onderwijsketen gelijkwaardig te behandelen en de aanpak van Npuls ook toe te kunnen passen in het funderend onderwijs. Dit kan ook bijdragen aan het borgen van de opbrengst van NOLAI op de lange termijn. Hiermee benadruk je ook de aansluiting tussen de applicatielaag en de hublaag.

^{3 3} <https://www.uva.nl/over-de-uva/over-de-universiteit/ai/ai-in-het-onderwijs/uva-ai-chat/uva-ai-chat.html>