Paul Ossewold

Wie is verantwoordelijk voor leerlingdevices?

Een leidraad voor beleid, praktijk en bewustwording in het voortgezet onderwijs

Inhoudsopgave

blz.

“Wie verantwoordelijk is voor het leren, is ook verantwoordelijk voor de veilige omgeving waarin dat leren plaatsvindt.”

Voorwoord

Er is een moment waarop de vraag niet langer technisch is, maar principieel.
Niet: *welke laptop werkt het best?*
Maar: *wie is eigenlijk verantwoordelijk voor dat apparaat – en voor wat ermee gebeurt?*

In die ene vraag komt alles samen wat digitalisering in het onderwijs zo complex én zo wezenlijk maakt: eigendom, verantwoordelijkheid, vertrouwen en veiligheid.
Het raakt aan beleid én aan gedrag. Aan techniek én aan cultuur.
En precies daar – tussen die werelden in – ontstaat het gesprek over leerlingdevices.

De afgelopen jaren heb ik binnen scholen en besturen gezien hoe verschillend dat gesprek gevoerd wordt. Soms zakelijk en scherp, soms vermijdend en aarzelend.
Iedereen voelt dat de keuzes rond leerlingdevices gevolgen hebben, maar zelden is duidelijk *waar* die verantwoordelijkheid precies hoort te liggen.
Is dat bij de leerling, de ouder, de ICT-afdeling of het bestuur?
Het eerlijke antwoord: bij allemaal een beetje, maar bij niemand vanzelfsprekend.

Dit e-boek is bedoeld als gids in dat gesprek.
Niet als technisch handboek of juridisch advies, maar als hulpmiddel voor bestuurders, IBP-teams en schoolleiders die verantwoordelijkheid willen nemen en zoeken naar houvast binnen het **Normenkader Informatiebeveiliging & Privacy (IBP-FO)**.
Het brengt wetgeving, beleid en praktijk bij elkaar, zonder te doen alsof er één juiste oplossing bestaat.
Want digitale volwassenheid begint niet met regels, maar met bewuste keuzes.

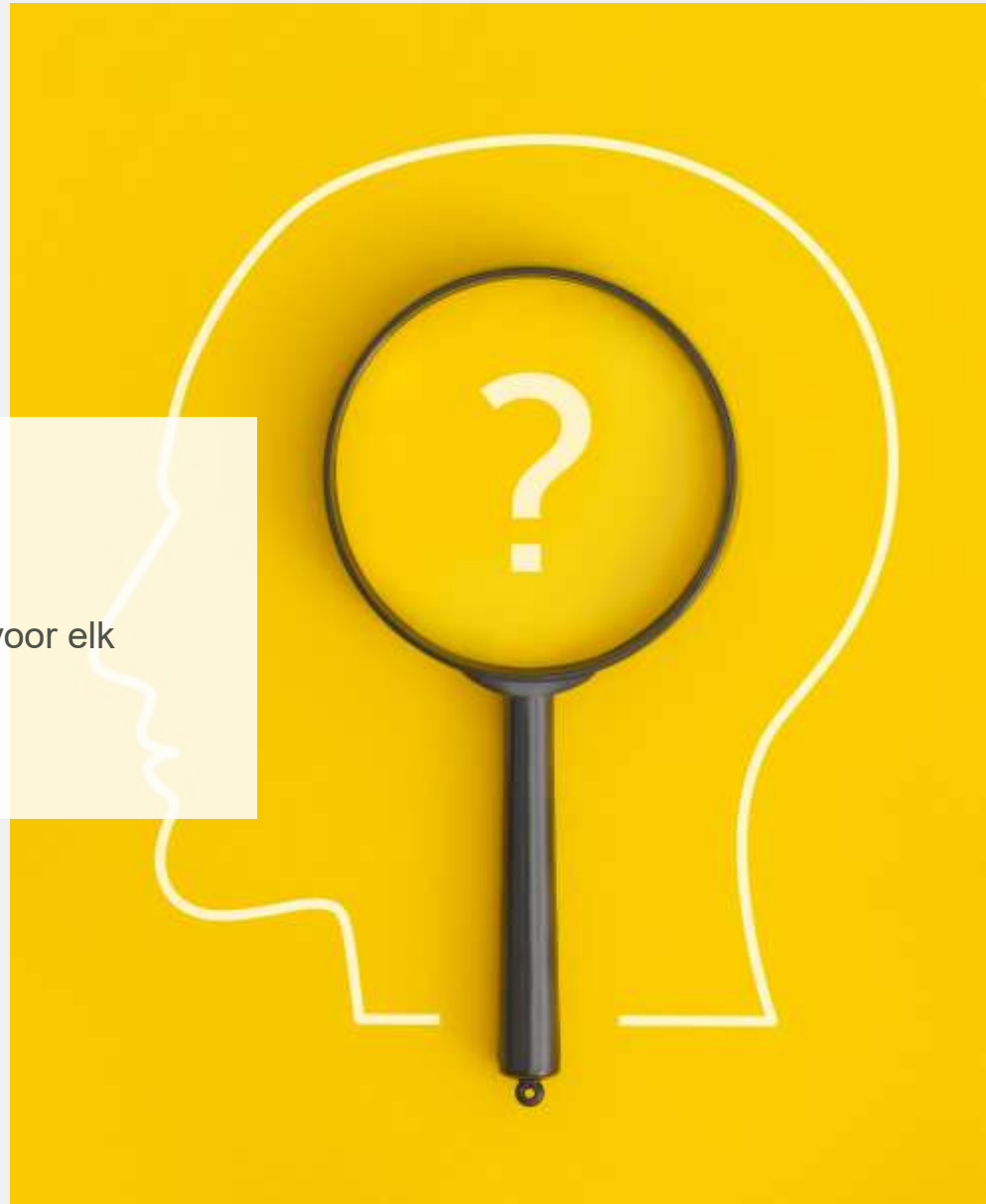
Wie verantwoordelijkheid draagt voor leren, draagt óók verantwoordelijkheid voor de digitale omgeving waarin dat leren plaatsvindt.
Dat is geen last, maar een teken van volwassenheid – van een organisatie die begrijpt dat zorgplicht verder reikt dan de klasdeur.

Paul Ossewold
Den Haag, november 2025

1 De vraag die alles losmaakt

Eén vraag legt bloot wat beleid vaak verbergt: Van wie is eigenlijk dat device?

Deze vraag lijkt praktisch, maar blijkt bestuurlijk van aard.
Ze raakt aan eigendom, zorgplicht en de grenzen van verantwoordelijkheid.
In dit hoofdstuk ontrafelen we waarom juist deze vraag het startpunt vormt voor elk gesprek over digitale volwassenheid in het onderwijs.



Er is op elke school wel een moment waarop de vraag op tafel komt, vaak achteloos gesteld maar met grote gevolgen: *“Van wie is eigenlijk die laptop?”*

Het lijkt een simpele vraag. Een kwestie van bezit, misschien van administratie of van beheer. Maar wie iets langer nadenkt, merkt hoe snel deze vraag zich vertakt in een web van verantwoordelijkheden, verwachtingen en risico’s.
Want als die laptop van de leerling of ouder is, wie bepaalt dan hoe ermee gewerkt wordt? En als er leerlinggegevens op staan, wie is daar dan verantwoordelijk voor? Wat gebeurt er bij verlies, bij een datalek, bij misbruik van accounts?

Wat begint als een praktisch vraagstuk – *mag een leerling eigen apparatuur gebruiken?* – groeit al snel uit tot een principiële kwestie over eigendom, zorgplicht en bestuurlijke verantwoordelijkheid.

Een verschuivende werkelijkheid

De digitalisering van het onderwijs is niet meer te stoppen. De laptop is geen luxe of experiment meer, maar een basisinstrument voor leren, communiceren en organiseren. Toch is het beleid rond die apparaten vaak nog ad hoc: een mengvorm van goedbedoelde afspraken, technische beperkingen en pragmatische keuzes.

Veel scholen staan voor dezelfde paradox:
ze erkennen dat leerlingen hun eigen apparaten gebruiken, maar behandelen die apparaten niet als onderdeel van hun informatiehuishouding. Er wordt van alles geregeld rond netwerken, accounts en applicaties – maar zelden rond het fysieke apparaat zelf.

Het gevolg is een schemergebied waarin iedereen iets voelt van verantwoordelijkheid, maar niemand die volledig draagt.

De blinde vlek

Dat schemergebied is precies waar risico's ontstaan. Een leerling die per ongeluk een bestand downloadt met persoonsgegevens. Een ouder die vanuit huis meeleest in schoolmail. Een onbeveiligde browser waarin toetsen worden gemaakt.

Het zijn geen incidenten van kwade wil, maar van onduidelijkheid. Zolang niet vastligt *wie waarvoor verantwoordelijk is*, kan niemand echt aangesproken worden – en wordt digitale veiligheid iets van toevallige zorg in plaats van structureel beleid.

Daarmee raakt deze ogenschijnlijk kleine vraag aan de kern van volwassen bestuur: niet de techniek bepaalt de verantwoordelijkheid, maar het bestuur dat beleid maakt over techniek.

Van discussie naar gesprek

De vraag "van wie is het device?" leidt op veel plekken tot discussie – over kosten, over autonomie, over vertrouwen. Maar het is vruchtbaarder om die discussie te vervangen door een gesprek: over *rolbewustzijn*, *samenwerking* en *afspraken die werken*.

Het gaat niet om meer controle of meer vrijheid, maar om beter gekozen verhoudingen. Om het besef dat verantwoordelijkheid niet verschuifbaar is, maar wel deelbaar – als iedereen weet wat zijn deel is.

Dit e-boek is geschreven om dat gesprek te helpen voeren: op directieniveau, in IBP-teams en tussen bestuur en ICT. Zodat de vraag niet langer blijft hangen bij "van wie is het device?", maar verdergaat met: "hoe zorgen we samen dat het veilig, eerlijk en werkbaar blijft?"

Wat bestuurders moeten weten

- **De vraag over eigendom is bestuurlijk, niet technisch.**
  Zij bepaalt waar de verantwoordelijkheid ligt voor privacy, veiligheid en continuïteit.
- **De school blijft verwerkingsverantwoordelijke.**
  Ook als het apparaat eigendom is van de leerling of ouder.
- **Onduidelijkheid is zelf een risico.**
  Een gebrek aan afspraken vergroot kwetsbaarheid, zowel juridisch als organisatorisch.
- **Een goed gesprek is beleid.**
  Heldere communicatie tussen bestuur, school en ouders voorkomt misverstanden en vormt de basis van vertrouwen.

ossewold.net

2

Van eigendom naar zorgplicht

Eigendom geeft bezit, geen vrijbrief. Zorgplicht vraagt bewijs.

Zodra een leerling met een schoolaccount inlogt, verandert een privé-device in een onderdeel van de informatiehuishouding van de school.
Hier begint de bestuurlijke verantwoordelijkheid.
We verkennen hoe zorgplicht juridisch, organisatorisch en moreel de basis vormt van elk devicebeleid — los van wie de laptop heeft betaald.

Op papier lijkt eigendom eenvoudig. Wie een laptop koopt, is eigenaar. Punt. Maar in het onderwijs houdt het daar niet op. Zodra datzelfde apparaat gebruikt wordt voor schooltaken, voor toegang tot leerlinggegevens en communicatie via schoolaccounts, krijgt eigendom een tweede laag: verantwoordelijkheid.

Het moment dat een leerling inlogt met een schoolaccount, verandert het apparaat van een privé-object in een onderdeel van de informatiehuishouding van de school. En precies dáár begint de zorgplicht.

De zorgplicht als bestuurlijke verantwoordelijkheid

Scholen verwerken dagelijks persoonsgegevens van leerlingen en medewerkers. Dat gebeurt via netwerken, applicaties, cloudopslag en – steeds vaker – via apparaten die niet van de school zijn. De wet is daar glashelder over:
de school is en blijft **verwerkingsverantwoordelijke** onder de Algemene Verordening Gegevensbescherming (AVG).

Die verantwoordelijkheid kun je niet uitbesteden aan ouders of leveranciers. Een ouder kan eigenaar zijn van de laptop, maar niet van de gegevens die erop verwerkt worden. Een leverancier kan beheerder zijn van een systeem, maar niet de eindverantwoordelijke voor wat daarin gebeurt.

De zorgplicht rust altijd bij het bestuur. Dat betekent: beleid vaststellen, risico's beheersen en aantonen dat passende maatregelen zijn getroffen.

Eigendom is niet hetzelfde als zeggenschap

In de praktijk lopen eigendom en zeggenschap vaak door elkaar. Ouders betalen het apparaat, maar de school bepaalt hoe ermee gewerkt wordt. ICT-afdelingen beheren accounts, maar niet altijd de fysieke toegang. En leerlingen gebruiken het device thuis én op school – met dezelfde instellingen, dezelfde opslag en dezelfde gewoontes.

Die vervlechting maakt het verleidelijk om te denken dat gedeelde verantwoordelijkheid ook gedeelde aansprakelijkheid betekent. Maar juridisch gezien is dat niet zo. De school is verantwoordelijk voor alles wat onder haar onderwijsactiviteiten valt, ongeacht wie de hardware bezit.

Het is daarom essentieel om in beleid vast te leggen waar de grenzen liggen:

- wat mag de school voorschrijven aan beveiligingsmaatregelen op privé-apparaten;
- welke eisen gelden voor gebruik binnen schoolnetwerken;
- en wat gebeurt er bij verlies, defect of datalek.

Zonder zulke afspraken wordt zorgplicht een kwestie van interpretatie – en dat is precies wat het Normenkader IBP-FO wil voorkomen.

De vertaalslag naar beleid

De zorgplicht vraagt niet om controle, maar om kaderstelling. Bestuurders hoeven geen technische beheerders te worden; ze moeten zorgen dat er beleid is dat technische keuzes richting geeft.

Dat beleid vertaalt zich naar drie niveaus:

- **Bestuurlijk:** vaststellen van uitgangspunten en verantwoordelijkheden.
- **Organisatorisch:** inregelen van processen, rollen en toezicht.
- **Operationeel:** uitvoering binnen ICT-beheer en klaspraktijk.

Pas wanneer die drie niveaus op elkaar aansluiten, ontstaat een betrouwbaar systeem van zorg en aansprakelijkheid.

Van reactief naar voorspelbaar

Veel scholen reageren pas op incidenten: een datalek, een kwijtgeraakte laptop, een klacht van ouders. Toch is de stap naar voorspelbaar beleid eenvoudiger dan vaak gedacht. Het begint met één bestuurlijke keuze: **eigendom bepaalt niet langer de reikwijdte van verantwoordelijkheid – zorgplicht wel.**

Vanuit dat uitgangspunt kun je alle praktische vragen beantwoorden:
Mag een leerling eigen apparatuur gebruiken?; onder welke voorwaarden?; en wie is aansprakelijk als het misgaat?

Zodra die uitgangspunten zijn vastgelegd, kunnen ICT-afdelingen, privacy-officers en scholen concreet handelen binnen een helder kader.

Wat bestuurders moeten weten

- **De school blijft altijd verwerkingsverantwoordelijke.**
  Eigendom van apparaten verandert daar niets aan.
- **Zorgplicht is niet deelbaar.**
  Leveranciers of ouders kunnen helpen bij uitvoering, maar niet bij verantwoordelijkheid.
- **Maak beleid op drie niveaus.**
  Bestuurlijk (keuzes), organisatorisch (processen) en operationeel (uitvoering).
- **Beleid voorkomt misverstanden.**
  Heldere afspraken over eigendom, beheer en gebruik beperken juridische en reputatierisico’s.

3 Drie (en een halve) realiteiten in het VO

Tussen volledige controle en totale vrijheid ligt de werkelijkheid van alledag.

Geen twee scholen organiseren digitalisering op dezelfde manier.
In dit hoofdstuk onderscheiden we vier modellen — van schooldevice tot vrije BYOD — en analyseren we hun bestuurlijke consequenties.
Zo ontstaat inzicht in wat wel, niet of slechts gedeeltelijk onder controle te houden is.

Wie rondkijkt in het voortgezet onderwijs, ziet een bont palet aan laptopbeleid.
De één noemt het BYOD, de ander spreekt over bruikleen, weer een ander over “eigen device met schoolinstellingen”.
En allemaal hebben ze gelijk – een beetje.

Er is niet één uniforme route.
De praktijk beweegt zich in een continuüm tussen **volledig centraal beheer** en **volledige vrijheid**.
In dat spectrum ontstaan vier herkenbare werkvormen, die elk hun eigen logica hebben:

- **Schooldevices (SMD)**
- **Managed BYOD**
- **Hybride light**
- **Vrije BYOD**

1. Schooldevices – volledige grip, volledige verantwoordelijkheid

In dit model schaft de school de apparaten zelf aan, beheert ze via een centraal systeem en leent ze uit aan leerlingen.
Het biedt rust, voorspelbaarheid en veiligheid.
Updates, antivirus, filtering, identiteiten – alles verloopt via de beheeromgeving.

Het nadeel is evident: het vraagt forse investering en blijvende aandacht voor beheer en vervanging.
Wie kiest voor maximale grip, kiest ook voor maximale verantwoordelijkheid – financieel, organisatorisch en juridisch.

Bestuurlijk perspectief:
Past bij organisaties die een volwassen ICT-afdeling hebben en digitale veiligheid als kernwaarde beschouwen.
De school kan aantoonbaar voldoen aan het Normenkader, maar betaalt daarvoor in tijd, geld en flexibiliteit.

2. Managed BYOD – gedeelde zorg, gedeeld beheer

Steeds meer scholen kiezen voor een tussenvorm.
Leerlingen (of ouders) schaffen zelf het apparaat aan, maar stemmen in met een beperkt schoolbeheer via een Mobile Device Management-systeem.
Dat betekent: de school kan veiligheidsinstellingen afdwingen, accounts beheren en – indien nodig – apparaten op afstand wissen.

Het apparaat is privébezit, maar tijdelijk onderdeel van de schoolomgeving.
De leerling gebruikt het device zowel thuis als op school, binnen afgesproken kaders.
Er is dus geen sprake van “controle over privédata”, maar van **gezamenlijke verantwoordelijkheid voor schooldata**.

Deze constructie vraagt heldere communicatie:

welke rechten heeft de school binnen het beheersprofiel;
welke data vallen daaronder;
hoe wordt privacy van leerling en ouder gewaarborgd.

Wanneer dat goed wordt uitgelegd en vastgelegd, ontstaat een model dat niet alleen uitvoerbaar is, maar ook past bij de cultuur van vertrouwen en gedeeld eigenaarschap die veel scholen nastreven.

Bestuurlijk perspectief:
Een werkbare balans tussen beheersbaarheid en autonomie.
Vergt duidelijke beleidsafspraken met ouders en leveranciers, en periodieke evaluatie van rechten en instellingen.

3. Hybride light – beleidssturing zonder technisch beheer

In sommige scholen is er wel beleid, maar geen actief beheer.
Er gelden richtlijnen voor software, beveiliging en opslag, maar geen technische afdwinging.
Leerlingen gebruiken eigen devices met schoolaccounts; de school vertrouwt op instructie en toezicht.

Deze aanpak lijkt laagdrempelig, maar leunt zwaar op gedragsafspraken. De effectiviteit hangt af van bewustzijn, discipline en ondersteuning van docenten.

Bestuurlijk perspectief:
Past bij kleinere organisaties of scholen in transitie.
Beperkt geschikt voor structurele naleving van het Normenkader, tenzij bewust gekozen als tijdelijke tussenfase.

4. Vrije BYOD – autonomie met risico

Aan het uiteinde van het spectrum ligt het vrije model: leerlingen kiezen zelf, installeren zelf en onderhouden zelf.
De school biedt enkel toegang tot het netwerk of de cloudomgeving.

Het voordeel is vrijheid; de keerzijde is versnippering, onduidelijkheid en verhoogde kwetsbaarheid.
Er is weinig zicht op beveiligingsniveau, dataopslag of updates.
In feite wordt verantwoordelijkheid gedeeld, maar niet geborgd.

Bestuurlijk perspectief:
Organisatorisch eenvoudig, maar risicovol.
Past niet bij de zorgplicht die de AVG en het Normenkader veronderstellen.
Alleen houdbaar als noodoplossing of tijdelijke overgangssituatie.

Samenvattend overzicht

Model	Eigendom	Beheer	Beveiliging	Kostenverdeling	Bestuurlijke aandachtspunten
Schooldevice	School	Volledig centraal	Uniform en hoog	School	Budget, lifecycle, audits
Managed BYOD	Ouder/leerling	Gedeeld via MDM-profiel	Hoog en afdwingbaar	Gedeeld	Overeenkomsten, communicatie, privacyafbakening
Hybride light	Ouder/leerling	Beperkt	Redelijk, niet gegarandeerd	Gedeeld	Beleid, instructie, bewustwording
Vrije BYOD	Ouder/leerling	Geen	Variabel, vaak laag	Ouders	Risicomanagement, beperkte compliance

De werkelijkheid ertussenin

Geen enkel model is statisch.
In de praktijk schuiven scholen op binnen dit spectrum: van vrij naar beheerd, of juist omgekeerd bij nieuwe aanbestedingen of strategische heroriëntatie.
Wat ertoe doet, is **bewust kiezen** – niet waar je staat, maar waarom.

Digitale veiligheid is geen bezit, maar gedrag in beleid.
Zolang beleid, techniek en communicatie elkaar versterken, is ieder model werkbaar.
Zolang die drie uit elkaar lopen, groeit het risico – ongeacht wie de laptop gekocht heeft.

Wat bestuurders moeten weten

- ❑ **Er bestaat geen standaardmodel.**
  Kies bewust, passend bij omvang, visie en volwassenheid van de organisatie.
- ❑ **Managed BYOD is een volwassen compromis.**
  Het combineert zorgplicht met realisme, mits goed juridisch en organisatorisch geborgd.
- ❑ **Beleid weegt zwaarder dan bezit.**
  De AVG en het Normenkader kijken naar verantwoordelijkheid, niet naar eigendom.
- ❑ **Communicatie is onderdeel van beveiliging.**
  Heldere uitleg richting ouders en leerlingen is even belangrijk als technische maatregelen.

ossewold.net

4 Wet, norm en beleid

Regels beschermen pas wanneer we ze vertalen naar ons eigen handelen.

De AVG en het Normenkader IBP-FO vormen de wettelijke en normatieve basis voor elk devicebeleid.
Maar naleving is geen papieren oefening: ze vraagt om structuur, toewijzing van rollen en aantoonbaarheid.
Dit hoofdstuk laat zien hoe scholen wet en norm kunnen omzetten in werkbaar beleid.

Van wettelijke plicht naar aantoonbare verantwoordelijkheid

Digitalisering in het onderwijs is allang geen vrijblijvend experiment meer. Zodra persoonsgegevens van leerlingen of medewerkers digitaal worden verwerkt, gelden er wettelijke verplichtingen. De kern daarvan is eenvoudig samen te vatten: **wie gegevens verwerkt, draagt de verantwoordelijkheid om ze te beschermen.**

De wettelijke basis – de AVG in het onderwijs

De **Algemene Verordening Gegevensbescherming (AVG)** vormt het fundament. Voor onderwijsinstellingen betekent dit dat het bestuur altijd de **verwerkingsverantwoordelijke** is: de partij die bepaalt *waarom* en *hoe* persoonsgegevens worden verwerkt.

Daaruit volgen drie concrete verplichtingen:

- **Zorgplicht:** de organisatie moet passende maatregelen nemen om gegevens te beveiligen.
- **Aantoonbaarheid:** de school moet kunnen laten zien dat ze dat ook doet (accountability).
- **Transparantie:** betrokkenen – leerlingen, ouders, medewerkers – moeten weten wat er met hun gegevens gebeurt.

De AVG schrijft niet voor *hoe* je dat precies regelt, maar maakt wél duidelijk dat “we wisten het niet” geen geldig argument is.

Het Normenkader IBP-FO – van wet naar toetsbare praktijk

Om scholen te helpen bij het invullen van die verplichtingen is het **Normenkader Informatiebeveiliging en Privacy voor het Funderend Onderwijs (IBP-FO)** ontwikkeld. Waar de AVG algemene beginselen biedt, vertaalt het Normenkader die naar **concrete normen, maatregelen en volwassenheidsniveaus**.

Het kader bestaat uit 15 domeinen voor informatiebeveiliging en 7 voor privacy. Samen vormen ze een instrument om aan te tonen dat een school haar zorgplicht serieus neemt.

Voor devicebeleid zijn vooral deze domeinen relevant:

- **Domein 1 en 2:** beleid en organisatie – wie beslist, wie voert uit;
- **Domein 6 en 7:** incident-, problem- en changemanagement – hoe handel je bij storingen of beveiligingsproblemen;
- **Domein 9:** datamanagement – wie is eigenaar van data, waar staat wat opgeslagen;
- **Domein 11 en 12:** security management en fysieke veiligheid – hoe borg je toegang en bescherming;
- **Domeinen P1 t/m P3:** privacybeleid, rollen en risicobeheersing.

Het Normenkader is geen toets op goede wil, maar een **spiegel voor volwassenheid**: van *ad hoc* handelen naar *beheerst* en uiteindelijk *continu verbeteren*. Het is daarmee evenzeer een groeimodel als een verantwoordingsinstrument.

Van regels naar beleid

De wettelijke en normatieve kaders zijn pas waardevol als ze worden vertaald naar beleid dat in de praktijk leeft.
Dat begint met drie bestuurlijke vragen:

- **Wie is verantwoordelijk voor wat?**
  Leg rollen en verantwoordelijkheden vast – niet alleen op papier, maar ook in mandaten en overlegstructuren.
- **Hoe wordt naleving geborgd?**
  Maak zichtbaar hoe beleid, uitvoering en controle elkaar versterken.
- **Wat betekent dit voor leerlingen en medewerkers?**
  Beleid is pas effectief als iedereen weet wat het betekent voor het dagelijks handelen.

Een goed beleidsdocument verbindt de juridische plicht aan de onderwijskundige opdracht: veilig leren, veilig werken, veilig ontwikkelen.

Van naleving naar leiderschap

Naleving is het begin, niet het doel. De scholen die digitaal écht veilig zijn, zijn niet die met de meeste documenten, maar die waar bestuurders, docenten en leerlingen begrijpen *waarom* die documenten bestaan.

De essentie van wet en norm ligt niet in controle, maar in zorg. Wie beleid maakt, doet dat niet voor inspecties of audits, maar om de digitale omgeving van leerlingen en medewerkers te beschermen. En dat vraagt om iets wat geen wet kan voorschrijven: **bewust leiderschap.**

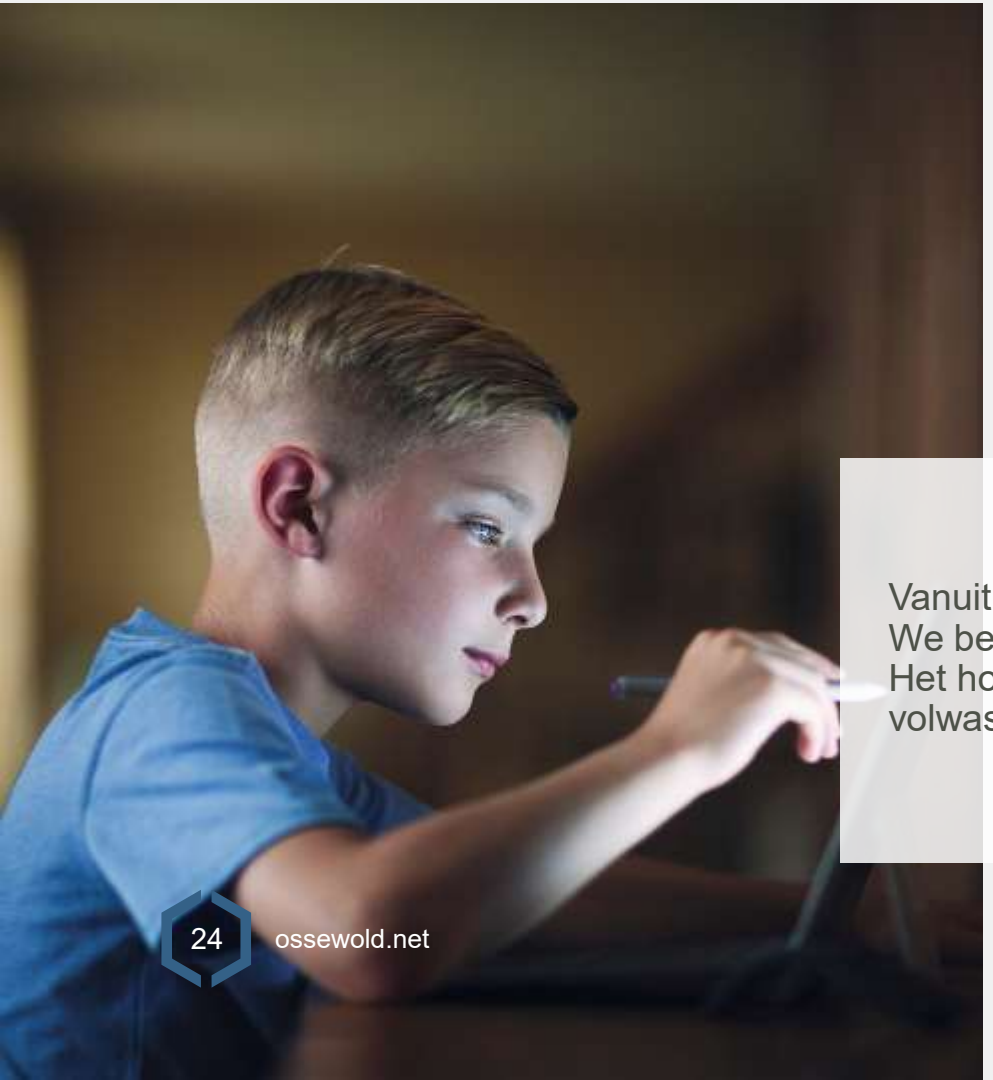
Het verband in één oogopslag

Niveau	Kader	Wat het regelt	Wie verantwoordelijk is	Wat scholen moeten aantonen
Wetgeving	AVG	Rechtmatigheid, doelbinding, beveiliging, transparantie	Schoolbestuur	Passende maatregelen, verwerkersovereenkomsten, DPIA's
Normatief kader	Normenkader IBP-FO	Concrete normen voor organisatie, processen en techniek	Schoolbestuur / IBP-verantwoordelijke(n)	Toetsbare werkwijzen, volwassenheidsniveaus, auditresultaten
Organisatiebeleid	IBP-beleid en Devicebeleid	Toepassing binnen de eigen context	Bestuur / IBP-manager / ICT	Documenten, procedures, communicatie
Praktijk	Uitvoering op scholen	Dagelijks gedrag en bewustzijn	Medewerkers / leerlingen / ouders	Veilige werkwijze en naleving in de praktijk

Wat bestuurders moeten weten

- **De AVG legt verantwoordelijkheid vast, het Normenkader maakt die toetsbaar.**
- **Aantoonbaarheid is net zo belangrijk als naleving.**
  “We doen het goed” telt pas als het ook zichtbaar is.
- **Beleid is de brug tussen regels en praktijk.**
  Zonder vertaling naar gedrag blijft compliance theorie.
- **Leiderschap is onderdeel van beveiliging.**
  Zorgplicht is niet alleen juridische plicht, maar morele keuze.

ossewold.net



5 Beheermodellen en beleidskeuzes

Veiligheid is geen technische instelling, maar een bestuurlijke keuze.

Vanuit wet en norm komt de vraag: *hoe organiseren we het dan?*
We beschrijven de vier beheermodellen, hun risico's, kosten en bestuurlijke impact.
Het hoofdstuk helpt besturen om keuzes te maken die passen bij hun schaal, cultuur en volwassenheid.

Van uitgangspunten naar keuzes die werken

Wetgeving en normen geven richting, maar ze zeggen niet *hoe* een school haar digitale omgeving precies moet organiseren. Daar begint het bestuurlijke vakmanschap: het vertalen van regels naar keuzes die passen bij de eigen schaal, cultuur en ambities.

Een beheermodel is daarbij meer dan techniek. Het is een manier om afspraken, bevoegdheden en verantwoordelijkheden met elkaar te verbinden. Het bepaalt wie beslist, wie uitvoert en wie toeziet — en dus ook waar de school haar risico's beheerst of juist vergroot.

De bestuurlijke bril

Besturen moeten beslissen over meer dan "wat werkt technisch het best?".
De vragen zijn fundamenteler:

- Hoeveel controle wil en kan de school uitoefenen?
- Welke risico's accepteert het bestuur, en welke niet?
- Hoe worden kosten, beheer en privacy in balans gebracht?

Een keuze voor een beheermodel is dus een keuze over **verantwoordelijkheid**: wie draagt die, wie voert uit, en hoe toon je aan dat het werkt.

De vier beheermodellen in samenhang

Zoals al in hoofdstuk 3 gezien, bewegen scholen zich doorgaans binnen vier herkenbare vormen van devicebeheer. Maar hoe kermerken deze modellen zich en hoe verhouden ze zich tot de positie van het bestuur?

Model	Eigendom	Beheer	Kernkenmerk	Bestuurlijke positie
Schooldevice (SMD)	School	Volledig centraal	Maximale grip, uniforme beveiliging	Hoge verantwoordelijkheid, hoge kosten
Managed BYOD	Ouders/leerling	Gedeeld (via MDM-profiel)	Gezamenlijk beheer, gedeelde zorg	Realistische balans tussen grip en autonomie
Hybride light	Ouders/leerling	Beperkt centraal	Richtlijnen, geen afdwinging	Overgangsvorm, leunt sterk op gedrag
Vrije BYOD	Ouders/leerling	Geen	Volledige vrijheid, variabele veiligheid	Minimaal beheersbaar, hoog risico

De matrix laat zien dat het niet gaat om “goed of fout”, maar om **passendheid**. Een school met beperkte ICT-capaciteit kan kiezen voor eenvoud, terwijl een brede scholengroep met volwassen beheerstructuren juist kiest voor centralisatie of gedeeld beheer.

Het principe van gedeelde verantwoordelijkheid

Welke variant een bestuur ook kiest, één principe blijft overeind: **de school blijft eindverantwoordelijk.**

Zelfs bij BYOD kan een bestuur niet zeggen: “Het is niet ons apparaat, dus niet ons probleem.” De zorgplicht gaat over data en toegang, niet over bezit. Dat betekent dat elke vorm van gebruik — van beheerde Chromebooks tot privé-laptops — onder dezelfde bestuurlijke kaders moet vallen:

- duidelijke afspraken over accounts, data-opslag en beveiliging;
- heldere communicatie naar ouders en leerlingen;
- toezicht en incidentafhandeling binnen de IBP-structuur.

De effectiviteit van een beheermodel staat of valt met die governance.

De keuze als proces

Een verantwoord beheermodel ontstaat niet in een vergadering, maar in een **afwegingsproces**. Dat proces doorloopt vier stappen:

- **Inventariseren:** welke behoeften, risico's en middelen zijn er?
- **Afwegen:** welke scenario's passen bij onze organisatie?
- **Besluiten:** wie beslist, en hoe wordt dat besluit vastgelegd?
- **Evalueren:** werkt het beleid in de praktijk, en is het aantoonbaar?

Het is verstandig om deze stappen jaarlijks te herhalen, zodat beleid meegroeit met technologie, wetgeving en schoolcultuur.

Beslismatrix voor bestuurders

Beslisvraag	Schooldevice	Managed BYOD	Hybride light	Vrije BYOD
Wie beheert het device?	School (centraal)	Gedeeld (school + gebruiker)	Gebruiker onder beleid	Gebruiker
Wie betaalt?	School	Ouders, soms lease en bijdrage via school	Ouders	Ouders
Beveiligingsniveau	Hoog, afdwingbaar	Hoog, deels afdwingbaar	Matig	Laag
Compliance (AVG/IBP)	Volledig aantoonbaar	Goed aantoonbaar	Beperkt	Moeilijk aantoonbaar
Autonomie leerling	Beperkt	Gedeeld	Groot	Volledig
Kosten voor school	Hoog	Gemiddeld	Laag	Zeer laag
Risicoprofiel	Laag	Beheersbaar	Middelmatig	Hoog
Aanbevolen bij	Scholen met stabiele ICT en nadruk op digitaal leren	Middelgrote scholen, balans kosten/beheer	Overgangssituaties	Uitzondering of noodscenario

De bestuurlijke keuze

De vraag is niet *welk* model de school kiest, maar *waarom*.
Een goed besluit is transparant, herleidbaar en gedragen.
Het wordt genomen door het bestuur, maar voorbereid door mensen die de praktijk kennen: ICT, IBP, schoolleiding en docenten.
Pas dan ontstaat beleid dat niet alleen op papier klopt, maar ook in de klas werkt.

Daarmee krijgt devicebeleid dezelfde status als elk ander onderdeel van goed bestuur: een afweging van risico, rendement en verantwoordelijkheid.

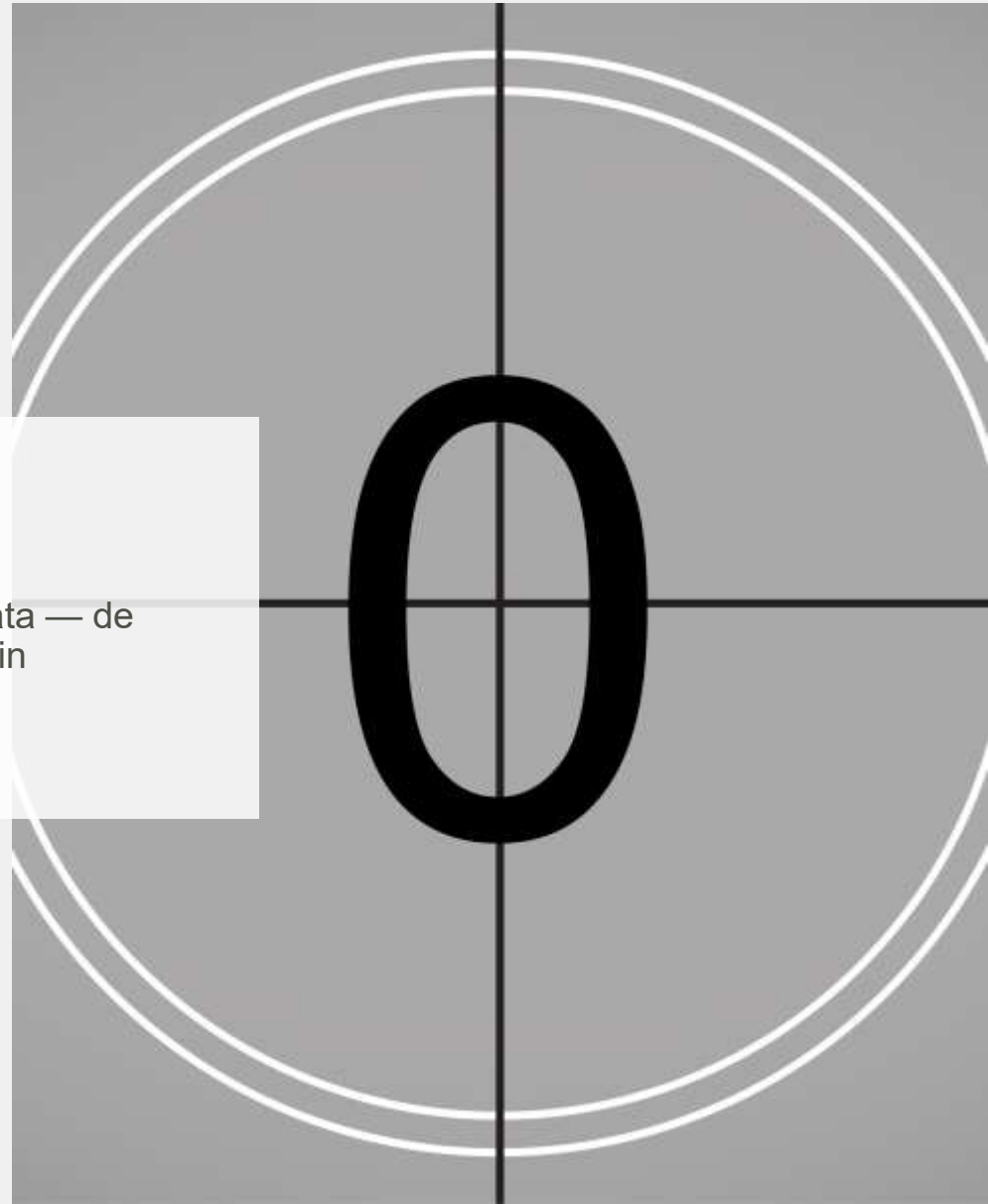
Wat bestuurders moeten weten

- **Een beheermodel is een bestuursbesluit, geen IT-keuze.**
  Het bepaalt de grenzen van zorgplicht en aansprakelijkheid.
- **Gedeeld beheer vraagt om gedeeld vertrouwen.**
  Managed BYOD kan alleen werken met duidelijke communicatie en toestemming.
- **Aantoonbaarheid hoort bij volwassen beleid.**
  Het gekozen model moet toetsbaar zijn binnen het Normenkader.
- **Herzie jaarlijks.**
  Technologie verandert sneller dan beleid; actualiteit is onderdeel van verantwoordelijkheid.

6 Beveiliging in lagen

Vertrouwen is waardevol — maar beveiliging begint bij bewijs.

Zero Trust is geen technische hype, maar een bestuursprincipe:
toegang op basis van identiteit, context en gedrag.
We laten zien hoe beveiliging in lagen — identiteit, apparaat, toegang en data — de zorgplicht vertaalt naar aantoonbare maatregelen, zeker als apparaten niet in schoolbezit zijn.



Van vertrouwen op gewoonte naar vertrouwen op bewijs

Digitale veiligheid begint vaak met een goed gesprek, maar eindigt met concrete instellingen. Het beleid bepaalt de richting, de techniek maakt het aantoonbaar. En juist daar ligt het spanningsveld: scholen vertrouwen op professionals, op leerlingen, op gezond verstand — maar systemen werken niet op vertrouwen, ze werken op bewijs.

Dat is de kern van het principe van **Zero Trust**:

“Vertrouw niemand automatisch, verifieer iedereen voortdurend.”

Voor het onderwijs betekent dit geen wantrouwen, maar volwassenheid: toegang wordt niet gebaseerd op gewoonte, maar op context.
Wie ben je, met welk apparaat log je in, en op welke data krijg je toegang?

De bestuurlijke vertaling van Zero Trust

Zero Trust is geen softwarepakket, maar een **organisatieprincipe**.
Het gaat niet om méér techniek, maar om het consistent toepassen van drie bestuurlijke keuzes:

- **Identiteit is de nieuwe grens.**
  Niet het netwerk bepaalt de toegang, maar de identiteit van de gebruiker.
- **Toegang is altijd voorwaardelijk.**
  Apparaten, locaties en risico’s bepalen of iemand binnen mag, en hoe.
- **Data zijn nooit onbeperkt beschikbaar.**
  Niet elk bestand hoort op elk apparaat; data volgen beleid, geen gemak.

Wie deze drie uitgangspunten bestuurlijk vastlegt, legt de basis voor elke beveiligingsmaatregel — of die nu in Intune, Google Admin of een ander platform wordt uitgevoerd.

Beveiliging in vier lagen

Effectieve digitale veiligheid bestaat uit vier samenhangende lagen. Elke laag heeft zijn eigen maatregelen en verantwoordelijkheden. Pas in combinatie vormen ze een sluitend geheel.

1. Identiteit – wie krijgt toegang?

De eerste laag is de identiteit van de gebruiker.
Authenticatie (MFA), sterke wachtwoorden, lifecycle-beheer van accounts en het uitschakelen van gedeelde logins zijn de basis.
Beleidsmatig betekent dit:

- accounts zijn persoonlijk, niet gedeeld;
- toegang vervalt automatisch bij vertrek of functiewijziging;
- externe gebruikers (zoals stagiairs of leveranciers) worden apart beheerd.

Bestuurlijke implicatie:
Identiteitsbeheer is geen ICT-taak, maar een continu HR-proces dat gekoppeld is aan instroom-, doorstroom- en uitstroomprocedures.

2. Apparaat – wat is betrouwbaar?

De tweede laag is het apparaat zelf.
Of een device nu eigendom is van de school of van de leerling, de organisatie bepaalt of dat apparaat **“compliant”** is met het beveiligingsbeleid.

Een apparaat dat niet voldoet — geen versleuteling, geen pincode, geen updates — krijgt beperkte of geen toegang.

Hier komt **Conditional Access** in beeld:
toegang tot data wordt alleen verleend aan apparaten die voldoen aan vooraf vastgestelde voorwaarden.

Bestuurlijke implicatie:
wanneer een school apparaten niet zelf beheert, moet ze wél beleid hebben dat regelt welke eisen worden gesteld vóórdat toegang wordt verleend.

3. Toegang – waar mag je bij?

Niet iedereen hoeft overal bij.
De derde laag bepaalt **welke applicaties, mappen of cloudomgevingen** toegankelijk zijn per rol of situatie.
Een leerling die via een onbekend apparaat inlogt, kan bijvoorbeeld alleen web-apps gebruiken; een docent op een beheerd device heeft volledige toegang.

Met **Cloud App Control** en toegangslabels kan beleid afdwingen dat gegevens alleen worden geopend binnen veilige apps of browsers, en niet worden gedownload naar onbeheerde apparaten.

Bestuurlijke implicatie:
het bestuur bepaalt via beleid welke risico’s aanvaardbaar zijn, en hoe die vertaald worden naar technische toegangsniveaus.

4. Data – wat mag het systeem onthouden?

De vierde laag gaat over de gegevens zelf. Hier speelt **dataclassificatie**: niet alle informatie is gelijk. Leerlingdossiers vragen een ander beschermingsniveau dan een schoolnieuwsbrief. Door labels, versleuteling en **Data Loss Prevention (DLP)**-regels kan worden vastgelegd wat er met data mag gebeuren: delen, downloaden, printen, of alleen lezen.

Bestuurlijke implicatie:
beleid moet aangeven welke soorten gegevens de school verwerkt, waar ze worden opgeslagen, en wie ze mag bewerken. Zonder die beleidsmatige classificatie is elke technische maatregel willekeurig.

Wat als je het apparaat niet beheert?

Veel scholen laten leerlingen werken op eigen apparatuur. Dat betekent niet dat er géén grip mogelijk is. Integendeel: juist dan moeten maatregelen op de andere lagen extra stevig zijn.

- **Identiteit:** verplicht MFA en sterke wachtwoorden.
- **Apparaat:** controleer via Conditional Access of het device voldoet aan basisveiligheid.
- **Toegang:** beperk toegang tot gevoelige data tot goedgekeurde apparaten.
- **Data:** blokkeer lokale opslag en downloads buiten de schoolcloud.

Het principe is eenvoudig:

“Hoe minder je het apparaat beheert, hoe meer je de toegang moet beveiligen.”

Bestuurders moeten dat besef expliciet opnemen in beleid. Geen beheer is geen excuus voor risico, maar een reden voor extra waarborgen.

Van techniek naar leiderschap

Beveiliging in lagen vraagt geen IT-kennis, maar leiderschap. Besturen hoeven niet te weten hoe Conditional Access wordt ingesteld, maar wél *waarom* het nodig is, wat het beschermt en wie verantwoordelijk is voor naleving.

Het bestuur stelt de kaders, ICT vertaalt ze naar instellingen, en gebruikers handelen binnen die kaders. Zo ontstaat een keten van vertrouwen die aantoonbaar werkt — niet op basis van aannames, maar op basis van beleid.

Wat bestuurders moeten weten

- ❑ **Zero Trust is een bestuurlijke houding.**
  Toegang wordt verleend op basis van bewijs, niet verondersteld vertrouwen.

- ❑ **Beheer is gelaagd.**
  Als je het device niet beheert, moet je identiteit, toegang en data extra beschermen.

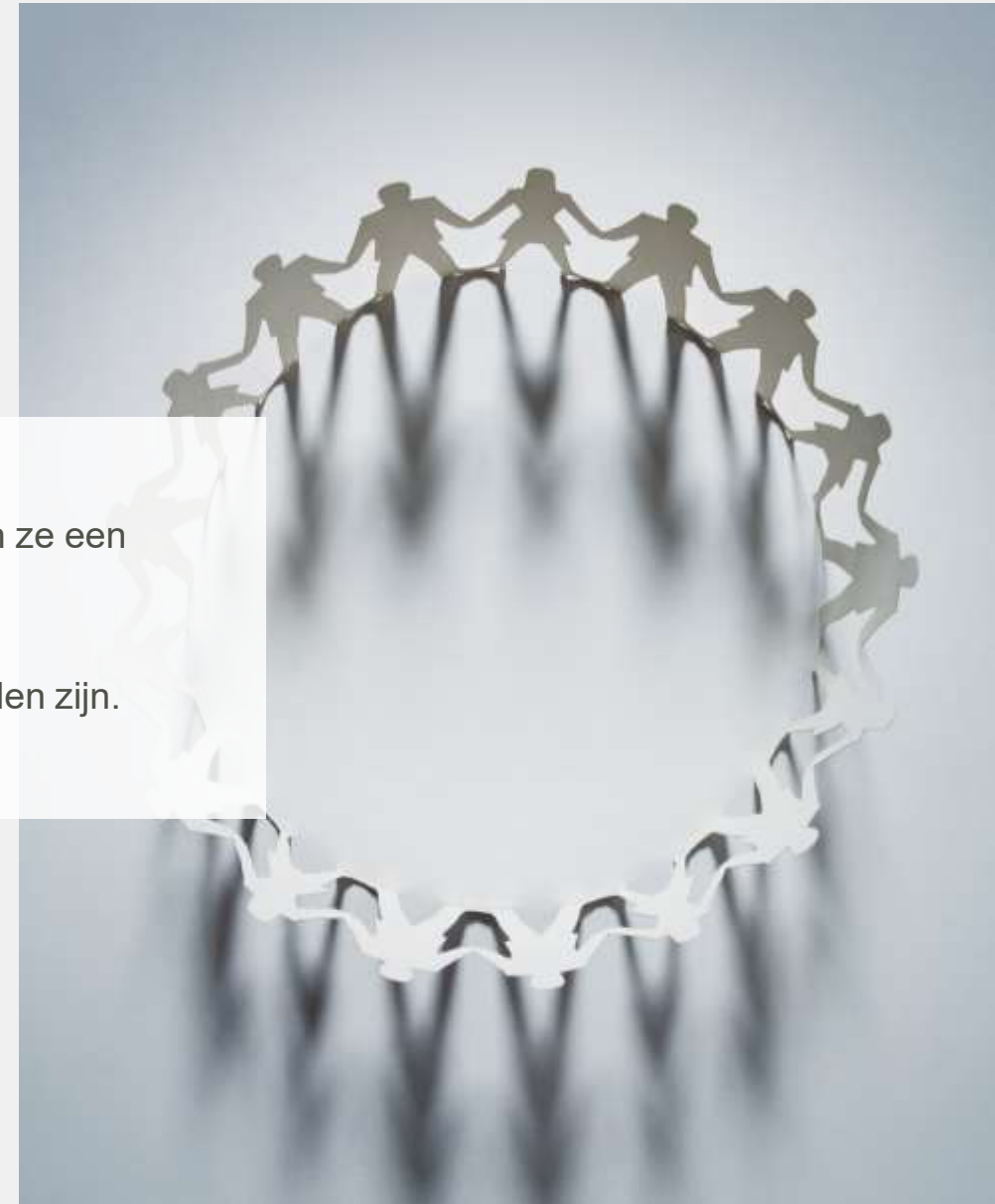
- ❑ **Conditional Access is beleid, geen knop.**
  Het dwingt bestuurlijke keuzes af over risico en verantwoordelijkheid.

- ❑ **Techniek volgt leiderschap.**
  Zonder duidelijke kaders worden technische maatregelen willekeurig of onvolledig.

7 Samen verantwoordelijk

Digitale veiligheid werkt alleen als iedereen zijn rol begrijpt.

Bestuur, ICT, ouders, leveranciers, docenten en leerlingen: allemaal dragen ze een stukje verantwoordelijkheid.
In dit hoofdstuk staat samenwerking centraal — in rollen, communicatie en verwachtingen.
Het laat zien hoe duidelijkheid en dialoog de sterkste beveiligingsmaatregelen zijn.



Digitale veiligheid is nooit een soloactie

Geen enkele school kan haar digitale verantwoordelijkheid alleen dragen.
Zelfs niet met het beste beleid, de meest bekwame ICT-afdeling of de strengste instellingen.
Digitale veiligheid ontstaat pas wanneer **iedere betrokkene** zijn deel van de verantwoordelijkheid begrijpt en ernaar handelt.

Informatiebeveiliging is geen technische discipline, maar een gedeeld systeem van zorg.

Een keten die pas sterk is als elke schakel weet wat zijn rol is — bestuur, ICT, docent, ouder, leerling én leverancier.

De keten van verantwoordelijkheid

De zorgplicht van een school begint bij het bestuur, maar eindigt niet bij de voordeur. Zodra gegevens de klas of de cloud verlaten, raken ook anderen erbij betrokken. Elke partij in die keten heeft een eigen rol, met bijbehorende verwachtingen en grenzen.

Actor	Rol in de keten	Verantwoordelijkheden	Verwachtingen richting school
Schoolbestuur	Verwerkingsverantwoordelijke	Vaststellen van beleid, aanstellen van functionarissen, toezicht op naleving	Transparantie, richting en consistentie
ICT-afdeling / IBP-team	Uitvoering en advisering	Beheer, monitoring, incidentafhandeling, logging	Duidelijke kaders en mandaat
Leveranciers / verwerkers	Technische partners	Naleving verwerkersovereenkomst, veilige hosting, updates, support	Heldere afspraken, tijdige informatie
Ouders	Medeverantwoordelijke in uitvoering	Zorgen voor veilig gebruik thuis, toezicht op leerlingen	Begrijpelijke communicatie, redelijke verwachtingen
Leerlingen	Gebruikers	Zorgvuldig omgaan met schoolaccounts en data	Begrip van regels en gedragscodes

Digitale veiligheid wordt pas duurzaam wanneer al deze partijen weten **waar hun rol begint en eindigt.**

De school als regisseur

De school heeft een unieke positie: ze verbindt alle partijen, maar heeft niet over iedereen directe zeggenschap. Dat vraagt om regie, niet om controle.

Regie betekent:

- verwachtingen uitspreken vóórdat iets misgaat;
- afspraken vastleggen in begrijpelijke taal;
- signalen serieus nemen, ook van buiten de ICT-afdeling.

Een goed functionerend IBP-beleid is daarom evenzeer een **communicatieplan** als een veiligheidsplan. Het maakt afspraken zichtbaar en toegankelijk, zodat iedereen begrijpt wat de bedoeling is.

Ouders als partners

Ouders spelen een cruciale rol bij leerlingdevices, zeker bij modellen waarin eigendom deels bij hen ligt.
Toch worden ze in veel scholen vooral geïnformeerd, niet echt betrokken.

Een volwassen beleid vraagt meer:

- uitleg over *waarom* bepaalde instellingen of beperkingen nodig zijn;
- transparantie over wat de school wel en niet kan zien of beheren;
- duidelijke afspraken over ondersteuning, schade en vervanging.

Ouders willen zelden méér vrijheid; ze willen duidelijkheid.
Wie uitlegt dat beheer niet gaat over wantrouwen, maar over bescherming van leerlinggegevens, krijgt doorgaans steun in plaats van weerstand.

Leveranciers en verwerkers

Leveranciers zijn geen buitenstaanders in het veiligheidsbeleid; ze zijn verlengstuk van de organisatie.
De kwaliteit van beveiliging hangt vaak meer af van hun processen dan van die van de school zelf.

Daarom is het essentieel dat scholen actief toezicht houden op de naleving van verwerkersovereenkomsten. Niet via juridische dreiging, maar via dialoog en periodieke check:

- hoe worden updates en kwetsbaarheden gemeld?
- hoe wordt dataopslag gescheiden per klant?
- wat gebeurt er na afloop van een contract?

Digitale veiligheid is een gedeeld ecosysteem, geen uitbesteed risico.

Leerlingen en medewerkers

Geen technische maatregel weegt op tegen menselijk gedrag. Leerlingen klikken, delen, vergeten — en docenten soms ook. Daarom hoort **bewustwording** evenzeer bij de beveiligingsstructuur als Conditional Access of DLP.

Dat vraagt om concrete acties:

- onboarding waarin digitale veiligheid standaard aan bod komt;
- terugkerende bewustwordingsmomenten (bijv. bij phishingcampagnes of start van het schooljaar);
- een open meldcultuur waarin fouten bespreekbaar zijn.

Wanneer leerlingen leren *waarom* iets niet mag, ontstaat verantwoordelijkheid van binnenuit, niet van bovenaf.

Bestuurlijke borging

Samenwerking is pas duurzaam wanneer ze bestuurlijk geborgd is.
Dat betekent dat rollen en verwachtingen worden vastgelegd in beleid, contracten en overlegstructuren:

- IBP is een vast agendapunt in directie- en teamvergaderingen;
- leveranciers worden jaarlijks geëvalueerd op IBP-criteria;
- ouders worden betrokken bij grote beleidswijzigingen.

Zo ontstaat een cultuur waarin samenwerking niet incidenteel is, maar vanzelfsprekend onderdeel van de digitale organisatie.

Wat bestuurders moeten weten

- **Digitale veiligheid is een ketenverantwoordelijkheid.**
  Succes hangt af van afstemming tussen bestuur, leveranciers, ouders en gebruikers.
- **Regie is belangrijker dan controle.**
  Besturen moeten richting geven, niet micromanagen.
- **Communicatie is preventie.**
  Een goed geïnformeerde ouder of docent is de eerste verdedigingslinie.
- **Bewustwording is beleid.**
  Mensen handelen naar wat ze begrijpen, niet naar wat ze ondertekend hebben.

8 De hybride route

Volwassen beleid zoekt geen perfectie, maar evenwicht.

Tussen volledige centralisatie en vrije BYOD ontstaat een werkbaar midden: de hybride route.
Hierin delen school, ouders en leerlingen eigendom én beheer.
We beschrijven hoe dit model juridisch, technisch en organisatorisch hanteerbaar wordt — zonder de menselijke maat te verliezen.

Realisme als beleid

Soms is het meest volwassen besluit niet het meest ideale, maar het meest realistische. De hybride route is daar een voorbeeld van.
Ze erkent dat scholen verschillende belangen moeten verenigen: beheersbaarheid, betaalbaarheid, autonomie en veiligheid. Geen van die belangen kan volledig winnen, maar samen kunnen ze wel in evenwicht komen.

De hybride strategie is geen compromis uit gemak, maar een **doordachte vertaling van de werkelijkheid naar beleid.**
Ze zegt niet: “Alles mag,” maar ook niet: “Alleen wat wij bezitten is veilig.”
Ze zegt: *veiligheid en vrijheid kunnen samengaan — mits ze gedeeld worden.*

De essentie van de hybride route

In de praktijk betekent de hybride route dat leerlingen een eigen apparaat gebruiken, maar dat de school er gedeeltelijk beheer over uitoefent.
Niet om privédata te zien, maar om de digitale schoolomgeving te beschermen.
Denk aan het installeren van een beveiligingsprofiel, het afdwingen van versleuteling of het blokkeren van lokale opslag van schoolbestanden.

Het eigendom blijft privé, maar de **verantwoordelijkheid is gedeeld**.
Ouders zorgen voor aanschaf en onderhoud, de school voor veilige inrichting en toegangsbeheer.
Die samenwerking vormt het fundament van een volwassen digitale cultuur: duidelijk, uitvoerbaar en toetsbaar.

Waarom dit werkt

De hybride route werkt omdat ze de realiteit niet ontkent, maar vertaalt in beleid.
Ze erkent de verschillen in bezit, gebruik en risico,
en maakt verantwoordelijkheid afhankelijk van context.

Bestuurlijk gezien:

- het bestuur behoudt zijn zorgplicht en aantoonbare naleving van AVG en Normenkader;
- ICT behoudt beheersbaarheid door toegang en beveiliging centraal te regelen;
- ouders behouden keuzevrijheid binnen heldere kaders;
- leerlingen leren werken met veilige instellingen die ook buiten school relevant zijn.

Dat is niet zwak beleid, dat is volwassen bestuur.

Hoe de hybride route eruitziet

Een hybride model krijgt pas waarde als het concreet wordt ingevuld. De volgende bouwstenen vormen samen de praktische inrichting:

1. Afspraken en beleid

- Ouders en leerlingen ondertekenen een overeenkomst waarin staat welke beveiligingsmaatregelen worden toegepast.
- Het beleid beschrijft precies wat de school wél en niet kan doen op het device.
- Alle maatregelen worden vooraf besproken, niet achteraf uitgelegd.

2. Technische inrichting

- Het apparaat wordt via een MDM-profiel geregistreerd bij de school.
- Alleen apparaten die voldoen aan beveiligingscriteria krijgen toegang tot schooldata.
- Via Conditional Access worden gevoelige toepassingen afgeschermd.
- Lokaal opslaan of downloaden van schoolbestanden wordt beperkt of gelogd.

3. Ondersteuning en communicatie

- Ouders krijgen uitleg over de werking van het profiel en de waarborgen voor privacy.
- Leerlingen leren wat de instellingen betekenen en waarom ze bestaan.
- De ICT-afdeling ondersteunt bij installatie en incidenten, zonder toegang tot privébestanden.

4. Evaluatie en toezicht

- Jaarlijkse evaluatie van effectiviteit en draagvlak.
- Rapportage aan bestuur en medezeggenschap over naleving en verbeteringen.
- Periodieke controle of instellingen nog in lijn zijn met beleid en nieuwe technologie.

De voordelen in balans

De hybride route biedt geen perfectie, maar evenwicht. Ze vermindert risico's zonder autonomie te verliezen en verdeelt verantwoordelijkheid zonder onduidelijkheid.

Belang	Wat het hybride model biedt
Beheersbaarheid	Centraal afdwingbare veiligheidsinstellingen en toegangscontrole.
Betaalbaarheid	Aanschaf bij ouders, beperkte structurele kosten voor school.
Veiligheid	Gedeelde verantwoordelijkheid, toezicht op compliance.
Autonomie	Leerlingen gebruiken eigen device, maar binnen veilige kaders.
Bewustwording	Veilig werken wordt een gezamenlijke gewoonte, niet een verplichting.

Het succes van dit model ligt niet in techniek, maar in duidelijkheid: iedereen weet wat hij mag, wat hij moet, en wat de ander doet.

Grenzen en voorwaarden

De hybride route werkt alleen als drie voorwaarden worden vervuld:

- **Transparantie:** alle betrokkenen weten welke rechten en plichten gelden.
- **Toestemming:** ouders en leerlingen stemmen expliciet in met het beheerprofiel.
- **Gelijkwaardigheid:** de school behandelt elk device binnen dezelfde beveiligingsstandaarden.

Zonder deze drie voorwaarden verandert gedeelde verantwoordelijkheid in een grijs gebied — precies wat dit model wil voorkomen.

Een volwassen vorm van vertrouwen

De hybride route is in feite de praktische vertaling van het Zero Trust-principe.

Ze gaat niet uit van goed vertrouwen, maar van **vertrouwen door bewijs**.

Door afspraken, controle en herhaling ontstaat niet wantrouwen, maar rust. Iedereen weet waar hij aan toe is.

Dat is misschien wel de grootste winst:
de veiligheid zit niet alleen in het systeem, maar in de manier waarop mensen er samen verantwoordelijkheid voor dragen.

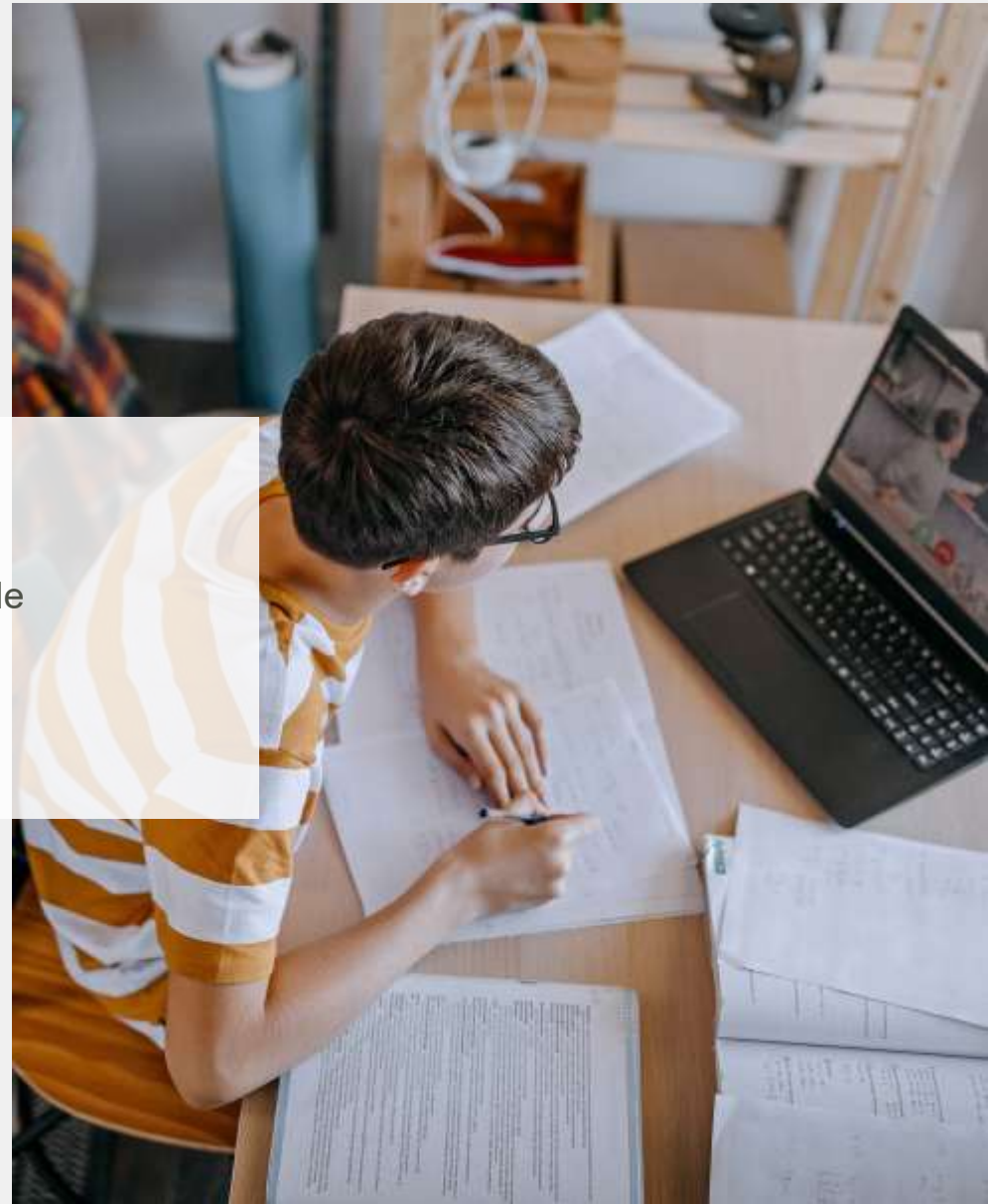
Wat bestuurders moeten weten

- **De hybride route is realistisch beleid.**
  Ze combineert bestuurlijke zorgplicht met uitvoerbare praktijk.
- **Beheer zonder eigendom is mogelijk.**
  Mits juridisch geborgd en technisch ondersteund.
- **Duidelijkheid is de sleutel.**
  Heldere afspraken voorkomen interpretatie en versterken vertrouwen.
- **Vertrouwen is meetbaar.**
  Zero Trust is geen wantrouwen, maar aantoonbare zorgvuldigheid.

9 Van visie naar aantoonbaarheid

Goed bestuur bewijst wat het zegt te doen.

Digitale veiligheid vraagt niet alleen beleid, maar ook bewijs.
We vertalen visie naar processen, rollen en documenten die aantonen dat de organisatie haar verantwoordelijkheid waarmaakt.
Zo groeit beleid uit tot een systeem van leren en verbeteren.



Zichtbaar maken wat goed bestuur doet

Beleid heeft pas waarde als het werkt in de praktijk.
Een school kan nog zo'n mooi IBP-plan hebben — als niet aantoonbaar is *hoe* het wordt toegepast, blijft het papier.
Daarom draait dit hoofdstuk om de bestuurlijke kern van digitale veiligheid: **aantoonbaarheid.**

Aantoonbaarheid is geen wantrouwen of controle, maar een manier om te laten zien dat een organisatie haar zorgplicht serieus neemt. Niet omdat de inspectie dat vraagt, maar omdat goed bestuur transparantie vanzelfsprekend vindt.

Van visie naar structuur

Elke school heeft een visie op digitalisering: leren, werken en organiseren in een moderne omgeving. Maar visie zonder structuur is kwetsbaar. Zodra het bestuur niet kan uitleggen *wie waarvoor verantwoordelijk is*, *hoe beleid wordt bewaakt* en *waar dat zichtbaar wordt*, verliest beleid zijn kracht.

De weg naar aantoonbaarheid kent drie stappen:

- **Van visie naar beleid:**
  uitgangspunten en keuzes worden vastgelegd in beleidsdocumenten (zoals IBP- en devicebeleid).
- **Van beleid naar uitvoering:**
  processen, rollen en afspraken worden ingericht en bekendgemaakt.
- **Van uitvoering naar bewijs:**
  registratie, logging, audits en rapportages tonen aan dat het beleid werkt.

Deze drie niveaus vormen samen de bestuurlijke ruggengraat van digitale veiligheid.

Wat aantoonbaarheid betekent

Aantoonbaarheid is geen extra administratie, maar een manier van werken. Het betekent dat besluiten worden onderbouwd, handelingen worden vastgelegd en verbeteringen worden gemonitord.

Bestuurlijk betekent dit:

- vastgelegde besluiten (raad van bestuur, directie, IBP-overleg);
- aantoonbare risicobeoordeling en keuzes (bijv. DPIA's of risicoanalyses);
- actuele versies van beleid en procedures;
- rapportage over incidenten, datalekken en verbetermaatregelen.

Wie dat op orde heeft, hoeft zich nooit te verdedigen — de structuur spreekt voor zich.

Governance en rollen

Om aantoonbaarheid mogelijk te maken, moet de governance helder zijn:

- **Het bestuur** stelt beleid vast en ziet toe op naleving;
- **De functionaris gegevensbescherming (FG)** bewaakt de onafhankelijkheid en toetst de uitvoering;
- **De IBP-manager met Privacy en Security Officer** vertalen beleid naar processen en bewustwording;
- **De ICT-afdeling** implementeert technische maatregelen en levert bewijs van naleving;
- **Schoolleiding en medewerkers** passen beleid toe en signaleren risico's.

Elk niveau draagt bij aan de keten van bewijs. Geen van deze rollen is optioneel: aantoonbaarheid is een gezamenlijke constructie.

Processen die aantoonbaarheid ondersteunen

Een volwassen organisatie borgt IBP niet via incidentmanagement alleen, maar via een continu proces van *voorkomen, detecteren, reageren en verbeteren.*

Belangrijke processen binnen dat systeem zijn:

- **Incidentmanagement:** melden, registreren, leren.
- **Risicomanagement:** periodiek herzien van dreigingen en maatregelen.
- **Audits en zelfevaluaties:** meten waar de organisatie staat ten opzichte van het Normenkader.
- **Documentbeheer:** actueel houden van beleid, procedures en bijlagen.
- **Bewustwording en training:** jaarlijks vastleggen van deelname en effectiviteit.
- Zo wordt digitale veiligheid geen project, maar onderdeel van de kwaliteitscyclus.

Het belang van audit en feedback

Een audit is geen examen, maar een spiegel. Ze laat zien waar beleid werkt, waar het nog te abstract is en waar gedrag achterblijft. Door jaarlijks intern of extern te laten toetsen, blijft beleid niet alleen aantoonbaar, maar ook actueel.

Aantoonbaarheid betekent immers niet alleen: *we doen het goed,* maar vooral: *we weten wat beter kan.*

Het helpt als bestuurders dit principe expliciet uitdragen. Wie audits ziet als kans in plaats van als verplichting, creëert een cultuur van leren in plaats van verdedigen.

Van compliance naar continu verbeteren

In de meest volwassen organisaties verschuift het gesprek over IBP van *"voldoen we?"* naar *"leren we?"*
Aantoonbaarheid wordt dan een instrument voor groei.

De school gebruikt incidenten en audits om beleid te verbeteren, niet om fouten te vermijden. Dat vraagt om openheid: fouten mogen benoemd worden, zolang er structureel van geleerd wordt.

Volwassenheid is niet dat alles goed gaat,
maar dat alles wat misgaat zichtbaar wordt hersteld.

Daarmee wordt aantoonbaarheid geen papieren bewijs, maar de uitdrukking van een lerende organisatie.

Van structuur naar vertrouwen

Wanneer bestuur, FG, IBP en ICT vanuit deze cyclus samenwerken, ontstaat iets wat geen document kan afdwingen: vertrouwen.
Niet blind vertrouwen, maar vertrouwen gebaseerd op inzicht.

Een school die haar beleid, uitvoering en controle zichtbaar op orde heeft, hoeft niet meer te overtuigen — ze straalt geloofwaardigheid uit.
Dat is de kern van aantoonbare volwassenheid.

Wat bestuurders moeten weten

- **Aantoonbaarheid is bewijs van volwassen bestuur.**
  Het laat zien dat beleid niet vrijblijvend is.
- **Governance is cruciaal.**
  Rollen en processen moeten elkaar versterken, niet overlappen.
- **Audits zijn leermomenten.**
  Ze maken beleid beter en gedrag bewuster.
- **Transparantie wekt vertrouwen.**
  Niet de afwezigheid van fouten, maar de aanwezigheid van inzicht maakt een organisatie geloofwaardig.

ossewold.net

10

Digitale geletterdheid en toekomstgericht beleid

Wie veilig wil werken, moet leren wat veiligheid betekent.

Digitale geletterdheid is meer dan vaardigheid: het is bewustzijn.
In dit hoofdstuk koppelen we de nieuwe kerndoelen aan devicebeleid en laten we zien hoe scholen leerlingen voorbereiden op een wereld waarin technologie en verantwoordelijkheid hand in hand gaan.

Veilig leren in een digitale wereld

Digitalisering in het onderwijs is geen bijzaak meer; het *is* de omgeving waarin leren plaatsvindt.
Toch is er één hardnekkig misverstand: dat digitale geletterdheid vooral een vak erbij is, terwijl het in werkelijkheid een **voorwaarde voor veilig leren** vormt.

Leerlingen kunnen pas veilig en kritisch omgaan met technologie als de school die veiligheid zichtbaar waarborgt. Beleid en onderwijs zijn daarin twee kanten van dezelfde medaille. Het één schept de randvoorwaarden, het ander geeft ze betekenis.

De school als digitale oefenplaats

Een school is niet alleen een plek om kennis over te dragen, maar ook om te leren *hoe* je verantwoord deelneemt aan een digitale samenleving.
Daar hoort bij dat leerlingen leren wat privacy betekent, hoe data werken en waarom beveiliging niet “iets van ICT” is, maar van iedereen.

Elke instelling is daarmee een oefenplaats:

- een plek waar leerlingen leren omgaan met accounts, wachtwoorden en identiteit;
- waar zij ervaren wat gedeelde verantwoordelijkheid inhoudt;
- waar digitale keuzes zichtbaar consequenties hebben.

De kwaliteit van digitale geletterdheid hangt dus niet alleen af van het curriculum, maar van de **cultuur van de organisatie**.

De nieuwe kerndoelen

De conceptkerndoelen voor digitale geletterdheid maken deze samenhang expliciet.
Ze onderscheiden vier domeinen:

- **Informatievaardigheden** – kunnen vinden, beoordelen en gebruiken van digitale informatie;
- **Mediawijsheid** – begrijpen hoe media werken en invloed uitoefenen;
- **Computational thinking** – kunnen redeneren met digitale systemen;
- **Digitale zelfredzaamheid en ethiek** – verantwoord, veilig en bewust omgaan met technologie.

Voor elk van deze domeinen geldt: zonder betrouwbare infrastructuur en veilig devicegebruik kan de leerling deze doelen niet duurzaam ontwikkelen.

Digitale geletterdheid vraagt dus niet alleen om lesmateriaal, maar om **toegang tot een veilige digitale leeromgeving.**

De rol van devicebeleid

Devicebeleid is, hoe technisch het ook klinkt, in feite onderwijskundig beleid.
Het bepaalt of leerlingen in een betrouwbare omgeving kunnen leren, communiceren en reflecteren.
Een onveilig of onbeheerd device ondermijnt niet alleen privacy, maar ook het vertrouwen in leren met technologie.

Daarom moet in toekomstgericht beleid worden vastgelegd:

- dat digitale veiligheid en digitale geletterdheid elkaar versterken;
- dat leerlingen leren *waarom* beveiliging nodig is;
- dat de school verantwoordelijkheid neemt voor de omgeving waarin dat leren gebeurt.

Met andere woorden:
devicebeleid is een vorm van didactiek.
Het leert leerlingen dat veiligheid niet ontstaat uit regels, maar uit bewust handelen.

De competenties van de toekomst

De maatschappij vraagt niet alleen om digitale vaardigheden, maar om digitaal bewustzijn: het vermogen om te begrijpen welke sporen je achterlaat, welke keuzes technologie beïnvloeden en hoe je verantwoordelijkheid neemt voor je eigen handelen.

Dat begint niet in de samenleving, maar in de klas. Daar leren leerlingen dat veiligheid en vrijheid elkaar niet uitsluiten, maar elkaar juist mogelijk maken.

“Digitale vrijheid zonder verantwoordelijkheid is roekeloosheid; verantwoordelijkheid zonder vrijheid is stilstand.”

Toekomstgericht beleid zoekt steeds de balans tussen die twee.

De betekenis voor bestuur en beleid

Voor bestuurders betekent dit dat digitale geletterdheid niet langer een onderwijsinnovatie is, maar een **strategisch thema**. Het raakt aan infrastructuur, professionalisering, privacy, burgerschap en zorgplicht.

Een toekomstgericht schoolbestuur formuleert beleid dat:

- digitale geletterdheid verankert in visie en kwaliteitszorg;
- devicebeleid en lespraktijk verbindt;
- professionalisering van personeel structureel meeneemt;
- evaluatie en bewustwording onderdeel maakt van de jaarcyclus.

Zo groeit de school niet alleen in compliance, maar in cultuur.

Een lerende organisatie

De scholen die digitaal het verst zijn, hebben één ding gemeen: ze zien technologie niet als project, maar als **onderdeel van leren**. Hun IBP-beleid is geen los document, maar een levend kompas.

Ze weten dat elke leerling, docent en ouder onderdeel is van het beveiligingsbeleid — niet omdat dat moet, maar omdat het werkt. Zo wordt digitale geletterdheid geen apart hoofdstuk, maar de rode draad van de toekomst.

Wat bestuurders moeten weten

- **Digitale geletterdheid is veiligheidsbeleid.**
  Leren en beschermen horen bij elkaar.
- **Devicebeleid is didactiek.**
  Het bepaalt hoe veilig en bewust leerlingen leren werken.
- **Bestuurders zijn cultuurdragers.**
  Hun keuzes bepalen of veiligheid een plicht blijft of een vanzelfsprekendheid wordt.
- **Toekomstgericht beleid verbindt techniek en mens.**
  Wie dat doet, maakt van digitalisering geen risico, maar een kracht.

11 Kosten, gelijkheid en haalbaarheid

Veiligheid kost geld — maar onveiligheid kost vertrouwen.

Een volwassen beleid is ook financieel realistisch.
We verkennen de verdeling van kosten tussen school en ouders, de risico's van ongelijkheid en manieren om beleid haalbaar en rechtvaardig te houden.
Transparantie blijkt daarbij de beste vorm van zekerheid.

Verantwoordelijkheid heeft ook een prijs

Beleid is pas geloofwaardig als het betaalbaar en uitvoerbaar is.
Digitale veiligheid mag dan een principiële opdracht zijn, ze vraagt ook om realistische keuzes over middelen, bekostiging en verdeling. Wie beleid maakt zonder die realiteit te erkennen, schrijft geen plan maar een wens.

In dit hoofdstuk gaat het niet over geld als obstakel, maar als **onderdeel van verantwoordelijkheid.** Een veilige digitale omgeving is niet gratis, maar wel onmisbaar. En wie wil dat leerlingen gelijke kansen hebben, moet ook zorgen dat de toegang tot technologie niet afhankelijk wordt van inkomen of toeval.

De prijs van veiligheid

Digitale veiligheid kent directe en indirecte kosten:

- aanschaf of lease van devices;
- licenties en beheerplatformen;
- beveiligingssoftware, back-up, logging;
- scholing en ondersteuning van medewerkers;
- communicatie en oudervoorlichting.

Geen enkele school kan al die kosten alleen dragen zonder keuzes te maken. Daarom is het belangrijk dat bestuurders deze kosten niet zien als ICT-post, maar als **strategische investering in onderwijscontinuïteit.**

Net zoals een brandverzekering vanzelfsprekend is, zo zou ook structurele investering in digitale veiligheid vanzelfsprekend moeten zijn.

Eigendom en kostenverdeling

De verdeling van kosten volgt meestal de verdeling van eigendom. Maar zodra het device onderdeel wordt van de schoolomgeving, wordt ook de bekostigingsvraag een gezamenlijke verantwoordelijkheid.

Model	Aanschaf	Beheer en onderhoud	Verzekering	Toegangsbeheer
Schooldevice	School	School	School	School
Managed BYOD	Ouders	Gedeeld (school + leverancier)	Ouders (met afspraken)	School
Hybride light	Ouders	Ouders	Ouders	School
Vrije BYOD	Ouders	Ouders	Ouders	Gebruiker

Het gaat hierbij niet om “wie betaalt de laptop”, maar om *wie verantwoordelijk is voor de continuïteit van leren als er iets misgaat.* Een goed ingericht model zorgt dat geen leerling buiten de boot valt bij schade, verlies of financiële beperkingen.

Gelijkheid en toegang

Digitalisering biedt kansen, maar vergroot ook verschillen. Wie thuis een moderne laptop, stabiel netwerk en digitale ondersteuning heeft, heeft een voorsprong op leerlingen die dat niet hebben.

Daarom hoort bij elk devicebeleid ook een **gelijke-kansenparagraaf.** Besturen moeten expliciet vastleggen:

- hoe zij omgaan met gezinnen die de kosten niet kunnen dragen;
- welke leen- of garantiefaciliteiten beschikbaar zijn;
- hoe zij voorkomen dat “veiligheid” een luxe wordt.

Echte gelijkheid gaat verder dan gelijke apparaten. Het gaat om gelijke toegang tot leren, zonder dat veiligheid of privacy op achterstand raken.

Bekostiging en samenwerking

Veel scholen staan voor dezelfde financiële dilemma's. Daarom ontstaan steeds vaker samenwerkingsvormen met leveranciers, gemeenten of stichtingen. Denk aan:

- gezamenlijke aanbestedingen of leasingconstructies;
- beheer in coöperatieve vorm (bijv. via SIVON of andere onderwijsnetwerken);
- regionale afspraken over reparatie, vervanging en service.

Dergelijke samenwerkingen maken schaalvoordelen mogelijk en verlagen de administratieve last. Maar ze vragen wél bestuurlijke sturing: de verantwoordelijkheid blijft bij de school, ook als uitvoering gedeeld wordt.

De balans tussen ambitie en haalbaarheid

Niet elk bestuur kan, of hoeft, direct naar het hoogste volwassenheidsniveau van het Normenkader te groeien. Belangrijker is een **realistisch groeipad**: stap voor stap verbeteren, zodat beleid duurzaam blijft in plaats van overbelastend.

Een goed devicebeleid:

- groeit mee met de financiële ruimte;
- maakt prioriteiten zichtbaar (bijv. eerst toegangsbeheer, dan devicebeheer);
- communiceert helder wat wél en nog niet gerealiseerd is.

Volwassen beleid is eerlijk over zijn grenzen.
Niet alles tegelijk doen, maar alles bewust doen.

Bestuurlijke keuzes in perspectief

Bij de afweging tussen kosten, gelijkheid en veiligheid spelen altijd drie waarden mee:

- **Rechtvaardigheid** – elk kind verdient dezelfde bescherming;
- **Doelmatigheid** – middelen worden ingezet waar ze het meest effect hebben;
- **Duurzaamheid** – beleid moet houdbaar zijn in tijd en geld.

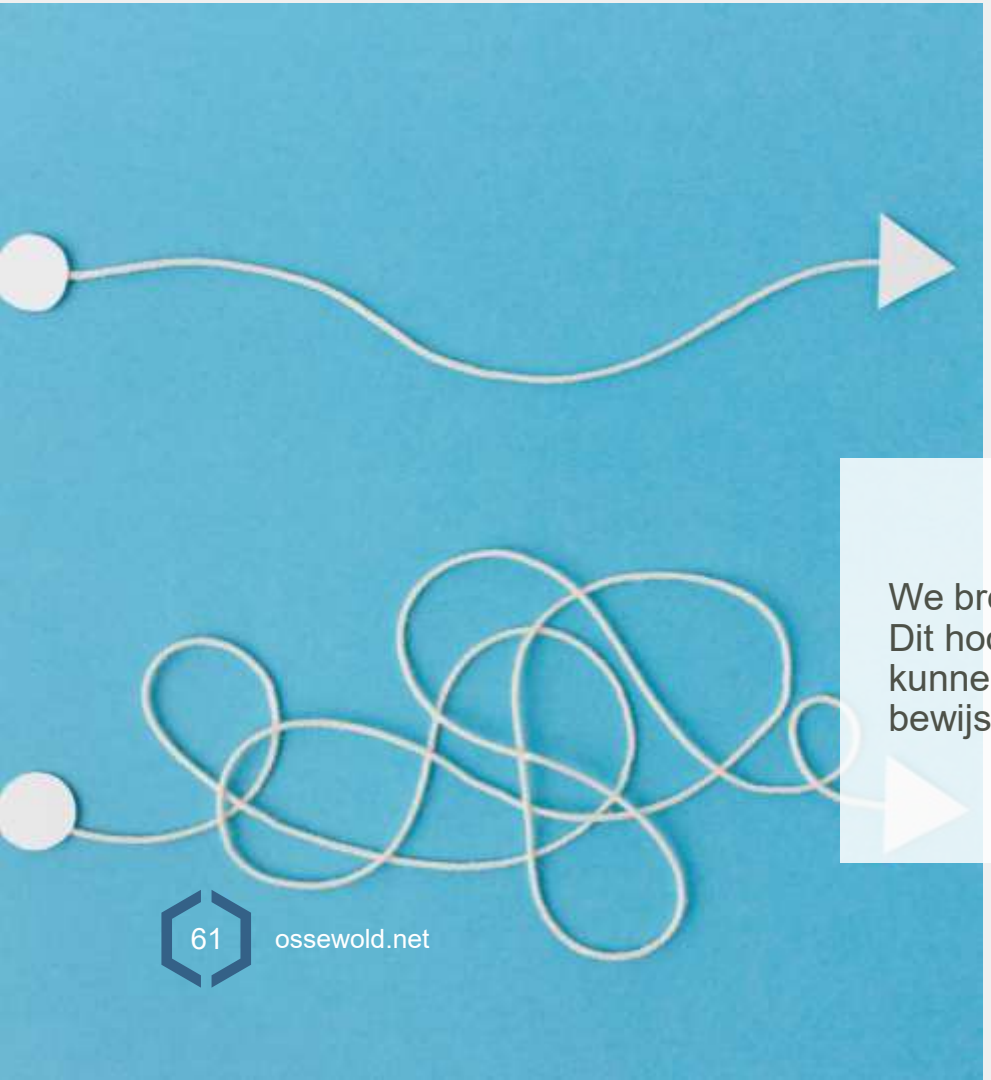
Die drie waarden helpen bestuurders om keuzes te verantwoorden, ook wanneer middelen beperkt zijn of prioriteiten moeten schuiven.

Een besluit dat uitlegbaar is, is verdedigbaar.

Wat bestuurders moeten weten

- ❑ **Digitale veiligheid is een structurele investering.**
  Niet incidenteel, maar onderdeel van de onderwijskosten.
- ❑ **Kosten en verantwoordelijkheid horen bij elkaar.**
  Wie beleid voert, moet zorgen voor realistische bekostiging.
- ❑ **Gelijkheid vraagt om concrete waarborgen.**
  Geen leerling mag buiten het digitale systeem vallen.
- ❑ **Ambitie zonder haalbaarheid verzwakt vertrouwen.**
  Bouw beleid op groeipaden, niet op beloften.

ossewold.net



12 Conclusie en handelingskader

Verantwoordelijkheid is geen last, maar een keuze.

We brengen alle inzichten samen in vijf principes en drie scenario’s.
Dit hoofdstuk biedt een handelingskader waarmee besturen verantwoordelijkheid kunnen vertalen naar concrete stappen — van visie naar uitvoering, van beleid naar bewijs.

Van beleid naar volwassenheid

De vraag *“Wie is verantwoordelijk voor leerlingdevices?”* lijkt eenvoudig, maar blijkt bij nader inzien de kern te raken van volwassen digitaal bestuur. Want eigendom, zorgplicht en vertrouwen lopen niet vanzelf gelijk.

Dit boek heeft laten zien dat verantwoordelijkheid geen bezit is, maar een houding — bestuurlijk, organisatorisch én menselijk. Wie haar serieus neemt, kijkt verder dan techniek en kosten. Die ziet digitale veiligheid als voorwaarde voor goed onderwijs.

Digitale volwassenheid betekent dat beleid, techniek en gedrag elkaar versterken. Dat een school niet alleen *voldoet*, maar ook *begrijpt* waarom. Dat is de stap van compliance naar cultuur — en die stap maakt het verschil.

De vijf bestuurlijke inzichten

Door alle hoofdstukken heen keren vijf inzichten telkens terug. Samen vormen ze het fundament van elk toekomstbestendig devicebeleid:

- **Verantwoordelijkheid is niet overdraagbaar.**
  De school blijft verwerkingsverantwoordelijke, ongeacht wie het device bezit.
- **Beleid bepaalt techniek, niet andersom.**
  De keuze voor systemen volgt uit bestuurlijke uitgangspunten, niet uit leveranciers.
- **Zorgplicht is gelaagd.**
  Beheer, toegang en gedrag moeten elkaar versterken.
- **Samenwerking is de sleutel.**
  Ouders, leerlingen en leveranciers maken deel uit van één veiligheidsketen.
- **Transparantie schept vertrouwen.**
  Aantoonbaarheid is geen verplichting, maar een vorm van geloofwaardigheid.

Wie deze vijf principes hanteert, bouwt niet alleen een veilig systeem, maar een organisatie die digitaal volwassen is.

Drie scenario's in bestuurlijk perspectief

Geen enkele school start op hetzelfde punt. Daarom is het zinvol om te werken met drie bestuurlijke scenario's: niet als etiket, maar als hulpmiddel om koers te bepalen.

Scenario	Kenmerk	Risico-profiel	Aanbevolen stappen
A. Basisveiligheid (minimaal)	Vrije of hybride light BYOD; beperkte beheersing	Hoog	Start met beleid en bewustwording; stel minimumeisen voor toegang en opslag.
B. Gedeelde verantwoordelijkheid (volwassen)	Managed BYOD; gedeeld beheer via MDM of profiel	Beheersbaar	Borg afspraken juridisch; implementeer Conditional Access, evalueer jaarlijks
C. Volledige beheersing (geavanceerd)	Schooldevices of centrale lease; uniform beheer	Laag	Verfijn governance, automatiseer rapportages, focus op continue verbetering

Elk scenario kent eigen kansen, kosten en risico's. De volwassenheid van beleid zit niet in het model, maar in de onderbouwing van de keuze.

Het handelingskader voor besturen

Een bestuur dat vandaag wil beginnen, hoeft geen groot project te starten. Wat telt, is structuur.

Onderstaande handreiking biedt een concreet startpunt voor groei.

Stap 1 – Stel uitgangspunten vast

- Beschrijf visie en verantwoordelijkheid rond eigendom, zorgplicht en veiligheid.
- Formuleer het gewenste volwassenheidsniveau op basis van het Normenkader.

Stap 2 – Richt beleid in

- Combineer IBP-, ICT- en devicebeleid tot één consistent geheel.
- Benoem rollen (bestuur, IBP-manager, FG, ICT, schoolleiding).
- Leg afspraken met ouders en leveranciers schriftelijk vast.

Stap 3 – Organiseer beheer

- Maak inzichtelijk wat centraal geregeld is en wat gedeeld wordt.
- Pas Zero Trust-principes toe: toegang op basis van identiteit en context.
- Voer audits uit om naleving te toetsen.

Stap 4 – Investeer in bewustwording

- Zorg dat medewerkers en leerlingen begrijpen waarom maatregelen bestaan.
- Communiceer jaarlijks met ouders over beleid en verantwoordelijkheid.

Stap 5 – Evalueer en verbeter

- Gebruik incidenten, audits en evaluaties als leermomenten.
- Herzie beleid jaarlijks en rapporteer over voortgang.
- Zo wordt beleid geen document, maar een proces van continue groei.

De stap vooruit

De scholen die het verschil maken, zijn niet per se de scholen met de meeste middelen. Het zijn de scholen die durven kiezen: voor duidelijkheid, voor samenwerking en voor lerend bestuur.

Digitale veiligheid is geen eindpunt, maar een manier van werken.
Een volwassen organisatie weet dat fouten kunnen gebeuren, maar zorgt dat ze zichtbaar, herstelbaar en leerzaam zijn.

In die houding ligt de echte toekomstbestendigheid: niet in techniek of regels, maar in vertrouwen — het vertrouwen dat ontstaat wanneer beleid en praktijk elkaar versterken.

Slotgedachte

De vraag *“van wie is het device?”* blijkt uiteindelijk een spiegel te zijn.
Niet voor techniek, maar voor volwassenheid.

“Wie verantwoordelijk wil zijn voor leren, moet ook verantwoordelijkheid durven nemen voor de digitale wereld waarin dat leren plaatsvindt.”

Slotwoord – De verantwoordelijkheid die we delen

Toen ik aan dit boek begon, dacht ik vooral na over techniek, beleid en verantwoordelijkheid. Maar gaandeweg merkte ik dat het onderwerp veel dieper gaat. Het raakt aan vertrouwen, aan zorg, aan volwassenheid — woorden die in het onderwijs eigenlijk heel vanzelfsprekend zouden moeten zijn.

Want achter elke laptop, achter elke beleidsregel en achter elke norm zit uiteindelijk een mens. Een leerling die wil leren, een docent die wil begeleiden, een ouder die zich betrokken voelt, een bestuurder die het goed wil doen. Dat besef maakt digitale veiligheid niet lichter, maar wel betekenisvoller.

Ik heb geprobeerd een brug te slaan tussen die werelden: tussen de taal van bestuur en de realiteit van de klas, tussen techniek en gedrag, tussen regels en vertrouwen. Niet om antwoorden te geven die voor iedereen gelden, maar om een kader te bieden waarbinnen scholen hun eigen antwoorden kunnen vinden.

Mijn hoop is dat dit boek bijdraagt aan dat gesprek — eerlijk, kritisch en met respect voor elkaars rol. Dat we verantwoordelijkheid niet langer zien als last, maar als uitdrukking van professionaliteit en zorg voor elkaar.

De digitale wereld verandert sneller dan ons beleid kan bijhouden. Maar wat niet verandert, is de opdracht die we delen: onderwijs bieden dat veilig, rechtvaardig en toekomstgericht is. Dat vraagt niet alleen kennis van technologie, maar vooral aandacht voor mensen.

“*Uiteindelijk draait digitale volwassenheid niet om systemen, maar om mensen.*”

Paul Ossewold, november 2025

Belangrijke begrippen in de context van dit eboek

TERM	*BETEKENIS*
AVG	*Algemene Verordening Gegevensbescherming*; Europese privacywet die regels stelt aan het verwerken van persoonsgegevens.
Back-up	Veiligheidskopie van gegevens om verlies of verstoring te voorkomen.
Beleid IBP	Vastgelegd beleid voor informatiebeveiliging en privacy; bepaalt verantwoordelijkheden, processen en controle.
BYOD	*Bring Your Own Device*; beleid waarbij leerlingen hun eigen apparaat gebruiken binnen afgesproken schoolkaders.
Cloud	Digitale omgeving waarin data en applicaties via internet worden opgeslagen en beheerd.
Digi-competenties	Digitale geletterdheid en vaardigheden die nodig zijn om veilig, bewust en effectief te leren en werken.
DPIA	*Data Protection Impact Assessment*; verplichte risicoanalyse bij verwerkingen met een hoog privacyrisico.
Devicebeheer	Technisch en organisatorisch beheer van laptops of tablets, inclusief beveiliging, updates en toegang.
FG	*Functionaris voor de Gegevensbescherming*; onafhankelijke toezichthouder die naleving van de AVG bewaakt.
IAM	*Identity & Access Management*; systeem voor het beheren van gebruikers, rollen en toegangsrechten.
IBP-manager	Functionaris die beleid voor informatiebeveiliging en privacy coördineert en borgt binnen het bestuur.
Intune	Microsoft-omgeving voor centraal apparaat- en toegangsbeheer, vaak gebruikt bij BYOD of hybride modellen.
MDM	*Mobile Device Management*; systeem waarmee apparaten worden geregistreerd en beveiligingsinstellingen worden afgedwongen.
Microsoft 365 (M365)	Cloud-omgeving van Microsoft voor e-mail, documenten en samenwerking, inclusief beveiligingsfuncties.
Normenkader IBP FO	Landelijke set van 22 normen (15 voor informatiebeveiliging en 7 voor privacy) voor scholen in het funderend onderwijs.
PO	*Privacy Officer*; medewerker die toeziet op uitvoering van het privacybeleid en naleving van de AVG.
Risicomanagement	Proces van het herkennen, beoordelen en beheersen van risico's rond informatiebeveiliging en privacy.
Security Officer (SO)	Functionaris die verantwoordelijk is voor technische en organisatorische beveiligingsmaatregelen.
Serverloze school	ICT-architectuur waarbij lokale servers zijn vervangen door cloud-diensten; beheer en data zijn online centraal geregeld.
Tenant	Afgesloten cloud-omgeving binnen Microsoft 365 waarin gebruikers, rechten en data van één organisatie worden beheerd.
Verwerkersovereenkomst	Overeenkomst tussen school (verwerkingsverantwoordelijke) en leverancier (verwerker) over gebruik en beveiliging van persoonsgegevens.
Zero Trust	Bestuurs- en beveiligingsprincipe: niemand krijgt automatisch toegang; identiteit, apparaat en context worden altijd gecontroleerd.

Colofon

Titel: *Wie is verantwoordelijk voor leerlingdevices?*
Auteur: Paul Ossewold
Uitgave: ossewold.net – Advies & Programma's voor digitaal onderwijs
Eerste editie: november 2025
Redactie en vormgeving: Paul Ossewold met assistentie van ChatGPT (OpenAI)
Afbeeldingen: Microsoft stock images
Publicatie: Digitale uitgave (PDF / e-boek)

Voor meer informatie, contact en updates:
ossewold.net
info@ossewold.net

Disclaimer

Dit boek is met zorg samengesteld, maar pretendeert geen juridische of onfeilbare waarheid te bieden.
De inhoud is gebaseerd op praktijkervaring, actuele inzichten uit het onderwijsveld en publiek beschikbare informatie over de AVG en het Normenkader IBP FO.

De auteur is geen jurist; de teksten zijn bedoeld als **handvat** voor scholen, bestuurders en ICT-professionals om intern het gesprek te voeren over verantwoordelijkheid, beleid en beveiliging rond leerlingdevices.
Gebruik dit boek als inspiratiebron, niet als juridisch advies.

Hoewel de informatie met de grootst mogelijke zorgvuldigheid is verzameld, kunnen aan de inhoud geen rechten worden ontleend.
Voor specifieke interpretaties of juridische toetsing wordt aanbevolen advies in te winnen bij de Functionaris Gegevensbescherming of een gespecialiseerd jurist.

Met kennis als fundament, passie als drijfveer en groei als doel — voor een veiliger en bewuster digitaal onderwijs.