HANDREIKING
DE ROL VAN DE RVT BIJ DIGITALE VEILIGHEID

Versie: december 2024

VTOI NVTK PO RAAD VO RAAD Bit by Bit Samen voor digitaal veilig onderwijs

INLEIDING

In deze handreiking gaan we in op de manier waarop het intern toezicht kan toezien op de digitale veiligheid van onderwijsinstellingen en kinderopvangorganisaties. Deze handreiking maakt onderdeel uit van een serie handreikingen waarin de belangrijkste aspecten van het intern toezicht in het onderwijs en de kinderopvang worden behandeld.

"Digitale veiligheid is een onderwerp dat regelmatig oppopt, maar daarmee niet per definitie top of mind is. Het belang wordt wel gevoeld, maar het onderwerp dringt zich niet op. Wat je wilt voorkomen is dat het top of mind wordt door een probleem. Dan heb je het al snel over een hack en ben je te laat. Zorg dat je aan de preventieve kant zit, niet aan de curatieve kant."

Mario Verbeek, Lid RvT Zuiderbos, Lid RvT Dongemond College

OPZET

In deze handreiking wordt in het eerste deel beschreven wat het belang is van toezien op digitale veiligheid en de verantwoordelijkheden van de Raad van Toezicht.
In het tweede deel leggen we uit wat het Normenkader Informatiebeveiliging en Privacy (IBP) inhoudt. Hoewel dit Normenkader ontwikkeld is voor het funderend onderwijs, bevat het ook interessante elementen voor andere sectoren, zoals de kinderopvang. Daarnaast bieden we een gespreksleidraad met essentiële vragen en onderwerpen voor de dialoog. We eindigen de handreiking met praktische tips en onderwerpen die je kunt bespreken met de bestuurder.

WAT IS DIGITALE VEILIGHEID EN WAT IS HET NIET?

Digitale veiligheid is een brede term. In deze handreiking richten we ons op informatiebeveiliging en privacy. Bij informatiebeveiliging hebben we het over het beveiligen van alle data waar je als organisatie of instelling mee werkt, en bij privacy bedoelen we het goed en veilig omgaan met gegevens over personen; gegevensbescherming. Privacy wordt voor een groot gedeelte geregeld in de Algemene Verordening Gegevensbescherming (AVG).

Een beveiligingsincident of datalek kan grote gevolgen hebben voor de leerlingen, hun ouders, leraren en het imago van de instelling – en daarmee dus ook voor de toezichthouder. Dat maakt dit een belangrijk thema.

Inhoud

1 **WAAROM TOEZIEN** OP DIGITALE VEILIGHEID?

2 **HET NORMENKADER INFORMATIEBEVEILIGING EN PRIVACY (IBP)** VOOR HET ONDERWIJS

3 **PRAKTIJKVOORBEELD** STICHTING CARMELCOLLEGE

4 **DE ROL VAN DE INTERN TOEZICHTHOUDER:** WAAR KUN JE OP LETTEN?

5 **BESPREEKPUNTEN** MET BESTUURDERS

6 **VERDER LEZEN** OVER DIGITALE VEILIGHEID

WAAROM TOEZIEN OP DIGITALE VEILIGHEID?

Digitale veiligheid is een steeds belangrijker aspect in het dagelijks leven, en dus ook in het onderwijs en de kinderopvang. De fysieke en digitale wereld lopen steeds meer in elkaar over, waardoor incidenten vaker een digitaal component kennen. Met de toename van digitale middelen en online platforms in het onderwijs en de kinderopvang, komt ook de verantwoordelijkheid om deze omgevingen veilig te houden voor alle betrokken partijen. Het is daarom belangrijk om digitale veiligheid integraal te benaderen in het veiligheidsbeleid en -plan. Van belang hierbij is dat de bestuurder inzicht heeft in de risico's en kwetsbaarheden.

WAAROM IS DIT BELANGRIJK?

1. **Het bestuur is eindverantwoordelijk** voor goed (digitaal) onderwijs en digitale veiligheid. De interne toezichthouder bevraagt de bestuurder hoe deze verantwoordelijkheid wordt ingevuld.
2. **Bescherming van persoonlijke gegevens:** Scholen en kinderopvangorganisaties verzamelen en verwerken veel gevoelige informatie van minderjarigen. Het is van belang dat deze gegevens goed beschermd worden tegen ongeoorloofde toegang en dat het onderwijs/de opvang en de werkzaamheden ook door kunnen gaan in geval van een incident. Daarnaast kun je een boete krijgen van de Autoriteit Persoonsgegevens (AP) als je de beveiliging van de gegevens van de leerlingen/kinderen en ouders niet goed op orde hebt. Hetzelfde geldt als je overige verplichtingen van de AVG niet naleeft.
3. **Sociale, fysieke en digitale veiligheid:** De fysieke en digitale wereld lopen steeds meer in elkaar over. Digitale leermiddelen en platforms worden steeds meer geïntegreerd in het dagelijks leven. Het is belangrijk om oog te hebben voor de risico's die dat met zich meebrengt.

4 **Wettelijke verplichtingen:** Instellingen moeten voldoen aan wet- en regelgeving zoals de Algemene Verordening Gegevensbescherming (AVG). Uit deze wetgeving vloeit ook de verplichting om voldoende passende organisatorische en technische maatregelen te nemen om deze gegevens te beschermen. Hetzelfde geldt voor kinderopvangbesturen: ook voor hen is de AVG verplicht en is gegevensbescherming belangrijk.

5 **Vertrouwen en reputatie:** Een inbreuk op digitale veiligheid kan leiden tot verlies van vertrouwen bij ouders, leerlingen en medewerkers, wat een langdurige negatieve impact kan hebben op de reputatie van de organisatie.

6 **De digitale dreiging neemt toe:** Denk aan phishing e-mails, ransomware en andere cyberaanvallen. Het is niet meer de vraag of je gehackt wordt, maar wanneer. Het is van belang om voorbereid te zijn, een crisisplan te hebben en hiermee te oefenen, maar het is ook van belang om de kans op een incident te verkleinen door (basis) maatregelen te nemen zoals back-ups en segmentatie. Als er dan een incident is, is de (financiële, materiële en immateriële) schade beperkt en kan de organisatie sneller herstellen. Meer informatie in het Dreigingsbeeld Funderend Onderwijs.

"Als toezichthouder breng je de buitenwereld naar binnen. Het is belangrijk om digitale veiligheid en privacy onder de aandacht te brengen, het op de agenda te zetten en er vragen over te stellen. Ga het gesprek aan, maar waak ervoor om niet op de stoel van de bestuurder te gaan zitten. Het bestuur is verantwoordelijk voor de digitale veiligheid en het waarborgen van de privacy. Zij dient te zorgen voor een plan en de uitvoering hiervan. Als RvT houd je toezicht en monitor je de voortgang."

- Angela van der Plas, Lid RvT Stichting De Linge

2

NORMENKADER INFORMATIE-BEVEILIGING EN PRIVACY (IBP) VOOR HET ONDERWIJS

Met de toenemende digitalisering in het onderwijs, nemen ook de dreigingen en privacyrisico's toe. Een datalek kan ervoor zorgen dat gegevens van kinderen, leerlingen, ouders en medewerkers op straat komen te liggen én dat je systemen platliggen, waardoor lessen niet kunnen doorgaan. Daarom werkt de onderwijssector toe naar één norm voor digitaal veilig onderwijs: het Normenkader Informatiebeveiliging en Privacy voor het onderwijs[1]. Het Normenkader IBP beschrijft wat scholen moeten doen om informatiebeveiliging en privacy op orde te krijgen. Hoewel het Normenkader ontwikkeld is voor het funderend onderwijs, bevat het ook relevante elementen voor andere sectoren, zoals de kinderopvang.

INFORMATIEBEVEILIGING

De normen voor informatiebeveiliging helpen om je instelling goed te beschermen tegen digitale dreigingen van binnen en buiten je organisatie. Door de normen toe te passen, bescherm je jouw systemen – en dus je onderwijs/kinderopvang – tegen uitval, ongeoorloofde toegang en verstoringen. Overkomt het je toch? Dan ben je voorbereid en weet je hoe je moet handelen. De normen zijn onderverdeeld in verschillende domeinen.

De domeinen van informatiebeveiliging:

Domein 1: Bestuur
Domein 2: Organisatie
Domein 3: Risicomanagement
Domein 4: Personeelsbeheer
Domein 5: Configuratiemanagement
Domein 6: Incident- en problem-management
Domein 7: Changemanagement
Domein 8: Systeemontwikkeling
Domein 9: Datamanagement
Domein 10: Identity- en access-management
Domein 11: Securitymanagement
Domein 12: Fysieke beveiliging
Domein 13: It-operatie
Domein 14: Bedrijfscontinuïteits-management
Domein 15: Ketenbeheer

[1] Het Normenkader IBP is ontwikkeld in samenwerking met het onderwijs en op initiatief van het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en de VO-raad.

PRIVACY
Met de toenemende digitalisering in het onderwijs en de kinderopvang, nemen ook de privacyrisico's toe. Door het gebruik van kind- of leerlingvolgsystemen, adaptieve leermiddelen en apps in de klas of de groep worden steeds meer gegevens verwerkt. De normen voor privacy gaan over de bescherming van persoonsgegevens. Aan de hand van de AVG zijn concrete maatregelen gemaakt die je als school/opvang moet nemen om aan deze wet te voldoen.

De domeinen van privacy:

Domein 1: Beleid
Domein 2: Processen
Domein 3: Organisatorische inbedding
Domein 4: Rechten van betrokkenen
Domein 5: Samenwerking
Domein 6: Beveiliging
Domein 7: Verantwoording

GROEIPAD
Het Normenkader IBP is omvangrijk en vraagt veel van schoolbesturen. Het kan lastig zijn om te bepalen waar je moet beginnen. Daar helpt het Groeipad bij. Het Groeipad is een wegwijzer door het Normenkader IBP, zodat besturen stapsgewijs de digitale veiligheid in hun school op orde kunnen brengen. Waar kun je het beste mee starten? Wat doe je daarna? Afhankelijk van waar de organisatie of instelling staat, kun je instappen in een van de fasen van het Groeipad. Als intern toezichthouder is het belangrijk om te weten dat zo'n groeipad bestaat, zodat je daarover met je bestuurder in gesprek kunt over de te nemen stappen.

DE ROL VAN DE INTERN TOEZICHTHOUDER
Een hack of incident kan een grote impact hebben op de financiële positie, op de continuïteit van het onderwijs of de opvang en op de (digitale) veiligheid van leerlingen en medewerkers. Informatiebeveiliging en privacy moeten daarom een integraal onderdeel zijn van de organisatie of instelling. Als RvT is het belangrijk dat je het onderwerp op de agenda zet - als het bestuur dit (nog) niet doet - en geregeld vragen stelt aan de bestuurder. Vraag daarbij ook door als het antwoord niet concreet genoeg is.

Toezicht houden op digitale veiligheid in de kinderopvang en het onderwijs komt in hoge mate overeen. De doelgroep betreft in beide gevallen minderjarige kinderen/leerlingen en daarom is het extra belangrijk om de gegevens van deze groep te beschermen. Ook wil je de gegevens van medewerkers beschermen en de continuïteit van je organisatie borgen. Zowel kinderopvang als scholen hebben te maken met systemen zoals kind- of leerlingvolgsystemen, oudercommunicatieapps en digitale werk- en leerplatformen. Digitale dreigingen zoals cyberaanvallen of hacks komen voor in heel Nederland, dus ook in de kinderopvang of het onderwijs. Het Dreigingsbeeld Funderend Onderwijs biedt meer inzicht in de type dreigingen en voorbeelden uit de praktijk.

DE FUNCTIONARIS GEGEVENSBESCHERMING (FG)
Sinds de invoering van de AVG in 2018 is het voor scholen verplicht om een FG aan te stellen. Ook binnen de kinderopvang kan het raadzaam zijn om een FG aan te stellen. Deze functionaris heeft een interne toezichthoudende rol op naleving van de AVG. Om deze rol goed te kunnen vervullen is het van belang dat de FG een onafhankelijke positie heeft in de organisatie en dat deze rol niet gecombineerd wordt met uitvoerende taken. De FG rapporteert aan het schoolbestuur. Tip: nodig de FG uit om in gesprek te gaan met de RvT over de bevindingen en bespreek het jaarlijkse verslag van de FG.

Meer informatie over de rol en positie van de FG

PRAKTIJKVOORBEELD
STICHTING CARMELCOLLEGE

DIGITALE VEILIGHEID VEREIST NAUWE SAMENWERKING TUSSEN RAAD VAN TOEZICHT EN BESTUUR

Het waarborgen van digitale veiligheid is uitdagend en een nauwe samenwerking tussen de Raad van Toezicht (RvT) en het Bestuur van onderwijsinstellingen kan daarbij behulpzaam zijn. Stichting Carmelcollege is een goed voorbeeld van hoe deze samenwerking in de praktijk vorm krijgt. In een uitgebreid interview delen Jan Kees Meindersma, bestuurder bij Carmel, en Oscar van Leeuwen, RvT-lid en voorzitter van de auditcommissie, hun inzichten en ervaringen rondom digitale veiligheid binnen hun schoolorganisatie.

Zowel Meindersma als Van Leeuwen benadrukken dat digitale veiligheid een gezamenlijke verantwoordelijkheid is, die niet alleen rust op de schouders van het Bestuur of de IT-afdeling. “Het is belangrijk dat er binnen de hele organisatie een gedeeld besef is van het belang van digitale veiligheid,” zegt Meindersma. “We moeten ervoor zorgen dat dit onderwerp niet alleen op de agenda staat, maar dat er ook echt naar wordt gehandeld.”

De Raad van Toezicht speelt een cruciale rol in het waarborgen van de digitale veiligheid binnen Carmel. Volgens Van Leeuwen is het de taak van de auditcommissie om continu te monitoren of de organisatie voldoende in control is: “Onze auditcommissie bestaat uit leden van de RvT, bestuurders van Carmel, enkele schooldirecteuren en de verantwoordelijken voor de bedrijfsvoering. Dit brede perspectief zorgt ervoor dat we IT-onderwerpen vanuit verschillende hoeken kunnen bekijken en dat we een goed beeld krijgen van de daadwerkelijke impact van beslissingen.”

Meindersma waardeert de kritische maar ondersteunende rol van de RvT: “Als bestuurder ben je verantwoordelijk voor de uitvoering, maar het is waardevol als de RvT je helpt om de juiste vragen te stellen. Bijvoorbeeld: waarom nemen we drie jaar de tijd om een bepaald niveau van digitale veiligheid te bereiken? Welke risico’s lopen we als we die tijd nemen? Die kritische vragen zorgen ervoor dat we scherp blijven en de juiste keuzes maken.”

Lees hier het volledige interview

4

DE ROL VAN DE INTERN TOEZICHTHOUDER

WAAR KUN JE OP LETTEN

1 BORG REGELMATIGE BIJSCHOLING EN INFORMATIEVOORZIENING

- Zorg dat je als toezichthouder op de hoogte blijft van de laatste ontwikkelingen op het gebied van digitale veiligheid. Dit kan door deelname aan seminars, webinars, het volgen van een opleiding via de VTOI-NVTK Academie of het lezen van relevante publicaties.
- Werk nauw samen met het bestuur om ervoor te zorgen dat je regelmatig wordt geïnformeerd over de status van digitale veiligheid binnen de organisatie.
- Bevraag en maak afspraken over hoe de bestuurder werkt aan de eigen professionalisering. Bespreek ook die van de medewerkers. Hoe blijven zij op de hoogte van de ontwikkelingen en houden ze kennis up-to-date?

2 VERANKER INFORMATIEBEVEILIGING EN PRIVACY IN HET INTERN TOEZICHT EN HET BELEID

- Digitale veiligheid moet een vast onderdeel zijn van het algemene risicomanagement van de organisatie. Dit betekent dat er structureel aandacht aan wordt besteed in het reguliere toezicht.
- Stel iemand binnen het intern toezicht aan als dossierhouder voor toezicht op digitale veiligheid. Uiteraard blijft het onderwerp de eindverantwoordelijkheid van het bestuur.
- Zet het thema op de RvT-agenda. Bijvoorbeeld op het moment dat er visie, strategie en beleid wordt ontwikkeld. Besteed aandacht aan het thema op vaste momenten in het jaar, denk aan het bestuursverslag en de rapportage van de accountant, en neem het mee in het onderwerp risicomanagement.

3 WEES PROACTIEF EN KRITISCH

- Wacht niet tot er problemen ontstaan, maar wees proactief in het stellen van vragen en het evalueren van de huidige maatregelen.
- Blijf kritisch en vraag door waar nodig. Digitale veiligheid is complex en vraagt voortdurende aandacht.

4 BETREK ALLE STAKEHOLDERS

- Digitale veiligheid is niet alleen de rol of taak van de medewerkers informatiebeveiliging, privacy en IT; Bewustwording is belangrijk in alle lagen van de organisatie. Betrek daarom ook leerkrachten, pedagogisch medewerkers, managers, ouders en leerlingen/kinderen in gesprekken over digitale veiligheid, bijvoorbeeld via de (G)MR.
- Vraag om inzicht in de governance van informatiebeveiliging en privacy: zijn rollen, taken en verantwoordelijkheden belegd en hoe werkt het in de praktijk?
- Organisaties zijn verplicht om een Functionaris Gegevensbescherming (FG) aan te stellen. Is er een FG? En is er sprake van functiescheiding tussen de controlerende en de uitvoerende taken?
- Informatiebeveiliging en privacy raken alle domeinen in de organisatie: denk aan HR, financiën, facilitair, ICT, inkoop en onderwijs. Zijn de verantwoordelijkheden bij domein- of proceseigenaren belegd?
- Sluit aan op de jaarcyclus van de organisatie of instelling: komt het onderwerp periodiek terug in de jaarkalender? Zie erop toe dat dit thema meegenomen wordt in de planning & control-cyclus: denk aan het (meerjaren)plan, de begroting, monitoring en verantwoording. Informatiebeveiliging en privacy zijn vanaf 2024 een verplicht onderdeel in het jaarverslag.

"Wees je ervan bewust hoe kwetsbaar digitale systemen zijn in de organisatie. En controleer ook of de verantwoordelijken voor het beheer voldoende bekwaam zijn. Het Normenkader IBP doet iemand er niet zomaar even bij."

- Kees Sluis, Toezichthouder Ceder Scholengroep Amsterdam-Amstelveen

5 BESPREEKPUNTEN MET BESTUURDERS

1 BRENG HET GESPREK OP GANG

- In hoeverre zijn jullie op de hoogte van de ontwikkelingen rond het Normenkader Informatiebeveiliging en Privacy? (Indien van toepassing)
- Hoe werken jullie daaraan? Volgen jullie het groeipad of een eigen roadmap?
- Op welk volwassenheidsniveau bevindt het schoolbestuur zich nu en hoe weet je dat? En wat is de ambitie in het groeipad naar een volgend volwassenheidsniveau?

2 VRAAG NAAR DE GOVERNANCE

- Hoe hebben jullie de verantwoordelijkheden voor informatiebeveiliging en privacy in de organisatie belegd?
- Hoe is de FG gepositioneerd? Is er sprake van functiescheiding tussen controlerende en uitvoerende taken? Wordt het verslag van de FG gedeeld en besproken met de RvT?
- Hoe zorgen jullie ervoor dat het meer is dan alleen een onderwerp voor de IT-afdeling, maar dat juist ook verantwoordelijken in andere afdelingen (HR, financiën, facilitair, ICT, inkoop en onderwijs) hun rol vervullen?

3 BESPREEK IN GEVAL VAN MEERDERE LOCATIES EN EEN BESTUURSBUREAU

- Lukt het om centraal de regie te voeren op digitale veiligheid?
- Stellen jullie beleid hiervoor als bestuur vast, en hoe gaan de locaties daar dan mee om?

4 INFORMEER NAAR DE PRIORITERING

- Welke dreigingen baren jullie de meeste zorgen?
- Hoe werkt dat door in de prioritering van jullie maatregelen?
- Baseren jullie de risico's op het 'Dreigingsbeeld Funderend Onderwijs'?

5 CHECK HOE HET BELEID IN DE PRAKTIJK UITPAKT

- Hoe houden jullie zicht op de naleving van het beleid omtrent digitale veiligheid?
- Hoe staat die naleving ervoor?
- Wat zijn belangrijke hordes om die naleving te verbeteren? (Tip: nodig bij dit punt eventueel ook een interne verantwoordelijke of toezichthouder op dit vlak uit, zoals de adviseur informatiebeveiliging of de FG)

6 BEVRAAG DE PLAATS DIE INFORMATIEBEVEILIGING EN PRIVACY INNEEMT BIJ INKOOP

- Welk deel van de ict van de organisatie is uitbesteed?
- Hoe zorgen jullie ervoor dat informatiebeveiliging en privacy bij de aanschaf van ict-diensten en (digitale) leermiddelen consequent en op tijd ter sprake komen?
- Hebben jullie met alle leveranciers verwerkersovereenkomsten afgesloten?

7 BESPREEK HET BELEID EN DE STRATEGIE

- Heeft de organisatie een actueel beleid voor informatiebeveiliging en privacy? Hoe wordt dit beleid gehandhaafd?
- Is er een strategie voor informatiebeveiliging en privacy op lange termijn, en hoe wordt deze geïntegreerd in het algemene risicomanagement?

- Wordt het beleid en de uitvoering geëvalueerd? Zijn er rapportages? Hoe legt het bestuur verantwoording af in bijvoorbeeld het jaarverslag?

8 VRAAG NAAR DE RISICOANALYSE EN INFORMATIEBEVEILIGING EN PRIVACY-MAATREGELEN

- Welke risicoanalyses worden uitgevoerd rond informatiebeveiliging en privacy? Worden deze periodiek herzien?
- Hoe zijn risico's van ketenpartners – zoals leveranciers en ICT-dienstverleners– in beeld gebracht? En hoe controleert het schoolbestuur deze ketenpartners en leveranciers?
- Worden persoonsgegevens buiten de Europese Economische Ruimte (EER) verwerkt, zijn persoonsgegevens in te zien van buiten de EER en zo ja, gebeurt dit op een rechtmatige manier?
- Is de toegang tot gevoelige informatie goed beheerd? Is duidelijk wie toegang heeft tot welke data en hoe dit wordt gecontroleerd?

9 INFORMEER NAAR HET INCIDENTMANAGEMENT EN RESPONS

- Is er een incidentenresponsplan voor het geval van een digitale veiligheidsinbreuk? Hoe vaak wordt dit plan getest en bijgewerkt?
- Zijn er recente incidenten geweest en hoe zijn deze afgehandeld? Welke lessen zijn geleerd?

10 VRAAG NAAR BEWUSTWORDING EN TRAINING

- Hoe worden medewerkers bewust gemaakt en gehouden van informatiebeveiliging en privacy? Welke trainingen of cursussen worden aangeboden?
- Hoe worden leerlingen en ouders betrokken bij het bevorderen van informatiebeveiliging en privacy?

- Hoe transparant communiceert de organisatie over de verwerkingen van persoonsgegevens, bijvoorbeeld in de privacyverklaring en in jaarverslagen?

11 BESPREEK DE SAMENWERKING EN EXTERNE EXPERTISE

- Met welke externe partijen werkt de organisatie samen op het gebied van informatiebeveiliging en privacy? Wordt er in de regio samengewerkt met andere schoolbesturen?

12 INFORMEER NAAR COMPLIANCE EN AUDITS

- Hoe wordt ervoor gezorgd dat de organisatie voldoet aan relevante wet- en regelgeving op het gebied van IBP?
- Worden er regelmatig self-assesments of audits uitgevoerd om de naleving van normen te controleren?

13 GA IN GESPREK OVER DILEMMA'S

- *Als schoolorganisatie moet je zorgen dat je functioneren niet in gevaar komt. Je moet dus veel doen aan informatiebeveiliging en privacy. Het blijft wel zoeken naar de balans tussen goed onderwijs verzorgen en 100% voldoen aan alle veiligheidsnormen. De lumpsum is beperkt.*

  – Kees Sluis, Toezichthouder Ceder Scholengroep Amsterdam-Amstelveen

6

VERDER LEZEN
OVER DIGITALE VEILIGHEID

VOOR TOEZICHTHOUDERS

- Het Dreigingsbeeld Funderend Onderwijs is dé bron om hoog-over geïnformeerd te worden over relevante IBP-dreigingen en risico's in de sector.

- Het Sectorbeeld Onderwijs van de Autoriteit Persoonsgegevens laat zien hoe de privacytoezichthouder naar het onderwijs kijkt, en kan daarmee ook inzicht bieden in hun prioriteiten bij het toezicht.

- Op het gebied van privacy heeft de Autoriteit Persoonsgegevens een goede handreiking voor de RvT. Daar staan veel nuttige voorbeeldvragen in.

VOOR HET SCHOOLBESTUUR *(maar ook bestuurders in kinderopvang kunnen hier nuttige informatie vinden)*

- De overzichtspagina van het programma DVO biedt inzicht in het bestaande ondersteuningsaanbod voor schoolbesturen, zodat je als toezichthouder weet waar je organisatie bij kan aansluiten.

- Het Normenkader Informatiebeveiliging en Privacy beschrijft wat scholen moeten doen om informatiebeveiliging en privacy op orde te krijgen. Bij het normenkader zijn ook een Groeipad en hulpmiddelen ter ondersteuning.

De handreiking Sturen op Digitale veiligheid – IBP in de Jaarcyclus. Deze interactieve handreiking ondersteunt besturen om regie te pakken en bevat een visualisatie om IBP mee te nemen in de planning & controlcyclus.

TRAININGEN VOOR TOEZICHTHOUDERS

- Toezicht op ict en digitale transformatie
- Toezicht op digitalisering
- Toezicht op privacy en gegevensbescherming

TRAININGEN VOOR BESTUURDERS

- Leertraject Regie op digitalisering
  → aanmelden PO via PO-Academie
  → aanmelden VO via VO-academie

COLOFON
Versie: december 2024

De handreiking 'De rol van de RvT bij digitale veiligheid' is ontwikkeld door de PO-Raad, VO-raad en VTOI-NVTK in samenwerking met Kennisnet, als onderdeel van programma Digitaal Veilig Onderwijs.

Digitaal Veilig Onderwijs:
Met het programma Digitaal Veilig Onderwijs bundelen het ministerie van OCW, Kennisnet, SIVON, de PO-Raad en VO-raad hun krachten voor een onderwijssector waarin iedere leerling digitaal veilig kan leren en medewerkers digitaal veilig kunnen werken. Het programma biedt schoolbesturen en leveranciers heldere leidraden en een concreet ondersteuningsaanbod. Zo kunnen zij voldoen aan hun verantwoordelijkheid om een digitaal veilige organisatie te realiseren. Stap voor stap, Bit by Bit.

Met speciale dank aan:
Mario Verbeek, Kees Sluis, Jan Kees Meindersma, Oscar van Leeuwen, Mieke Boas, Frank Haenen, Angela van der Plas en Bernice Ruiter.