CYBERWEER-BAARHEID IN HET PO EN VO

INHOUD

WAAROM AANDACHT VOOR CYBERWEERBAARHEID?

Het belang om leerlingen digitaal geletterd te maken wordt steeds duidelijker. Leerlingen volgen het nieuws via Tiktok, staan continu met elkaar in verbinding via sociale media, stellen iedere vraag die ze hebben aan ChatGPT en gebruiken de hele dag door apps en apparaten die gebruik maken van artificial intelligence. Sinds de komst van de conceptkerndoelen op het gebied van digitale geletterdheid (SLO, 2024b) zijn veel basisscholen en middelbare scholen eerste stappen aan het zetten om structureel aandacht te besteden aan digitale geletterdheid. Cybercrime krijgt echter nog weinig aandacht tijdens lessen over digitale geletterdheid. Thema's als whats-app gebruik en betrouwbare informatie online vinden krijgen meer aandacht (SLO, 2024a).

Een van de conceptkerndoelen richt zich echter specifiek op veiligheid en privacy (SLO, 2024b), waaruit blijkt dat aandacht voor het veilig omgaan met digitale systemen, data en privacy wel een belangrijk onderdeel is van digitale geletterdheid (zie afbeelding 1). Ook in veel andere conceptkerndoelen komt de verbinding met online veiligheid en privacy indirect terug. Het kritisch leren beoordelen van informatiebronnen (onderdeel kerndoel 2) helpt bijvoorbeeld leerlingen niet in de val te lopen van cyberaanvallen die gebruik maken van misleiding. Een ander voorbeeld is dat begrip over AI mechanismen leidt tot een vergroot bewustzijn over privacy en hoe kwaadwillende (zoals hackers) data kunnen misbruiken.

Kerndoel 3 – veiligheid en privacy

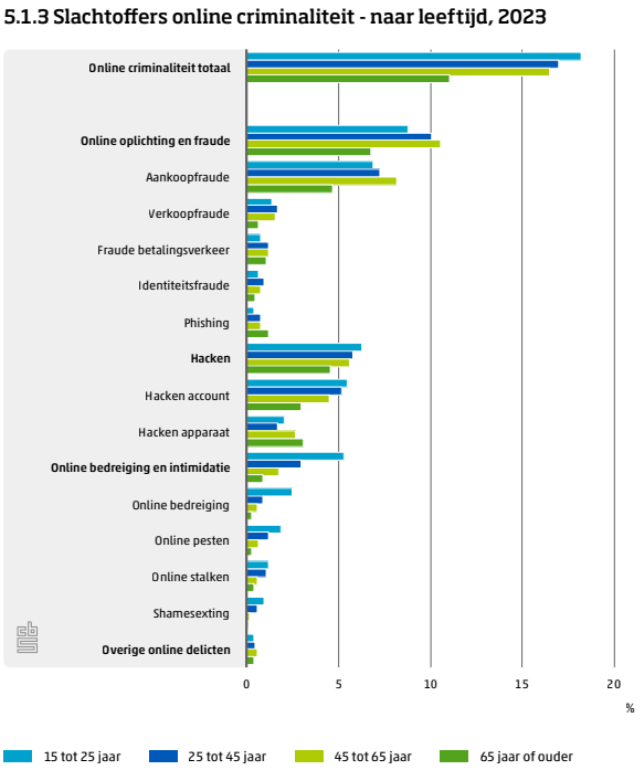
Doelzin PO:	**Doelzin onderbouw VO:**
De leerling gaat veilig om met digitale systemen, data en de privacy van zichzelf en anderen.	De leerling gaat veilig om met digitale systemen, data en de privacy van zichzelf en anderen.
Het gaat hierbij om:	**Het gaat hierbij om:**
• herkennen van veiligheidsrisico's bij het gebruik van digitale systemen en data; • veilig gebruiken van digitale systemen, data en informatie, en passende technische maatregelen nemen om deze te beschermen; • wegen van dilemma's bij het delen van zowel eigen persoonsgegevens, data, informatie en digitale content als die van anderen; • adequaat omgaan met ongepaste content, ongepast gedrag en veiligheidsrisico's in digitale omgevingen.	• kennis hebben van rechten en plichten van individuen en instellingen ten aanzien van de bescherming van persoonsgegevens, data en privacy; • herkennen van veiligheidsrisico's bij het gebruik van digitale systemen van bedrijven, instellingen en overheden; • beschermen tegen zwakke plekken in gebruikte digitale systemen en netwerken; • herkennen hoe anderen omgaan met privacy en de veiligheid van door hen verzamelde of bewaarde data; • adequaat omgaan met ongepaste content, ongepast gedrag en veiligheidsrisico's in digitale omgevingen.

Afbeelding 1: Kerndoel 3 – Veiligheid en privacy. SLO

Cyberweerbaarheid: wat houdt het in?

Digitale en cyberweerbaarheid verwijst naar het vermogen van een persoon om adequaat te reageren op en zichzelf succesvol aan te passen tijdens een cyberincident en veilig en bewust om te gaan met persoonsgegevens (Lee & Hancock, 2023). Dit omvat vier verschilende aspecten, namelijk: (1) kunnen begrijpen wanneer je (digitale) risico's loopt, (2) weten wat te doen en weten hoe hulp te zoeken, (3) leren van opgedane ervaringen en (4) het hebben van gepaste ondersteuning om te kunnen herstellen (Manning, 2021)

Ondanks dat cybercrime nog weinig aandacht krijgt in het onderwijs, nemen de zorgen over de online veiligheid van jongeren wél toe bij zowel ouders als onderwijsprofessionals. Veel ouders maken zich bijvoorbeeld zorgen over de digitale (on)veiligheid van hun kinderen (Wissink, 2021). Dit is niet onterecht: Jongeren blijken het meest slachtoffer te worden van online criminaliteit in vergelijking met oudere leeftijdsgroepen (zie afbeelding 2). Professionals uit het onderwijs die betrokken zijn bij project Digitaal Niet Te Foppen geven aan dat leerlingen vaak al vroeg risico lopen op het gebied van online veiligheid en privacy. Daarnaast zien zij dat leerlingen regelmatig meer op de hoogte zijn van hetgeen wat op het gebied van online criminaliteit mogelijk is dan volwassenen. Ook kan online pesten of bijvoorbeeld het creëren van een nepprofiel voor veel onrust in de klas zorgen. Genoeg reden volgens hen om pro actief in te zetten op de cyberweerbaarheid van leerlingen.



Afbeelding 2: Veiligheidsmonitor 2023. CBS (2024).

Om digitale en cyberweerbaarheid van leerlingen te vergroten moet er met regelmaat gewerkt worden aan verschillende vaardigheden van de leerling. Alleen het overdragen van kennis op het gebied van veiligheid en privacy blijkt hierin onvoldoende. Leerlingen moeten onder andere digitale vaardigheden ontwikkelen om effectief door de digitale wereld te kunnen navigeren. Daarnaast moeten zij vertrouwen ontwikkelen in hun eigen technologische vaardigheden (*self-efficacy)*. Ook moeten zij getraind worden om een medestander te zijn voor hun leeftijdgenoten die online gevaar lopen. En tot slot moeten de leerlingen leren hoe en waar zij terecht kunnen voor hulp (Lee & Hancock, 2021).

AAN DE SLAG MET CYBERWEERBAARHEID

Wanneer je als school structureel en terugkerend aandacht wil geven aan cyberweerbaarheid, is het van belang om goed af te wegen op welke wijze je dit wilt doen. Hieronder geven we drie verschillende mogelijkheden om samen met je team af te wegen, aangevuld met voor- en nadelen volgens (basis- en middelbare) scholen die deelnemen aan project Digitaal Niet Te Foppen en in de praktijk al actief aan de slag zijn met cyberweerbaarheid op hun school.

1. Integratie van het thema cyberweerbaarheid in andere vakken

Wanneer je kiest voor integratie met andere vakken kun je samen met je team onderzoeken welke subthema's je aandacht wil geven als het gaat om cyberweerbaarheid, om vervolgens na te gaan welke al bestaande inhouden van vakken hiermee in verbinding staan. Voorbeelden van subthema's op het gebied van cyberweerbaarheid zijn bijvoorbeeld phishing, hacken, online stalken en fraude. In het basisonderwijs zijn bijvoorbeeld verbindingen te maken met lessen die je geeft over waarden en normen tijdens wereldoriëntatie onderwijs of met lessen gericht op de sociaal-emotionele ontwikkeling van leerlingen. Ook het begrijpend leesonderwijs biedt mogelijkheden, door leerlingen teksten te laten lezen die over onlnie veiligheid en privacy gaan. In het voortgezet onderwijs zijn voor de hand liggende verbindingen te maken met het vak informatiekunde en maatschappijleer. Bekijk vervolgens welke lesmaterialen aansluiten bij het bestaande onderwijsaanbod. Op de website van Wikiwijs vind je een overzicht van beschikbare lesmaterialen op het gebied van cyberweerbaarheid.

> "Wij zien kansen om cyberweerbaarheid aandacht te geven wanneer we het nieuws met leerlingen bespreken. We spelen tijdens onze lessen regelmatig in op de actualiteiten, bijvoorbeeld tijdens Nieuwsbegrip. Onze leerkrachten zouden dan wel nog meer inzicht nodig moeten hebben in de doelen op het gebied van digitale geletterdheid, om hier op zo'n moment ook bewust op in te kunnen spelen".
>
> PO Talisman, SKPO

Voor- en nadelen van deze manier van werken volgens de scholen:

- Aandacht aan cyberweerbaarheid geven tijdens al bestaande lessen kan zorgen voor meer betekenisvol onderwijs, bijvoorbeeld doordat de inhoud aansluit bij een thema waar je met de leerlingen al uitgebreid aandacht voor hebt.
- Leerlingen zijn consequent(er) met cyberweerbaarheid bezig doordat het thema tijdens meerdere momenten, binnen verschillende vakken aan bod komt.
- Op deze wijze aandacht besteden aan cyberweerbaarheid geeft geen extra druk op het lesrooster.
- Doelbewust integreren met andere vakken vraagt veel kennis over en inzicht van de onderwijsprofessional in de doelen op het gebied van digitale geletterdheid.

2. Het organiseren van op zichzelf staande (gast)lessen over cyberweerbaarheid

Er zijn verschillende lesmaterialen beschikbaar om op zichzelf staande lessen over cyberweerbaarheid te geven aan leerlingen. Met je team kun je een afweging maken welk materiaal het beste bij jullie past qua inhoud, duur, frequentie, vorm en doelgroep. Sommige lesmaterialen zullen zich bijvoorbeeld meer focussen op een kennisbasis, terwijl ander materiaal een accent heeft gelegd op uitwisseling en interactie over de inhoud. Door dit bewust na te gaan en te overwegen, sluit je uiteindelijke keuze aan bij jullie visie op onderwijs. Bekijk hiervoor het aanbod op de website van Wikiwijs of navigeer direct naar het lesaanbod van bijvoorbeeld HackShield, De Kiesraad of MijnCyberrijbewijs. Het is ook mogelijk om gastlessen door bijvoorbeeld de politie, GGD of bureau HALT te organiseren.De Kiesraad of MijnCyberrijbewijs. Het is ook mogelijk om gastlessen door bijvoorbeeld de politie, GGD of bureau HALT te organiseren.

> "Per periode zou je bijvoorbeeld een dag kunnen organiseren waarin je met behulp van bestaand lesmateriaal en gastdocenten alle brugklassen een les kunt geven over een subthema van cyberweerbaarheid. Als dit eenmaal is georganiseerd vraagt het weinig voorbereiding van jou als docent en kun je toch 8 onderwerpen per jaar bespreekbaar maken met leerlingen".
>
> VO Mezzo Elzendaal Gennep

Voor- en nadelen van deze manier van werken volgens de scholen:

- Door te werken met op zichzelf staande lessen wordt het gemakkelijker om verschillende subthema's op het gebied van cyberweerbaarheid te borgen. Met behulp van een duidelijke planning en goede afspraken kun je ervoor zorgen dat alle thema's aan bod komen.
- Bij complexere subthema's kun je gastdocenten (bijv. een wijkagent) vragen om een les te geven. Zij hebben de expertise én kunnen bevlogen over het thema in gesprek gaan met leerlingen.
- Deze manier van werken vraagt om het vrijmaken van tijd in het lesrooster en het maken van een goede planning wat betreft eventuele betrokkenheid van gastdocenten. Dit is in de praktijk soms lastig om te realiseren.

3. Aandacht voor cyberweerbaarheid tijdens een projectweek

Met behulp van een projectweek kun je op een intensievere wijze tijdens een aantal lesdagen in een afgesproken periode het thema cyberweerbaarheid aandacht geven. Je kunt hierbij overwegen om aan te sluiten bij bekendere projectweken, zoals de Week van de Mediawijsheid, de Week van de Veiligheid of 'Safer Internet Day'. Het is ook mogelijk om aan te sluiten bij thematische (project)weken vanuit bestaande lesmethodes of zelf projectweken te organiseren. Bespreek vervolgens met elkaar welk lesmateriaal het best aansluit bij de betreffende projectweek.

> "Een projectweek zou als voordeel kunnen hebben dat je de hele school echt in beweging kunt zetten rondom dit thema en ook ouders actief kunt betrekken".
>
> PO De Achtbaan - SKPO

Voor- en nadelen van deze manier van werken volgens de scholen:

- Tijdens een bestaande projectweek hebben leerlingen en hun ouders vaak vanzelfsprekender aandacht voor de digitale wereld. Er is bijvoorbeeld aandacht voor het onderwerp in het nieuws, tijdens tv-programma's of in reclames.
- Tijdens een projectweek heb je met je hele team dezelfde focus. Dit maakt het gemakkelijker om elkaar te helpen en onderling uit te wisselen, omdat je allemaal op hetzelfde moment aan het voorbereiden bent en het project uitvoert.
- Meerdere projectweken in een schooljaar organiseren rondom dit thema is bijna niet mogelijk. Leerlingen worden tijdens een projectweek dus wel ondergedompeld, maar wel maar eenmalig gedurende het schooljaar. Hierdoor kun je je afvragen of je hetgeen wat je de leerlingen wilt leren ook daadwerkelijk beklijft.

PLAN VOOR DE PRAKTIJK

Wanneer je bewust en kritisch hebt nagedacht over de wijze waarop je structureel en terugkerend aandacht wil besteden aan cyberweerbaarheid, kun je je overwegingen vertalen naar een plan voor de praktijk. Hieronder vind je vijf praktische tips om dit plan handen en voeten te geven.

Tip 1

Maak twee teamleden verantwoordelijk voor de organisatie en de uitvoering van het plan. Samen kom je verder en heb je meer slagkracht om het e.e.a. daadwerkelijk te organiseren.

Tip 2

Zet de afspraken die je maakt helder op papier. In bijlage 1 hebben we een voorbeeld toegevoegd wat je hiervoor kunt gebruiken. De digitale versie van dit document kun je vinden op edux.nl/cyberweerbaarheid.

Tip 3

Bedenk op welke wijze je de afspraken met het team wil delen. Denk bijvoorbeeld aan een studiemoment of het nieuwsbericht van jullie school voor alle teamleden.

Tip 4

Weeg af of en zo ja op welke manier je de ouders van leerlingen op de hoogte wil stellen van jullie aanpak. Ouders betrekken kan ervoor zorgen dat zij gemotiveerd worden om ook thuis het gesprek aan te gaan over cyberweerbaarheid.

Tip 5

Bedenk op welke wijze je feedback van collega's wil verzamelen nadat je jullie plan tot uitvoering hebt gebracht. Plan een evaluatiemoment in om de feedback te analyseren en waar nodig aanpassingen te doen voor een volgende periode.

OVER PROJECT DIGITAAL NIET TE FOPPEN

Dit document komt voort uit het project "Digitaal Niet Te Foppen". Dit project is aangejaagd door de Politie Oost-Brabant en uitgevoerd in samenwerking met een aantal scholen en verschillende onderwijs-netwerkpartners. Doelstelling van dit project is om de aandacht voor cyberweerbaarheid te borgen in het curriculum van het primair- en voortgezet onderwijs. Edux heeft vanuit Digitalig bijgedragen aan dit project door bestaande kennis op het gebied van digitale weerbaarheid te koppelen aan praktijkervaringen van (basis- en middelbare)scholen en dit te bundelen in dit document.

De input vanuit de praktijk is opgehaald bij de volgende scholen:

De Talisman – SKPO

De Schakel – SKPO

De Achtbaan – SKPO

Mezzo Elzendaal Gennep - OMO

Bovenstaande scholen zijn daarnaast actief aan de slag gegaan met het borgen van cyberweerbaarheid binnen hun curriculum. De universiteit van Utrecht en Avans Hogeschool zijn daarbij een onderzoek gestart om de doeltreffendheid van de ingezette lesmaterialen te evalueren en de ervaringen van docenten/leerlingen op te halen. Alle inzichten voortkomend uit project Digitaal Niet Te Foppen kun je vinden op de website van Wikiwijs.

Samenwerkende partijen in dit project:

Projectaanjagers

Onderzoek en visievorming

Opschaling

Training van onderwijsprofessionals

BIJLAGE 1:

PLAN VAN AANPAK CYBERWEERBAARHEID

INVULBLAD

Naam school …… Invuldatum ……

Naam stichting ……..

Betrokken verantwoordelijken: …….

WAAROM

Voor onze school is het van belang om aandacht te hebben voor digitale criminaliteit omdat:

HOE

- Geïntegreerd in andere lessen
- Met behulp van op zichzelf staande (gast)lessen
- Met behulp van een projectweek

Wij hebben deze keuze gemaakt omdat:

PRAKTIJKUITWERKING

Te gebruiken materiaal:

Planning:

Communicatie naar team (afspraken):

Communicatie naar ouders:

Wijze van feedback verzamelen:

Evaluatiemoment:

Met behulp van dit plan willen wij cyberweerbaarheid structureel en terugkerend aandacht geven binnen ons onderwijs. Ondergetekenden willen de verantwoordelijkheid nemen om het plan verder uit te werken en in de praktijk te brengen:

Naam:

Handtekening:

Naam:

Handtekening:

BIJLAGE 2: REFERENTIES

CBS. (2024). Veiligheidsmonitor 2023. In *CBS*. https://download.cbs.nl/maatwerk/Veiligheidsmonitor-2023.pdf

Lee, A. Y., & Hancock, J. T. (2023). Developing digital resilience: An educational intervention improves elementary students' response to digital challenges. *Computers And Education Open*, *5*, 100144. https://doi.org/10.1016/j.caeo.2023.100144

Manning, C. (2021). *A framework for digital resilience: supporting children through an enabling environment*. Parenting For A Digital Future. https://blogs.lse.ac.uk/parenting4digitalfuture/2021/01/20/digital-resilience/

SLO. (2024a). Factsheet - basisvaardigheden digitale geletterdheid. In *www.slo.nl* [Report]. https://www.slo.nl/publish/pages/20961/factsheet-digitale-geletterdheid.pdf

SLO. (2024b). *Concept-kerndoelen Digitale geletterdheid*. SLO, Amersfoort. https://www.slo.nl/publish/pages/21532/slo_conceptkerndoelen_en_toelichtingsdocument_digitale_geletterdheid_opleverversie_dd-29-2-2024-.pdf

Wissink, I. (2021, 1 oktober). *Jeugdrecht en jeugdbescherming: De online jeugddelinquent*. Utrecht University. https://research-portal.uu.nl/en/publications/jeugdrecht-en-jeugdbescherming-de-online-jeugddelinquent