

mijn kind  
Online

**KINDEREN EN ONLINE**  
**PRIVACY**





## VOORWOORD

**Privacy is de private ruimte in ieder mens: je eigen gedachtewereld, je gevoelsleven, je innerlijk. Het is de ruimte waar je gedachten en gevoelens alleen toegankelijk zijn voor jezelf. Soms ga je naar buiten met wat je denkt en voelt, bewust of**

**onbewust, door te bloggen of te blozen.**

Hoe belangrijk privacy op internet is - iedereen heeft wel wat te verbergen - drong extra tot ons door toen we ontdekten dat niet alleen wereldleiders, maar ook Nederlandse burgers, u en wij, door de Amerikaanse overheid in de gaten worden gehouden. Wat je mailt, de berichten die je met je smartphone verstuurt, de NSA kon erbij. Kan er nog steeds bij. Dat vinden we erg.

Desondanks geven ouders heel veel informatie zelf weg. Ze zijn sharents, die van alles over hun kinderen op Facebook delen. Van babyfoto's tot vakantiekiekjes: alles gaat online. Oók als school een leuke activiteit organiseert. Met een druk op de knop staat het op Facebook of Twitter. Maar er zijn ook kritische geluiden: steeds meer vaders en moeders maken bezwaar als de school of de kinderopvang foto's van hun kinderen via sociale media met de hele wereld deelt. Terecht natuurlijk.

Hoe zorgen we dat we de privacy van kinderen waarborgen, nu deze door de technologie steeds verder in de verdrukking komt? Hoe zorgen we dat kinderen zelf hun identiteit kunnen bepalen, zonder dat wij dat al voor ze doen door foto's online te zetten waar ze als puber met afgrijzen naar kijken? Hoe gaan we eigenlijk om met onze eigen privacy? En die van onze leerlingen?

Geen makkelijke vragen, maar wel hele belangrijke. In deze brochure van Digibewust, Mijn Kind Online en Kennisnet, helpen we u, ouder én leerkracht, graag op weg.

Toine Maes,  
Directeur Kennisnet

## INHOUD

- 
- 4** **Wat van jou is, moet van jou blijven, óók online.**
  - 7** Remco Pijpers (Mijn Kind Online): **'Ik wil niet dat mijn kinderen online terug te vinden zijn'**
  - 8** **10 tips voor ouders**  
TV-journalist Liesbeth Staats: 'Een leuke foto van de kinderen mail ik wel gewoon naar mijn ouders'
  - 10** **Zo maak je privacy belangrijk**  
Een stappenplan
  - 13** **Help, ik word bespied!**  
De 4 grootste gevaren voor je online privacy
  - 16** **10 tips voor jonge gebruikers**  
Internetondernemer Midas Kwant: 'Ik weet precies wat ik moet tweeten om meer volgers te krijgen'
  - 18** **Online privacy voor kinderen?**  
App-makers nemen het niet zo nauw
  - 20** **10 tips voor leerkrachten**  
Leerkracht Tessa van Zadelhoff: 'Ik vraag me altijd af: mogen mijn moeder, buurvrouw en baas dit lezen?'
  - 22** Vraag en antwoord met Job Vos (Kennisnet): **Online privacy voor scholen**
  - 24** **Vuistregels voor privacy**
  - 24** **Colofon**





# WAT VAN JOU IS MOET VAN JOU BLIJVEN **OÓK ONLINE!**

**‘Op Facebook kun je je in een huiskamer met vrienden wanen, terwijl je de reikwijdte van het medium compleet vergeet’, zegt televisiejournalist Liesbeth Staats verderop in deze brochure. Hoe leer je kinderen wat die reikwijdte is? En wat het veiligstellen van je online privacy nu precies betekent? Weten wij volwassenen eigenlijk wel wat dat inhoudt?**

**O**nline privacy gaat veel verder dan voorzichtig zijn met het achterlaten van je adresgegevens of telefoonnummer, of het niet accepteren van vreemde vriendschapsverzoeken. Minstens zo belangrijk is het dat kinderen beseffen dat wat je rondtoert op Twitter daadwerkelijk door de hele wereld te lezen is. En dat het nooit meer verdwijnt, ook. En dat het op Facebook posten van een foto van een wild feestje, met alle tags erop en eraan, ervoor zorgt dat ook de vrienden van vrienden van vrienden kunnen meegiffelen.

## **Gebrek aan besef**

Wie kinderen een besef van online privacy wil bijbrengen, kan het beste eerst bij zichzelf te rade gaan, zegt Justine Pardoën, hoofdredacteur van Ouders Online en mediawijsheidsdeskundige bij Bureau Jeugd & Media. Want we mogen ons dan verbazen over onze kinderen en hun totale gebrek aan besef van online privacy, we kunnen er zelf ook wat van. Wie zet er een constante stroom aan kiekjes van de pasgeboren baby online? Of van de aandoenlijke briefjes vol spelfouten die ze ons schrijven in groep 3 en de liefdesbrieven vol roze hartjes die ze ontvangen van leeftijdsgenootjes? Wie grijpt er meteen naar zijn smartphone om die té grappige uitspraak van peuterlief of puberdraak online te gooien? Juist. ‘Je hoort vaak dat kinderen geen besef hebben van privacy. Maar dat is niet zo. Ieder mens voelt zich ongemakkelijk wanneer persoonlijke informatie terecht komt bij mensen voor wie het niet bedoeld was. Een tienjarige vindt het helemaal niet prettig om zichzelf als zevenjarige in zwembroek terug te vinden op internet’, zegt Pardoën. Door steeds

over ze te schrijven, ze te taggen en te fotograferen, ontnemen we onze kinderen de kans om zelf beslissingen te nemen over hun eigen online identiteit, hun eigen digitale voetafdruk, vindt zij. ‘Tegen de tijd dat zij actief worden op sociale media, is er al veel over hen te vinden waarover ze misschien geen controle meer hebben. Als ze jong zijn doen ze bovendien na wat anderen doen, wat jij doet. Als je daar niet bewust mee omgaat, moet je straks niet gek opkijken als je kinderen ook allerlei persoonlijke dingen gaan posten - dus ook foto’s van hun moeder die een gekke uitgljider maakt. Het lijkt me goed als ouders zich meer bewust zijn van hun invloed op het online imago van hun kinderen. En dat ze dus ook afspraken maken met de school, kinderopvang en oppas over het al dan niet online plaatsen van foto’s van hun kind.’

## **Online imago**

Volgens Tessa van Zadelhoff, projectleider ICT en 21st Century Skills bij PRODAS, een overkoepelende scholenorganisatie in Noord-Brabant, zijn kinderen tegenwoordig al heel vroeg bezig met dat online imago. ‘Het zijn vooral de bijna-twintigers en dertigers die zich daar nog niet altijd even bewust van zijn. Terwijl je bij kinderen ziet dat ze al beter nadenken over wat ze willen dat er online over hen te vinden is. Ze doen als het ware aan personal branding. Kijk maar eens naar hun Instagram, de ene foto ziet er nog professioneler uit dan de andere. Maar mediawijs zijn moet je wel leren.’ Want tegelijkertijd hebben kinderen vaak geen idee dat alles wat ze doen voor iedereen zichtbaar is, zegt Justine Pardoën. ‘Kinderen experimenteren en maken fouten. En dat moet ook, die ruimte hebben ze nodig om te kunnen groeien. Daarbij hebben kinderen net als wij behoefte aan verbinding, ze beseffen dat het delen van intiem kapitaal – het jezelf tot op zekere hoogte blootgeven – een manier is om je verbonden te voelen. Vroeger gingen ze dan een keer onderuit omdat ze iets vertrouwelijks aan een minder goede vriendin vertelden, die het dan weer doorvertelde. Maar in deze tijd verspreidt zo iets zich razendsnel en zijn de gevolgen veel groter.’

## 'Juist kinderen kunnen heel moeilijk overzien wat de gevolgen zijn van hun online gedrag'

### Controle

Tim Toornvliet van de digitale burgerrechtenorganisatie Bits of Freedom: 'Online privacy is het hebben van controle over je eigen gegevens en over wat anderen over jou weten en wat ze met die informatie doen.' Als je die controle niet hebt, en anderen kunnen zomaar informatie over jou verzamelen en gebruiken, dan verlies je je vrijheid. 'Neem bijvoorbeeld vakantiefoto's die je opeens op een site tegenkomt waar je ze zelf niet hebt gepost, of het feit dat bedrijven jouw zoektermen op Google verzamelen, zodat je prompt op elke website aanbiedingen op dat gebied tegenkomt. Kinderen die nu opgroeien zijn al hun hele leven online, maar het is juist voor hen heel moeilijk te overzien wat de gevolgen kunnen zijn van hun online gedrag.'

Volgens Toornvliet zouden we moeten beginnen met kinderen te leren wat internet nu eigenlijk is. 'Ze snappen nog niet dat Twitter of Whatsapp geen nutsvoorzieningen zijn, zoals het water uit de kraan, maar dat er bedrijven achter zitten die geld verdienen aan jouw gegevens. Of dat de foto's die je op Facebook zet niet meer van jou zijn, maar dat ze opgeslagen worden op servers in Amerika.'

Toornvliet pleit ervoor om kinderen op school te laten experimenteren met het bouwen van eigen netwerkjes. 'Zodat ze kunnen ervaren hoe open de communicatie is op zo'n netwerk, en hoe het voelt als anderen jouw berichtjes ook kunnen lezen.'

'Als het over het recht op privacy gaat, hebben we het meestal over de relatie tussen overheid en burger of bedrijven en burger', voegt Justine Pardoën toe. 'Maar voor de relatie tussen mensen zijn geen regels. Dus is het van groot belang dat kinderen leren hoe ze online met elkaar om moeten gaan. Ze moeten empathie ontwikkelen, en besef van de grenzen van zichzelf en die van anderen. Al van heel jongs af aan kun je ze dat bijbrengen. Als ze met oma Skypen kun je vragen: Hoe is het om zo met haar te praten? En waarom is dat anders dan wanneer we haar gewoon bellen en alleen haar stem horen? Wat voegt het toe dat je haar ook kunt ruiken en voelen tijdens een bezoekje bij haar thuis? Maak ze stapje voor stapje bewust van de grenzen en mogelijkheden van online communicatie. Wat deel je met anderen en wat zijn de gevolgen? Wat gebeurt er met een foto die je op Facebook zet? Wie kan dat allemaal met elkaar delen? En wat als je over iemand roddelt die getagged is in een foto, wie leest er dan allemaal mee?'



### WAT KAN DE SCHOOL DOEN?

De bewustwording over privacy op scholen verbetert met de dag: zo plaatsen veel scholen foto's en gegevens van leerlingen inmiddels alleen op een beveiligd gedeelte. Toch valt er nog een wereld te winnen. De geïnterviewden in deze brochure noemden de volgende verbeterpunten:

- Nu alle informatie over leerlingen online wordt bewaard, is het nóg belangrijker om goed na te denken over de formuleringen die je gebruikt bij bijvoorbeeld het vastleggen van sociaal gedrag van kinderen. Wees je ervan bewust dat anderen het in de toekomst wellicht ook kunnen lezen en er hun eigen interpretatie op los kunnen laten.
- In deze tijd van data-lekken is het verstandig om gevoelige rapporten en dossiers te versleutelen. Email lijkt veilig, maar is in feite een vrij open medium.
- Besteed in de lessen aandacht aan privacy. Google een paar kinderen in de klas en lees voor wat je allemaal over ze te weten bent gekomen. Lees hardop comments voor die ze op een forum hebben gepost, of berichtjes die ze naar elkaar hebben gestuurd. Zo ervaren ze het ongemak en worden ze mediabewuster. Praat met leerlingen over hun online gedrag en maak afspraken. Wat zetten we online over elkaar en wat niet? Wat is leuk en wat is stom? Wat doe je online om aardig gevonden te worden? Om een band met iemand op te bouwen moet je ook iets van jezelf laten zien, maar wanneer gaat dat te ver?



Zet je je kinderen in de digitale schijnwerpers, of niet? Remco Pijpers, een van de oprichters van Mijn Kind Online én vader van 3, doet het liever niet. Helaas heb je dat niet altijd in de hand, is zijn ervaring.



### Remco Pijpers:

## 'IK WIL NIET DAT MIJN KINDEREN ONLINE TERUG TE VINDEN ZIJN'

De Gouden Apenstaart, de verkiezing van beste kindersite van Nederland, is voor mij een van de hoogtepunten van het jaar. Maar die keer, op woensdag 17 april 2013, was het wel een heel bijzondere editie. De presentator haalde me het podium op, om te vragen hoe we met de verkiezing zijn begonnen en waarom het zo'n succes is geworden. Ik stapte op hem af, applaus, applaus, dank u wel, toen de presentator zei: 'Ik weet dat ook je zoon in de zaal zit. Ik ga hem interviewen!'

Het was hilarisch.

Hij vroeg mijn toen 7-jarige oudste of hij weleens op de iPad mocht. 'Ja', antwoordde hij. 'Maar alleen in het weekend en maar 5 minuten.'

De zaal bulderde van het lachen. De Mijn Kind Online-oprichter promoot positieve content voor kinderen en is enthousiast over het internetgebruik van kinderen, maar zijn eigen kinderen schermt hij resoluut af. 5 minuten op zaterdag en 5 minuten op zondag... Spartaans!

De realiteit is dat voor zoonlief een uur op de iPad als 5 minuten voelt én hij wilde zijn vader afschilderen als iemand die het juiste doet voor zijn kind: niet te lang op het scherm!

Hoe het ook zij, de presentator stelde voor om mijn zoon elke zaterdag en zondag niet een uur, maar een uur en een kwartier, op de iPad te laten. Ik toonde me grootmoedig: 'Dat is goed'.

'Akkoord?', richtte hij zich tot mijn zoon. 'Nou, dan liever anderhalf uur.'

De wijsneus.

### Ongemakkelijk

Dit zou ik een volgende keer niet meer willen.

Ik wil mijn kinderen namelijk niet in de publiciteit.

Ik wil geen foto's van ze online. Niet op de site van de naschoolse opvang (gebeurde toch, ondanks een expliciet 'nee' vooraf) en niet op de site van de

school. En niet op Twitter na een publiek optreden bij Beeld en Geluid. Wat wel gebeurde. Het regende tweets en foto's op Instagram waar je mijn zoon ziet schitteren en mij ongemakkelijk ziet staan, met de handen in de zakken.

### Terugdraaien

Waarom ik niet wil dat mijn kinderen online terug te vinden zijn? Om twee redenen. Ten eerste weet ik zeker dat ik een keer een enorme blunder zal begaan. Ik zeg iets op de radio waar iedereen over valt of ik doe een verspreking waarmee ik me onsterfelijk belachelijk maak. De kans dat ik een keer iets doms doe is reëel – iedereen maakt fouten. Daar kan ik mee leven. Maar ik wil niet dat na een zoektocht op mijn naam via Google, Twitter of Facebook, mijn kinderen tevoorschijn komen. Ik wil niet dat mijn kinderen het slachtoffer zijn van mijn stomiteiten. Ten tweede vind ik dat ze zelf moeten kunnen beslissen wat er van hen online staat. Ze kunnen foto's niet meer terugdraaien als ze ouder zijn. Ik post weleens foto's van ze, bijvoorbeeld als ze een bepaald spelletje op de iPad spelen, maar dan zo dat ze onherkenbaar zijn. Dat is functioneel. Zo kan ik een app noemen, waarbij ik mijn volgers laat zien dat ik óók een vader ben, met soms ook zijn onzekerheden.

Gaat het me lukken om mijn kinderen online te verbergen? Dat is ontzettend moeilijk, zo niet onmogelijk, zo blijkt. Onlangs discussieerde ik online met universiteitsstudenten uit Parijs over de kwaliteit van kinder-apps, toen mijn 4-jarige dochter doodleuk het beeld in kwam lopen. Google Hangout, waar de discussie plaatsvond, was voor haar interessanter dan Babar op DVD. Ik dacht nog: het kan geen kwaad, laat haar maar zwaaien, alleen de Franse studenten zien dit. Maar een dag later stond de sessie op YouTube. En dat gaat nooit meer weg.

## OUDERS

**1 Maak samen met je kind een profiel aan** op Facebook, Twitter, Instagram of [vul maar in]. Let erop dat de standaard-instelling bij de meeste sociale netwerken openbaar is en dat foto's voor promotiedoeleinden kunnen worden gebruikt. Bedenk samen met je kind wie foto's en berichten mogen bekijken. 'Alleen voor vrienden', is de veiligste optie. Ook Twitter en Instagram kun je afschermen zodat alleen vrienden je kind kunnen volgen.



**2 Vertel je kind dat het alleen vrienden toelaat die hij of zij vertrouwt.** Maak een tastbare vergelijking: als je iemand op het schoolplein niets persoonlijks zou vertellen, waarom zou je die persoon dan wel als vriend accepteren? Vertel hem of haar om geen verzoeken te accepteren van onbekenden, omdat niet iedereen hoeft te zijn wie hij zegt te zijn. Achter een leuke meisjes-ava kan evengoed een vijftigjarige man schuil gaan.



**3 Praat met je kind over de risico's van de webcam.** Filmpjes en foto's kunnen gemakkelijk worden opgeslagen en verspreid, en zijn dan nauwelijks nog te verwijderen.



**4 Spreek met je kind af dat hij alleen met jouw toestemming iets mag downloaden.** Zo voorkom je dat er virussen of spyware op de computer of tablet belanden.

**5 Leg je kind uit dat hij geen telefoonnummers en adresgegevens moet achterlaten op internet,** en dat hij ook de naam van de school beter achterwege kan laten.

**6 Google samen eens op de naam van je kind.** Welke informatie is er te vinden? Welke gevolgen kan dit hebben, bijvoorbeeld voor het zoeken naar een baantje?

**10 Respecteer de privacy van je eigen kind.** Zet niet zomaar foto's of persoonlijke briefjes en uitspraken online, zonder toestemming. Maak duidelijke afspraken met de oppas en school over het al dan niet posten van foto's. Wees je ervan bewust dat jij mede het online imago van je kind bepaalt.

**7 Waarschuw je kind dat door tags of door de instellingen van anderen bepaalde comments en posts alsnog zichtbaar kunnen worden** voor veel meer mensen dan hij of zij misschien zelf had bedoeld.

**8 Leg je kind uit wat internet is en wat sociale media zijn.** Vertel ook dat er bedrijven achter zitten die geld verdienen met zijn of haar persoonlijke gegevens. Voer samen zoektermen in op Google, bezoek daarna een paar websites en let op de advertenties.

**9 Maak je kind stapje voor stapje bewust van de verschillen in communiceren.** Hoe voelt het wanneer je alleen iemands stem hoort? En wanneer je iemands gezichtsuitdrukkingen ziet? Wanneer is Whatsappen prettig en wanneer juist niet? Hoe kunnen misverstanden ontstaan?



Volg Liesbeth op @liesbethstaats

TV-journalist Liesbeth Staats (40) houdt haar gezin buiten beeld:

### 'Een leuke foto van de kinderen mail ik wel gewoon naar mijn ouders'

Ik Twitter graag en ben ook actief op Facebook, maar ik heb het daar eigenlijk nooit over mijn kinderen. Ze zijn vier en zeven, ze hebben nog geen idee wat sociale media zijn. Ik vind het een ongemakkelijk idee dat zij kunnen worden aangesproken op een foto die de wereld in is gegaan, zonder dat zij daar zelf iets over te zeggen hebben gehad. Natuurlijk, heel soms bezondig ik me er wel aan, zoals laatst, toen mijn oudste zoon een heel schattig briefje voor me had opgehangen toen ik thuis kwam. Dat postte ik op Facebook. Op dat moment vond ik dat heel leuk, maar later had ik er toch een beetje spijt van. Ik had hem niets gevraagd. De grote les van Facebook is wat mij betreft bovendien dat schattige, vertederende uitspraken van je kinderen vooral leuk zijn voor jezelf. Op Facebook kun je je in een huiskamer met vrienden wanen terwijl je de reikwijdte van het medium compleet vergeet. Door 'Wie is de Mol?' ben ik daar alerter op geworden. Toen kreeg ik zoveel vriendschapsverzoeken dat ik uiteindelijk maar iedereen heb toegelaten. Dus nu gebruik ik het vooral zakelijk en post ik wel eens een filmpje of een artikel dat me raakt, maar persoonlijker dan dat wordt het meestal niet. Een leuke foto van mijn kinderen mail ik wel gewoon naar mijn ouders. Op Twitter ben ik me nog bewuster van het openbare karakter, ik weet inmiddels dat ik onmiddellijk meer reacties krijg zodra ik daar een enigszins persoonlijke tweet of foto plaats. Al is het maar een foto van de tafel waaraan ik zit te eten. Toch schrik ik daar telkens weer van. Er zijn best veel bekende persoonlijkheden voor wie het onderdeel van hun imago is om ook persoonlijke dingen te delen. Dat past niet bij mij. Ik ben journalist, ik maak soms best scherpe verhalen, dan vind ik het prettiger wanneer er weinig persoonlijke informatie over mij of mijn kinderen te vinden is. Als mijn kinderen later zelf een smartphone willen en gaan twitteren of facebooken, zal ik ze zeker uitleggen wie er allemaal kunnen meelesen en wat de risico's zijn. Ik hoop dat ik zo'n relatie met ze opbouw, dat ze het tegen die tijd leuk vinden als ik ze volg. Maar ik zal ze niet controleren, zoals mijn moeder ook mijn dagboeken niet las.'

# ZO MAAK JE PRIVACY BELANGRIJK

## EEN STAPPENPLAN

Wat kinderen online doen en laten, kun je als ouder of leerkracht niet controleren. Maar je kunt ze wél duidelijk maken dat hun online privacy goud waard is. Help kinderen in 6 stappen naar het bewaken van hun eigen online identiteit.

### Stap 1

#### Begin bij jezelf

Iets online plaatsen is gemakkelijk, maar iets verwijderen van internet is minder eenvoudig. Juist daarom is het zo belangrijk om kritisch te zijn over je online gedrag. Het helpt problemen voorkomen. Dat geldt niet alleen voor kinderen, maar voor iedereen. Word je om te beginnen bewust van je eigen online gedrag. Denk na over wat je wel en niet deelt op het internet. Mag iedereen weten waar je

woont? Of hoe je familie eruit ziet? Waar je op vakantie gaat? Google jezelf en bekijk wat je tegenkomt. Probeer te bepalen waar jouw grenzen liggen op het gebied van online privacy. Praat er als ouder over met anderen en deel ervaringen.

#### Op school

Ook voor scholen is bewustwording en oriëntatie de eerste stap. Organiseer een bijeenkomst of zet privacy op de agenda van een teamvergadering. Breng in kaart wat de houding van de school is ten

opzichte van sociale media en privacy. Zetten jullie alles online? Ga na of er afspraken zijn over privacykwesties en of die afspraken vastliggen in een protocol of in het Schoolveiligheidsplan. Als dat zo is, bespreek dan of de afspraken nog voldoen. Is er behoefte aan meer informatie? Nodig een deskundige uit: een wijkagent, een mediacoach van de bibliotheek of een specialist op het gebied van sociale media. Of informeer eens bij andere scholen wat hun privacybeleid is en hoe zij het aanpakken.



### Stap 3



#### Bepaal wat je wilt

Waar wil je kinderen bewust van maken? Maak een lijstje van onderwerpen en de volgorde waarin je ze wilt bespreken. Leer kinderen vooral dat ze niet alles hoeven te delen op internet. Praat bijvoorbeeld over waarom je persoonlijke informatie, zoals je adres, je school, telefoonnummer, achternaam of foto's waarop te zien is waar je woont of naar school gaat, beter niet online kunt plaatsen. Heb het over de voordelen van een anoniem e-mailadres voor registratie op websites of om te reageren op sites en blogs.

#### Op school

Neem als school het lesaanbod op gebied van mediawijsheid onder de loep om te bepalen hoe mediawijs de leerlingen al zijn. Stel een gezamenlijke visie op over privacy. Maak leerlingen medeverantwoordelijk, door ze erbij te betrekken. Bespreek bijvoorbeeld met de leerlingenraad wat zij belangrijk vinden. Betrek ook de ouders: het bewust maken van het belang van privacy is een gedeelde verantwoordelijkheid. Organiseer eens een ouderavond over privacy. Deel het standpunt van de school. Geef ouders én de kinderen de mogelijkheid om te vertellen wat zij belangrijk vinden. Luister naar elkaar en doe er je voordeel mee.



### Stap 2

#### Doe mee online

Wanneer je kinderen en hun online leefwereld serieus neemt, bereik je meer. Ga eens naast een kind zitten en toon belangstelling door vragen te stellen als: Heb je vandaag nog iets leuks meegemaakt op internet? Waar ben je mee bezig? Hoe werkt het? Wat is er zo leuk aan? Onderzoek ook welke diensten kinderen veel gebruiken en welke sociale media en sites populair zijn.

#### Op school

Zet op school hiervoor het mentoruur in, of maak een enquête. Met handige tools als [nl.surveymonkey.com](http://nl.surveymonkey.com) is dat vrij eenvoudig. Alleen praten is niet genoeg. Door zelf mee te doen, weet je pas echt waar kinderen het over hebben. Maak een Facebookprofiel, neem een Twitteraccount, chat en gebruik de webcam. Vraag je daarbij steeds af wat anderen van je mogen weten. Niet iedereen voelt zich thuis online. Een sociale media-workshop door een ervaren collega of een externe kenner kan hel-

pen. Ouders beschikken in veel gevallen al over de best denkbare coach: hun kind. Vaak vinden kinderen het alleen maar leuk om hun ouders of leerkracht uit te leggen hoe iets werkt.

**TIP!** Geef het goede voorbeeld. Ga zelf verstandig om met je privacy! Scherm je profielen af en zet geen persoonlijke informatie over kinderen online zonder hun toestemming. Plaats als school alleen foto's en privacygevoelige informatie op een beveiligd deel van de website.



### Stap 4

#### Maak een plan

Bij kinderen in de basisschoolleeftijd werken een voorlichtende aanpak en afspraken maken nog wel. Als ze wat ouder worden, ontwikkelen jongeren steeds meer een eigen online leven waarop ouders in veel gevallen geen zicht hebben. Alleen regels opstellen is dan niet meer genoeg. Je kunt ze niet meer constant controleren en bovendien ervaren pubers regels al snel als vervelend. Ze willen zelf dingen ontdekken en beslissingen nemen. Meer dan ge- en verbieden, is het raadzaam om pubers te leren inzien wat ze online wel

en wat ze beter niet kunnen doen. Geef hen mee dat een gezonde mate van geheimzinnigheid handig is: het heeft zo z'n voordelen om niet alles online te zetten. Zo kunnen ze zelf bepalen wat ze wel en niet delen met de buitenwereld en zichzelf van hun meest voordelige kant laten zien. Pubers bewust maken van zichzelf en hun online gedrag, bereik je door met hen in gesprek te gaan. Hoe je dat aanpakt, lees je bij stap 5. Bedenk een geschikt moment voor een gesprek over sociale media. Een ontspannen en veilige sfeer is belangrijk.

#### Op school

Spreek op school af wie aandacht gaat besteden aan privacy en wanneer. Kies je voor een lessenserie tijdens mediawijsheid, maatschappijleer of de mentorlessen? Of wordt het een projectweek?

**TIP!** Het boek *Handboek mediawijsheid, praktische gids en inspiratie voor het onderwijs* staat vol lesideeën en praktische tips. Op [www.mijnkindonline.nl](http://www.mijnkindonline.nl) is het gratis te downloaden. Ook leuk en inspirerend voor ouders!

## Stap 5

### Stel Echte Vragen

Om een goed gesprek te kunnen voeren met tieners, is het belangrijk dat zij het gevoel hebben dat je ze serieus neemt. Wees je daarom niet alleen bewust van de risico's maar ook van de kansen en mogelijkheden van internet en sociale media. Sta open voor hun wereld en oordeel niet te snel. Werken aan bewustwording betekent niet dat zij altijd het antwoord geven dat je het liefst wilt horen. Natuurlijk kun je als ouder of leerkracht een andere mening hebben over hun online gedrag, maar geef jongeren ook voldoende ruimte voor hun eigen verhaal. 'Het stellen van de juiste vragen is een voorwaarde om een gesprek op gang te brengen', schrijft Justine Pardoën in haar boek 'Focus. Over sociale media als de grote afleider'. Zij adviseert om 'Echte Vragen' te stellen: open vragen waar je zelf het antwoord niet op weet. Het antwoord is nooit goed of fout. Echte Vragen nodigen kinderen uit om te praten en om na te denken over hun eigen online gedrag.

## Stap 6

### Blijf bewust

Blijf thuis regelmatig op een open manier in gesprek met je kind. Vraag hoe het gaat, waar ze mee bezig zijn en of er online nog iets bijzonders is gebeurd met hen of met hun vrienden.

### Op school

Zet als school privacy regelmatig op de agenda. Bespreek of de lessen nog aansluiten en of de afspraken nog kloppen. Doe dit niet alleen in het team maar ook met leerlingen. Vergeet niet om positieve ervaringen te delen.

## GESPREKSSTARTERS

Een paar voorbeelden van Echte Vragen om een gesprek te beginnen.

**Wat doe jij het liefst op internet?** Kun je uitleggen waarom?

**Wat vind je van Facebook?** Wat vertel je er over jezelf en wat niet? Waarom? Zijn Facebookvrienden hetzelfde als je echte vrienden? Waarom wel/niet?

**Is er voor jou verschil tussen iets online of offline vertellen?**

Wat zou je niet online zetten bijvoorbeeld? Waarom niet?

**Chat je weleens?** Ook met mensen die je niet kent? Gebruik je een webcam?

**Ben je weleens beledigd online?** Hoe voelde dat? Is er een verschil tussen een persoonlijke belediging, via Whatsapp, en een openbare (via Facebook of Twitter)? Is het weleens een van je vrienden overkomen? Hoe voelde dat voor jou? Wat deed je?

**Zijn al je online vrienden hetzelfde of is er verschil?** Zijn er vrienden die je alleen online spreekt? Wat is het verschil tussen deze vrienden en je 'echte' vrienden?

**Wat is jouw online imago?** (Google eens op je eigen naam of laat kinderen elkaar googlen) Klopt het beeld met hoe jij jezelf ziet? Voelt het goed? Als dat niet zo is: hoe zou je het dan kunnen veranderen? Is op internet veel persoonlijke informatie te vinden over jou? Hoe voelt dat? Zou je het willen veranderen?

**Meer lezen?** Focus! Over sociale media als de grote afleider, door Justine Pardoën.

# HELP, IK WORD BESPIED!

Soms gaat het mis. Privacy is voor de meeste kinderen niet hun eerste aandachtspunt. Sterker nog, kinderen en jongeren gebruiken digitale media nou juist vaak om heel veel van zichzelf te laten zien. En ze denken niet altijd na over de gevolgen daarvan.

## DE 4 GROOTSTE GEVAREN VOOR JE ONLINE PRIVACY

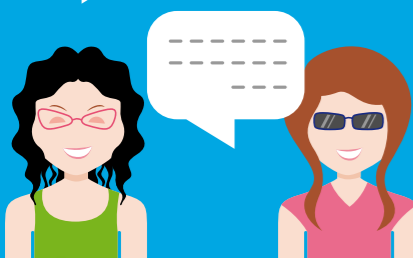
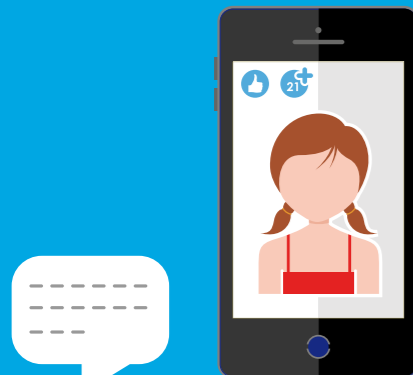
### 1 Virtuele diefstal

Diefstal komt op internet regelmatig voor. Dat klinkt misschien gek, want wat valt er nou te halen in de virtuele wereld van internet? Veel, zo blijkt, maar beroving op internet gaat anders dan in huis of op straat. Het kan bijvoorbeeld gaan om het stelen van wachtwoorden en inlogcodes of het stelen van een identiteit. Een veel voorkomende vorm van diefstal is het roven van aankopen in online games, bijvoorbeeld door iemand zijn accountgegevens te ontfutselen. Bestolen worden op internet kan gebeuren door bekenden, die bijvoorbeeld uit pesterij op het account van een ander kind gaan. Soms gebeurt dat onder bedreiging. Het kan ook gebeuren door onbekenden, hackers die niet om een persoonlijke reden stelen, maar omdat ze op een andere

manier kwaad in de zin hebben. Zij maken soms gebruik van phishing, waarbij slachtoffers naar valse websites worden gelokt, waar ze nietsvermoedend hun gegevens invullen – en kwijt raken. Bestolen worden op internet kan langdurige en vervelende gevolgen hebben, zeker als iemand zich met de gegevens en onder de naam van het slachtoffer op het net begeeft.

### Strafbaar?

Diefstal is strafbaar, waar het ook gebeurt. Virtuele diefstal is dus ook strafbaar. Die strafbaarheid is nog eens bevestigd in zaken die bij de rechter werden aangespannen na diefstal in bijvoorbeeld een spel als Runescape. Wie slachtoffer is van virtuele diefstal, kan daarvan aangifte doen bij de politie.



## 2 Hacking

Als je wordt 'gehackt', probeert iemand anders via een computer of netwerk toegang te krijgen tot jouw gegevens. Iemand probeert in te breken in een computersysteem of netwerk en doet dat met een virus, spyware, door phishing en met poortscans. Hacken kan 'voor de lol' gebeuren, maar meestal is men uit op het verkrijgen van persoonlijke gegevens, zoals wachtwoorden en gebruikersnamen. Hacken kan ook gebeuren met als doel om de ruimte op je computer of website te gebruiken voor het opslaan van (grote) illegale bestanden, die later opgehaald worden door andere inbrekers. Ook komt het voor dat hackers programma's installeren om spam mee te versturen of aanvallen te doen op andere computers. Dat kan ongemerkt gebeuren.

### Strafbaar?

Hacking is strafbaar als dit gebeurt zonder toestemming van de eigenaar van de gehackte gegevens. Een hacker kan iemand zijn inloggegevens afhandig maken door deze te raden of slimme vragen te stellen, maar er kan ook sprake zijn van dwang of bedreiging. Als je gehackt bent, en zeker als je daarbij bent bedreigd, kun je aangifte doen

INLOGGEGEVENS

## 3 Phishing

Phishing is een vorm van internetfraude. Het woord lijkt op 'vissen' en dat klopt ook wel: iemand probeert te vissen naar jouw vertrouwelijke gegevens. Een bekend voorbeeld is de email die eruit ziet alsof deze door de bank is verstuurd. Via een nep-mail van een doorgaans betrouwbare partij (een bank, of de beheerder van een online game), probeert men inloggegevens van mensen te krijgen. In dat mailtje wordt gevraagd om op een link te klikken en daar je persoonlijke gegevens in te vullen, waaronder je gebruikersnaam en je wachtwoord. Op die manier geef je vertrouwelijke gegevens weg aan iemand die er misbruik van wil maken, zonder dat je het weet.

### Strafbaar?

Phishing is strafbaar: het gaat om oplichting en (in sommige gevallen) om valsheid in geschrifte. Als je het slachtoffer van phishing bent geworden en daarvan schade hebt ondervonden, kun je aangifte doen bij de politie.

## 4 Belediging, smaad en laster

Op internet is het makkelijk om anderen te beledigen of iemands goede naam aan te tasten. Denk aan een Facebook-pagina met bewerkte foto's, een e-mailadres onder de naam van een ander aanmaken en daarmee kwetsende teksten rondsturen, of uit naam van een ander scheldpartijen op een forum plaatsen. Het kan heel moeilijk zijn om zulke praktijken te beëindigen en de beledigingen weer van internet te krijgen.

### Strafbaar?

Belediging, smaad en laster zijn strafbaar. In de praktijk gaat het vaak om uit de hand gelopen pesterijen. Pesten, uitschelden, treiteren of negeren maken je enorm kwaad of verdrietig, maar zijn niet strafbaar. Je kunt dus geen aangifte doen van pesten. Als de pesterij zó uit de hand loopt dat er sprake is van smaad of laster, kun je daarvan wel aangifte doen bij de politie. Ook als je beledigd of bedreigd wordt, kun je daarvan aangifte doen.

IDENTITEIT

## WANNEER STAP JE NAAR DE POLITIE?

### • Voor het doen van een MELDING.

Als je geen aangifte wilt doen of als er geen aangifte gedaan kan worden, kan een melding wel heel zinvol zijn. Je brengt de politie dan toch op de hoogte van de situatie en de feiten en dat kan in de toekomst belangrijk zijn. Je hoeft zelf geen slachtoffer of benadeelde te zijn om naar de politie te stappen. Ook als je wilt voorkomen dat een ander mogelijk slachtoffer wordt van strafbare feiten op internet, kun je aankloppen. Je kunt bij de politie ook vragen stellen over cybercrime.

### • Voor het doen van AANGIFTE.

Zoals bij alle andere vormen van criminaliteit kun je, als je slachtoffer van cybercriminaliteit bent of denkt te zijn, aangifte doen bij het politiebureau. Door het doen van aangifte verzoek je de politie een strafrechtelijk onderzoek in te stellen. De aangifte is doorgaans het begin van een politieonderzoek. De politie maakt dan een proces-verbaal van aangifte op. Als je minderjarig bent, is het goed om een van je ouders mee te nemen naar het politiebureau. Het doen van een (telefonische) melding is géén aangifte.

### • Wat neem je mee naar de POLITIE?

Noteer en verzamel zoveel mogelijk informatie en bewijsmateriaal, zoals:

- Data en (exacte) tijdstippen
- Email- en internetadressen (url)
- Gebruikersnaam en nickname(s) van betrokkene(n)
- Prints van chatlogs en mailberichten
- Bewaarde sms-berichten
- Schermafdruk (via print screen of maak een foto)

## HANDIGE SITES

- Op [www.meldknop.nl](http://www.meldknop.nl) vind je informatie over en hulp bij internetproblemen. Ook over pesten vind je hier informatie en advies over wat je kunt doen als je op internet wordt lastiggevallen. Je kunt via deze website de Meldknop ook installeren op je computer. Dan staat hij tijdens het internetten altijd in beeld en heb je met een klik op de Meldknop meteen informatie, hulp en advies. En je kunt direct een melding maken.

- [www.digibewust.nl](http://www.digibewust.nl) wil het veilig en verantwoord gebruik van internet en van computer, mobiele telefoons en andere digitale middelen stimuleren. Digibewust is onderdeel van het programma Digi-vaardig & Digiveilig dat een samenwerkingsverband is tussen overheid, bedrijfsleven en maatschappelijke organisaties. Op de site vind je advies en handige tips over veiligheid.

- Word een kind gepest, heeft het problemen thuis, ruzie met vrienden of voel hij zich rot, dan kan hij bellen of chatten met de **Kindertelefoon** (0800-0432 of Live Messenger-chat: chatbot@kindertelefoon.nl). Op de website [www.kindertelefoon.nl](http://www.kindertelefoon.nl) is ook veel informatie te vinden. De Kindertelefoon is er voor alle kinderen en jongeren tussen de 8 en 18 jaar.

- Op [www.vraagthedepolitie.nl](http://www.vraagthedepolitie.nl) kunnen kinderen tussen 12 en 18 jaar oud vragen én antwoorden vinden over veiligheid, zoals over loverboys, drugs, geweld, boetes, internet, alcohol of cybercrime. Ook kun je op deze site chatten met politieagenten.

- [www.mediawijsheid.nl](http://www.mediawijsheid.nl) is een site van Mediawijzer.net. Je kunt er meer informatie vinden over mediawijsheid en privacy.



# JONGE GEBRUIKERS



## 1 Gebruik een nickname

Door op blogs, fora en in chats met onbekenden een andere naam te gebruiken, ben je moeilijker te vinden voor vreemden. Gebruik voor dingen waarmee je je graag wilt profileren – bijvoorbeeld met dansen of zingen – juist wel je echte naam.



## 2 Scherm je profiel af

Stel je profiel op Facebook in op 'alleen vrienden', zodat alleen zij foto's en berichten mogen bekijken. Zet een slotje op je Twitter-account zodat alleen mensen die jij zelf toestemming geeft, je tweets kunnen lezen.

## 3 Voor altijd

Het internet is net een tattooage. Wat je online zet, gaat er nooit meer af. Ook als het niet direct zichtbaar is, is het nog terug te vinden. Denk daaraan bij alles wat je plaatst, of bij wat je doet voor een webcam. Wat vindt je toekomstige baas ervan als je later gaat solliciteren?

## 4 Gouden regel

Als je iets niet zou doen IRL (In Real Life), doe het dan ook niet in cyberspace.

## 5 Gebruik geen tags

Zodra je iemand anders tagt in een foto of bericht, krijgen ook al zijn of haar vrienden of zelfs vrienden van vrienden dat te zien en te lezen. Je kunt zelf ook aanvinken dat foto's waarin jij getagd wordt, niet zomaar op je tijdlijn verschijnen.

## 6 Respecteer andermans privacy

Zet geen gegevens of foto's van anderen online, zonder hun toestemming. Plaats geen gênante foto's van klasgenoten. Ook geen bewerkte foto's, ook al denk je zelf dat het heel grappig is. Het posten van stiekem opgenomen filmpjes kan zelfs strafbaar zijn.

## 7 Post geen persoonlijke gegevens

Vertel nergens de naam van je school, je woonadres, telefoonnummer of e-mailadres. En houd je wachtwoord geheim.

## 8 Online imago

Denk bewust na over je online imago. Reageer vlot op berichtjes en deel complimenten uit. Negeer ruzies en scheldpartijen. Wees positief, feliciteer en complimenteer je vrienden. Google jezelf regelmatig, zodat je weet wat anderen over jou terug kunnen vinden. Meld je aan op [google.com/alerts](http://google.com/alerts), zodat je kunt bijhouden wat er online over je wordt gezegd.

## 9 Wees kritisch op vrienden

Voeg alleen mensen toe die je goed kent. Ook vrienden worden met een groep of een Bekende Nederlander is geen goed idee. Dan kunnen plotseling veel onbekenden je profiel zien. Check zo nu en dan je vriendenlijst. Hoort iedereen er nog bij?



## 10 Niet zomaar afspreken

Bel of sms niet met mensen die je alleen van internet kent. Spreek nooit zomaar met iemand af die je online hebt leren kennen. Overleg met je ouders en neem een volwassene mee.



Volg Midas op @midaskwant

Internetondernemer Midas Kwant (16) heeft bijna 2500 volgers op Twitter:

**'Ik weet precies wat ik moet tweeten om meer volgers te krijgen'**

Het is niet dat ik er de hele dag mee bezig ben, maar ik zit toch wel dagelijks op Twitter en Facebook. Mijn 2500 volgers bestaan uit journalisten, mensen van school, mensen die gewoon geïnteresseerd zijn in wat ik doe en andere ontwikkelaars. De meeste van mijn volgers komen uit Amerika, dus mijn tweets schrijf ik meestal in het Engels. Als ik toch iets in het Nederlands wil tweeten, doe ik dat het liefst 's ochtends, wanneer ze in Amerika nog slapen. Ik houd altijd rekening met het tijdsverschil. Mijn Amerikaanse volgers vinden het irritant als ik ineens op een taal overga die ze niet begrijpen.

Ik begon drie jaar geleden met twitteren omdat ik zelf apps wilde ontwikkelen en nieuwsgierig was naar andere ontwikkelaars. Ik ben hard bezig om toegelaten te worden tot Stanford University en ik wil later graag bij Apple werken. Dus de interactie met hen leek me leuk. Sindsdien heb ik gemerkt dat je veel geretweet wordt als je als eerste een coole website vindt of commentaar hebt op een recente ontwikkeling. Ik doe echt mijn best om een goede tekst te verzinnen. Soms word ik dan ineens 300 keer geretweet en heb ik er zomaar 50 volgers bij.

Ik ben me bewust van mijn online imago en ik denk altijd na over wat ik online post. Ik besef dat alles gedeeld kan worden. Dus zet ik niet snel een feestfoto op Facebook van mij en mijn vrienden, ik wil serieus overkomen. Maar ik vind het wel leuk om mensen te laten weten hoe ik over dingen denk, wat ik wel en niet leuk vind en wat ik aan het doen ben, daar ben ik ook best eerlijk in. Als ik een keer in een discussie op Twitter beland over een onderwerp waar ik eigenlijk niet zoveel van afweet, dan geef ik dat gewoon eerlijk toe. Dat doe ik liever dan dat ik mijn tweets weer verwijder.

Ik praat op internet nooit negatief over andere mensen, dat blijft altijd terug te vinden en ik verander misschien nog wel van mening. Vroeger hebben mijn ouders wel met me besproken dat ik niet zomaar persoonlijke gegevens online moest zetten en geen vriendschapsverzoeken van onbekenden moest accepteren, maar nu hebben we het er eigenlijk nooit meer over. Ik neem aan dat ze het dus eens zijn met hoe ik me online profileer.'

# ONLINE PRIVACY VOOR KINDEREN?

## APP-MAKERS NEMEN HET NIET ZO NAUW

**Veel reken- en taalapps zijn gratis of kosten hooguit twee euro. Als gebruiker 'betaal' je op een andere manier. Veel apps verzamelen de persoonlijke gegevens, óók van kinderen, maar wat ze ermee doen is onduidelijk.**

**H**et aanbod aan apps is overweldigend: dagelijks worden er naar schatting 1600 nieuwe apps aangeboden. En daar is vraag naar. In 2013 hadden drie miljoen Nederlandse huishoudens een of meer tablets en gebruikte 58 procent van de Nederlanders een smartphone. En op al die apparaten installeren gebruikers hun favoriete apps. Óók de jonkies. Kinderapps doen het goed. In het onderzoek App Noot Muis (2011) zei al 71 procent van de ouders 'online' voor kinderen leuk en leerzaam te vinden. Gemiddeld speelt een kind op driejarige leeftijd voor het eerst met apps.

### Toestemming

Helaas raken met deze snelle opmars van interactieve spelletjes de rechten van de gebruiker nog weleens in het gedrang. De makers van de apps nemen het namelijk niet zo nauw met

de privacy van hun gebruikers. E-mailadressen, telefoonnummers, postadressen, vriendenlijsten en informatie over aankopen worden opgevraagd, verzameld en opgeslagen. Vaak zonder dat gebruikers of hun ouders daarvoor toestemming hebben gegeven. Deze persoonlijke gegevens gebruiken de bedrijven voor marketingdoeleinden. Kinderen krijgen zo aanbiedingen voor hun neus, afgestemd op hun leeftijd, locatie en zelfs hun gedrag op de website. En soms ook met advertenties waar ze niet op zitten te wachten.

In de Verenigde Staten wordt deze ontwikkeling met argusogen gevolgd. De Amerikaanse overheid vindt dat ouders geïnformeerd moeten worden over het feit dat gegevens van hun kind worden verzameld. In de Children's Online Privacy Protection Act staat dat ouders eerst toestemming moeten geven, voordat persoonlijke informatie verzameld mag worden. En die toestemming moet verifieerbaar zijn. Klinkt mooi, maar in de praktijk gebeurt dit nauwelijks. De Federal Trade Commission (FTC) in de Verenigde Staten constateerde in 2012 dat makers van apps op grote schaal informatie over kinderen met andere partijen delen. Dit gebeurt in zestig procent van de gevallen zonder goedkeuring of medeweten van de ouders.



**TIP!** Problemen met apps voor kinderen? Meld het op [www.consuwijzer.nl](http://www.consuwijzer.nl)

Zonder juiste informatie over apps, zo concludeerde de FTC, kunnen ouders geen weloverwogen keuzes maken op het gebied van privacy voor hun kinderen.

Een Europese onafhankelijke adviesgroep op het gebied van digitale privacy is het daarmee eens. De 'Artikel 29 Werkgroep' schrijft in een rapport dat in Europa persoonsgegevens alleen mogen worden opgeslagen wanneer de gebruiker daarmee akkoord is gegaan. Maar om dat te kunnen, is duidelijke en volledige informatie nodig. En die ontbreekt vaak. Als er wel informatie beschikbaar is, zijn deze teksten vaak veel te ingewikkeld.

### Leerlingen

Ook scholen hebben hiermee te maken. Veel leerkrachten (en leerlingen!) zijn enthousiast over interactief leren met apps. Educatieve software geeft het leren een boost: de lesstof sluit aan op elk individueel niveau. Kinderen onderhouden hun eigen tuin door reken- en taal oefeningen te

doen. Of ze voeren een 'monster' oplossingen voor rekensommen.

Maar deze 'spelletjes' zijn meer dan alleen educatieve leermethodes voor kinderen in de klas; het zijn ook manieren om vorderingen in de gaten te houden. Prestaties van leerlingen worden opgeslagen en vaak wordt deze informatie door scholen ook gedeeld met de leveranciers van educatief leermateriaal.

Of de leveranciers brengen software op de markt, die via een inlogpagina op internet te bereiken is. De software zelf, en dus ook de gegevens van de leerlingen, worden dan opgeslagen 'in de cloud'. Wat er precies met persoonlijke profielen en andere gegevens gebeurt, blijft voor scholen en ouders onduidelijk. En dus ook hoe deze gegevens worden beschermd.

### Kritische blik

In Californië wil men de online privacy van kinderen beter regelen. Er ligt een wetsvoorstel klaar, dat de commerciële handel in persoonlijke gegevens van kinderen aan banden legt. Onderwijswebsites, online diensten en mobiele apps mogen alleen informatie delen die van belang is voor de school en voor het verbeteren van het product zelf. Gegevens van leerlingen moeten worden versleuteld. Informatie over leerlingen mag niet langer worden bewaard dan nodig. Het verzamelen van informatie via educatieve programma's heeft op deze manier maar één doel: de ondersteuning van de leerling zelf.

Zover zijn we in Nederland nog niet. Omdat bij de meeste apps onduidelijk is welke gegevens van kinderen verzameld worden en waarvoor, zullen ouders zelf moeten beslissen of ze een app willen gebruiken of niet. Dat vraagt dus inzet en betrokkenheid van de opvoeder. En een kritische blik en dito aanpak: Welke informatie geven de makers in de Appstore en de Google Playstore? Wat als er geen duidelijk privacybeleid is? Stel jezelf vragen: Is de (gratis) app reclamevrij? Is het mogelijk om met de app contact te maken met onbekenden? Kun je via de app opeens op een andere website terecht komen? Kunnen kinderen in-app aankopen doen? Is deze optie vergrendeld op de tablet zelf? Dat laatste is geen overbodige luxe, want juist hier gaat het nogal eens mis. Apple moet dit jaar nog het betalingssysteem veranderen, zodat kinderen niet meer zonder goedkeuring van de ouders online spullen kunnen kopen. Ouders zullen zelf moeten beoordelen of een app geschikt is voor hun kind. En zo niet? Dan is de oplossing kinderlijk eenvoudig: met één vingerbeweging zijn ook 'gediskwalificeerde apps' zo naar de prullenbak te slepen.



## LEERKRACHTEN

**1 Sociale media inzetten op school?** Wees zorgvuldig, maar laat je niet weerhouden door de angst voor privacy-schending. Lees je in over de kansen en de mogelijke risico's en neem maatregelen, zodat het gebruik van sociale media leuk, leerzaam en veilig blijft.

**2 Stel een gedragscode op voor leerlingen én leerkrachten** met daarin de afspraken die je met elkaar maakt over digitaal pesten, bedreigingen, schelden en privacy. Maar ook over de grens tussen werk en privé.

**3 Verwijder kritische reacties van leerlingen of ouders niet meteen** (tenzij ze een fatsoensgrens overschrijden, natuurlijk). Reageer openbaar en neem eventueel contact op voor een persoonlijk gesprek.

**4 Ga zorgvuldig om met de privacy van leerlingen.** Plaats op de openbare website alleen groepsfoto's en maak herkenbare portretten en persoonlijke gegevens alleen beschikbaar voor ouders met een inlogcode. Koppel geen namen aan foto's.

**5 Denk bij het in gebruik nemen van de cloud nog beter na** dan je al deed over de formuleringen waarmee je het sociale gedrag en de voortgang van kinderen beschrijft. Wees je ervan bewust dat andere organisaties in de toekomst gegevens kunnen opvragen en koppelen, en er hun eigen interpretatie op los kunnen laten. Versleutel gevoelige rapporten en dossiers, in verband met mogelijke data-lekken.

**6 Neem een mediaprotocol op in het Schoolveiligheidsplan,** waarin je ook sociale media benoemt. Wat op het schoolplein gebeurt, gaat tenslotte op sociale media verder.

**10 In de cloud werken?** Gebruik de Checklist voor afspraken met softwareleveranciers voor scholen die te vinden is op [www.kennisnet.nl](http://www.kennisnet.nl).

**7 Bespreek in de klas de do's en don'ts op sociale media.** Wat is leuk en wat is niet meer leuk? Waar ligt de grens? Hoe houd je rekening met elkaar?



**8 Organiseer ontmoetingen met ouders over mediawijsheid.** Leg uit waarom het belangrijk is dat kinderen daarin worden onderwezen, benadruk de grote aantrekkingskracht op kinderen en daarmee de kansen voor het onderwijs, en leg uit wat je doet om de privacy van leerlingen te waarborgen.

**9 Besteed door alle lessen heen aandacht aan mediawijsheid.** Doe experimenten die schending van privacy invoelbaar maken. Laat leerlingen elkaar googelen en maak met hen een eigen netwerkje en kijk hoe snel informatie zich verspreidt.



Volg Tessa op @warempel

Leerkracht Tessa van Zadelhoff (43) won een prijs met virtueel reisbureau Beartravel en werd met haar klas in één klap bekend in binnen- en buitenland:

**'Ik vraag me altijd af: mogen mijn moeder, buurvrouw en baas dit lezen?'**

Ik ben me door alle aandacht voor Beartravel niet echt anders gaan gedragen. Ik was altijd al oplettend in wat ik wel en niet online deel. Ik deel namelijk heel bewust wél dingen over mijn privéleven, en dat ben ik blijven doen. Over mijn kinderen, mijn hond of over wat ik meemaak. Ik vind het bij anderen ook prettig wanneer ik de mens achter de organisatie of het bedrijf zie, en ze mij een inkijkje geven in hun niet-zakelijke leven. Je moet het natuurlijk niet overdrijven, ik hoef niet elke dag te lezen welke grappige dingen jouw kind nu weer heeft gezegd. Ik vraag me bij alles wat ik post of tweet af: vind ik het erg als mijn moeder, mijn buurvrouw of mijn baas dit leest? Als het antwoord bij een van hen 'ja' is, dan zet ik het er niet op. En nu mijn eigen kinderen ouder worden – ze zijn tien en twaalf – houd ik ook steeds meer rekening met hen. Ik twitter veel en heb bewust een openbaar account, omdat ik dat als onderwijsprofessional belangrijk vind. Ik ben me er daardoor meer van bewust dat ik nooit iets negatiefs over de organisatie, de school of over leerlingen zeg. Sommige leerkrachten zijn daar minder alert op, die tweeten gerust over een voorval in hun klas. Al noem je betrokkenen niet bij naam, ik vind dat je altijd rekening moet houden met de mensen óver wie je iets post. Met de leerlingen op school had ik de afspraak dat ze online vrienden met me mogen worden zodra ze de school verlaten. Ik heb nu ontzettend leuk contact met oud-leerlingen die ik vijftien jaar geleden in de klas had. Ik vind het weleens jammer dat sommige ouders zó bang zijn voor privacy-schending, dat ze mooie sociale-mediaprojecten of een digitale leergang van de school tegenhouden. Ik denk dat juist innovatieve scholen zich heel bewust zijn van de risico's op het gebied van online privacy. Natuurlijk zijn er risico's, en daarom is mediawijsheid ook zo belangrijk, maar alles komt uiteindelijk in de cloud, er is geen weg terug. Dan kun je maar beter kijken naar de kansen die dat biedt en je niet laten leiden door angst. Het heeft mij in elk geval heel veel gebracht.'

Volg Job op  
@jobavos



**Job Vos is jurist bij Kennisnet, ict-partner voor het onderwijs. Hij krijgt vaak vragen van scholen over hoe zij de online privacy van hun leerlingen kunnen waarborgen.**

# ONLINE PRIVACY VOOR SCHOLEN

## Hoe belangrijk is het voor scholen om na te denken over de online privacy van kinderen?

'Heel belangrijk. Kinderen gebruiken apps op tablets en zitten graag op sociale netwerken. Die apps en sociale netwerken verzamelen privégegevens. Deze gegevens worden bijvoorbeeld gebruikt door commerciële partijen, zodat er gericht advertenties kunnen worden aangeboden. Apps, sociale netwerken en educatieve software kunnen een verrijking zijn van het onderwijs. Als je er maar verstandig mee om gaat. Denk als school dus goed na over welke software, apps en sociale platforms je wilt gebruiken. En zoek uit wat er met de persoonlijke gegevens van kinderen wordt gedaan.'

## Ook scholen zelf verzamelen online persoonsgegevens van leerlingen. Om wat voor informatie gaat het?

'Het verzamelen van gegevens begint al vóór de eerste dag op school: wat zijn de contactgegevens, wie is de huisarts, de tandarts. Daarna worden de cijfers van de leerlingen opgeslagen, net als de leerresultaten van de leerling. Ook be-

waren scholen medische gegevens, bijvoorbeeld van een kind dyslectisch is, of ADHD heeft. Dat is gevoelige informatie. Daar moet je als school dus extra zorgvuldig mee om gaan. Als school mag je deze medische gegevens alleen gebruiken om leerlingen te kunnen begeleiden. En ook mag deze informatie niet gedeeld worden met andere partijen als daar niet uitdrukkelijk toestemming voor is gegeven.'

## Wat moeten scholen regelen voor gebruik van foto's van leerlingen?

'Een foto waarop een leerling herkenbaar in beeld is, zegt iets over de leerling, die foto is een persoonsgegeven. Als de school die foto op de website wil zetten van de school, dan eist de wet dat daar toestemming voor wordt gevraagd. Het is een hele uitdaging voor scholen om ieder jaar de toestemming te vragen aan ouders, daarom kan je er voor kiezen om uit praktisch oogpunt ieder jaar de ouders er op te wijzen dat ze bezwaar kunnen maken tegen foto's op de website. Dat is niet helemaal zoals de wet dat eist, maar het is wel een praktische oplossing voor ouders én school.'

Ik adviseer altijd wel om foto's op de website van de school te beveiligen, ouders hebben alleen toegang. Als de school een foto op sociale media wil zetten, is het verstandig daar wel apart toestemming voor te vragen. Een foto op Facebook of Twitter wordt niet meer op de school, maar in Amerika opgeslagen. Ook voor een folder of de schoolgids kan je het beste apart toestemming vragen. Vooraf regelen kan achteraf vragen en chagrijn voorkomen. Er zijn steeds vaker ouders die bewust geen foto's van hun kinderen delen op sociale media. Als ouders geen toestemming hebben gegeven voor gebruik van foto's, dan zorgt de school er natuurlijk voor dat de foto's niet op internet komen.'

## Worden persoonlijke gegevens goed beveiligd?

'Scholen zijn zich niet altijd bewust zijn van hun verantwoordelijkheid. Dan blijken bijvoorbeeld alle leerkrachten toegang te hebben tot de volledige leerlingenadministratie. Soms kan zelfs de conciërge bij de leerlinggegevens. Er is veel te winnen op het gebied van privacy als scholen nadenken over de vraag wie toegang nodig heeft tot welke gegevens. Heb je als school een heel medisch dossier nodig, of kun je volstaan met een samenvatting? Is het nodig om het rapport van een psycholoog op te slaan in je systeem? En hoe lang is het nodig om deze informatie te bewaren? Wie mag deze gegevens bekijken? Alle leerkrachten of alleen de klassendocent en de remedial teacher? Hoe beter er over online privacy wordt nagedacht, des te veiliger het systeem wordt en de kans op misbruik afneemt.'

## Wie is verantwoordelijk voor het beveiligen van deze informatie?

'Wettelijk gezien is het schoolbestuur verantwoordelijk voor hoe er wordt omgegaan met persoonsgegevens binnen de organisatie. Dat betekent dat de school er niet vanuit moet gaan dat de softwareleverancier de gegevens wel goed zal opslaan en beveiligen. De school moet dit goed met de leverancier regelen. En ook tegenover ouders heeft de school wettelijke verplichtingen. De ouders hebben bijvoorbeeld het recht om te zien welke gegevens de school van en over het kind verzamelt. Ze mogen de informatie ook corrigeren en soms zelfs verwijderen.'

## Scholen gebruiken steeds vaker programma's die resultaten van leerlingen opslaan om daarna oefeningen aan te bieden die aansluiten bij hun niveau. Wat betekent deze ontwikkeling voor de privacy van kinderen?

'Er komt veel meer informatie beschikbaar over het leren van leerlingen. Neem het educatieve softwareprogramma RekenTuin als voorbeeld. Het programma analyseert precies waar een

kind goed en slecht in is. Deze data worden verzameld om een kind beter te kunnen helpen met rekenen. Daar zijn het onderwijs én de leerling echt mee geholpen. Maar juist omdat zo'n programma persoonlijke informatie bewaart, is het belangrijk afspraken te maken over wat er met deze gegevens wordt gedaan. Je wilt toch niet als ouder dat je kind opeens een aanbod voor bijscholing van een particulier huiswerkinstituut krijgt, omdat je kind slecht scoorde op RekenTuin? Ouders moeten er op kunnen vertrouwen dat scholen zorgvuldig met de persoonlijke gegevens omgaan.'

## Wat kunnen ouders en docenten zelf doen?

'Ik adviseer docenten om bijvoorbeeld collega's te vragen naar hun ervaringen met bepaalde apps en software. Of vraag het mensen van de ict-afdeling. En wil je Facebook gebruiken in de klas? Stel Facebook dan zo in dat de informatie die jij erop plaatst, niet automatisch zichtbaar is voor iedereen. Of zomaar gedeeld kan worden. Je hoeft dus niet bang te zijn voor het gebruik van apps, sociale platforms of educatieve software op school. Maar je moet wel weten wat er met de gegevens van en over de leerlingen gebeurt.'





# VUISTREGELS VOOR PRIVACY

Hoe kun je als ouder nagaan of bedrijven en scholen zorgvuldig omgaan met de gegevens van je kind? Er zijn 5 wettelijke eisen waaraan moet worden voldaan:

## 1 Doel

Persoonsgegevens worden altijd verzameld met een vooraf vastgesteld doel. Eenmaal verzamelde gegevens mogen dus niet zomaar voor een heel nieuw doel gebruikt worden.

## 2 Doelbinding

Persoonsgegevens mogen alleen worden verwerkt voor zover dat nodig is om het vastgestelde doel (punt 1) te bereiken. Gegevens die daar geen verband mee houden, mogen dus ook niet worden verwerkt.

## 3 Grondslag

Persoonsgegevens mogen alleen verzameld worden als daar een wettelijke grondslag voor geeft. Voor het onderwijs is dat:

*a. Toestemming:* als de betrokkene toestemming geeft (bijvoorbeeld het vinkje aanklikken bij een inschrijfformulier).

*b. Overeenkomst:* gegevens mogen verzameld worden als dat nodig is voor uitvoering van de overeenkomst met de betrokkene (bijvoorbeeld de onderwijs-overeenkomst).

*c. Wet:* als de wet eist dat persoonsgegevens verwerkt worden (bijvoorbeeld voor het doorgeven van leerlinginformatie aan het ministerie van OCW).

*d. Gerechtvaardigd belang:* dit is het geval als het verzamelen van de persoonsgegevens belangrijker is dan het privacybelang van de betrokkene.

Dit vereist een zorgvuldige belangenafweging. De betrokkene mag zich verzetten tegen verwerking van zijn persoonsgegevens met deze grondslag.

## 4 Dataminimalisatie

Het verzamelen van persoonlijke gegevens moet minimaal zijn. De persoonsgegevens moeten redelijkerwijs nodig zijn om het doel te bereiken; ze moeten in verhouding staan tot het doel. Het doel kan niet met minder dan deze verzamelde gegevens worden bereikt.

## 5 Transparantie en rechten betrokkene

De betrokkene is vooraf in begrijpelijke taal geïnformeerd over wat er precies aan informatie wordt verwerkt en wat het doel daarvan is. De betrokkene heeft het recht op inzage, correctie en soms verzet of verwijdering van zijn persoonsgegevens.

# COLOFON

*Kinderen en online privacy* is een uitgave van Digibewust en Mijn Kind Online, onderdeel van Kennisnet.

Websites: [www.digibewust.nl](http://www.digibewust.nl),  
[www.mijnkindonline.nl](http://www.mijnkindonline.nl),  
[www.kennisnet.nl](http://www.kennisnet.nl)

Copyright: Mijn Kind Online/Kennisnet, Zoetermeer, april 2014

**Eindredactie** Martine Borgdorff, Remco Pijpers

**Teksten** Margreet Algra, Lotte Boot, Martine Borgdorff, Hester Otter, Job Vos

**Vormgeving** Yvette van Diepen (i.o.v. Tappan Communicatie)

**Fotografie** Rodney Kersten, Bigstock, Shutterstock

Deze uitgave is ook te downloaden van [www.mijnkindonline.nl/publicaties](http://www.mijnkindonline.nl/publicaties)



Hoe ga je prettig met elkaar om in WhatsApp? De les WhatsAppHappy maakt problemen met chatten bespreekbaar. Gratis te downloaden op [www.kennisnet.nl](http://www.kennisnet.nl)

Kennisnet

mijn kind  
Online

DiGi**bewust**

