|  |  |
| --- | --- |
| Logo | Informatiebeveiliging & privacy  goed geregeld! |
| ***Deel 1: De AVG - wat is dat eigenlijk?*** | |
| De AVG, informatiebeveiliging en privacy (IBP) - veelgehoorde termen, maar wat moet en kun je er eigenlijk mee in het onderwijs?  In negen IBP-berichten met animatiefilmpjes ben je helemaal up-to-date! In deel 1: de AVG.  [*Klik op het puzzelstukje voor een korte introductie!*](https://www.youtube.com/watch?v=A0yudch_5_U&t=0s&index=2&list=PLQI9hXCcoK1RYAfdrUXfFP4gXBN_GRhLf)  **Wat is de AVG?**  AVG staat voor de Algemene Verordening Gegevensbescherming, in het Engels the General Data Protection Regulation (GDPR). Deze nieuwe Europese privacywetgeving is op 25 mei 2018 ingegaan en iedere organisatie, ook scholen, moeten hieraan voldoen. Deze wetgeving gaat over de bescherming van privacygevoelige informatie en persoonsgegevens.  **Wat betekent privacy?**  Privacy is het recht om met rust gelaten te worden en om gegevens over jezelf (persoonsgegevens) te kunnen controleren. De privacywetgeving stelt eisen aan het verwerken\* van persoonsgegevens*.* Verwerken betekent alles dat je met persoonsgegevens kunt doen, van verzamelen tot vernietigen. | |  | | --- | | **En wat zijn persoonsgegevens?**  Persoonsgegevens zijn alle gegevens waarmee je direct of indirect mensen kunt identificeren. Denk bijvoorbeeld aan naam, adres en woonplaats, maar ook telefoonnummers en postcodes met huisnummers. Gegevens zoals ras, godsdienst of gezondheid worden als bijzondere persoonsgegevens gezien. Deze worden door de wetgever extra beschermd.  Om onderwijs te geven, hebben scholen gegevens nodig. Denk aan personeels- of leerlingdossiers. Maar volgens de AVG mag je alleen gegevens verwerken die strikt noodzakelijk zijn.    De AVG geeft ook meer rechten aan betrokkenen om controle over hun eigen persoonsgegevens te hebben en te houden. Betrokkenen zijn degenen op wie de persoonsgegevens betrekking hebben zoals medewerkers en leerlingen.  Meer weten? In [deze video](https://youtu.be/BB2owgG_vWE) legt Job Vos, privacy-expert bij Kennisnet, uit waarom privacy zo belangrijk is voor scholen. | |
| **\***Hetverwerken van persoonsgegevens is een erg ruim begrip, hieronder verstaan we in ieder geval:  het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, doorzenden, verspreiden, beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en het vernietigen van persoonsgegevens. | |
| **De AVG in de praktijk**  Volgens de AVG is het bevoegd gezag van een organisatie verantwoordelijk voor de verwerking en beveiliging van persoonsgegevens, ofwel de verwerkingsverantwoordelijke. In het onderwijs is dit het schoolbestuur. Als bestuur zorgen we daarom voor naleving van de AVG en moeten we dit ook kunnen aantonen.    De uitvoering van de AVG doen we in de dagelijkse praktijk met elkaar. Daarom vragen we de komende weken je aandacht voor deze berichten over informatiebeveiliging en privacy. Hiermee ben je helemaal up-to-date over wat de nieuwe wetgeving betekent voor scholen, medewerkers en leerlingen. | **Wie controleert dit alles?**  Om ervoor te zorgen dat de AVG wordt nageleefd, heeft elk lid van de EU een toezichthouder. In Nederland is dat de Autoriteit Persoonsgegevens (AP). Als de AP oordeelt dat wij als school niet (kunnen aantonen dat we) voldoen aan de AVG kunnen we daarop aangesproken worden of zelfs een flinke boete krijgen.  Meer informatie hierover kun je vinden op de site van de [Autoriteit Persoonsgegevens (AP).](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving)   * [versterking en uitbreiding van privacyrechten](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg#wat-merken-mensen-van-wie-persoonsgegevens-worden-verwerkt-van-de-avg-6211) * [meer verantwoordelijkheden voor organisaties](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg#wat-zijn-de-belangrijkste-veranderingen-voor-organisaties-6195) * [boetebevoegdheid voor alle Europese privacy toezichthouders](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-informatie-avg#hoe-hoog-zijn-de-boetes-onder-de-avg-6198) * [Scholen en de AVG](https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/onderwijs/scholen-de-avg)   De AP heeft voor het onderwijs een lessenserie gemaakt. Hiermee kun je leerlingen uitleggen wat privacy betekent. Zelf aan de slag? Bekijk het lespakket hier:   * [Lespakket: Privacy in de klas](https://primaindeklas.nl/lesson/index/314?hash=46c9614f) |
| Als medewerker van <naam schoolbestuur> vraagt dit van ons dat we weten:   * welke privacywetgeving van toepassing is, wat persoonsgegevens zijn en wat er allemaal onder verwerken valt. * dat we het recht hebben op een zorgvuldige omgang met onze persoonsgegevens. Hier moeten we op kunnen vertrouwen, ook als leerling. * hoe we zorgvuldig en verantwoord met persoonsgegevens moeten omgaan. Het aantoonbaar naleven van de privacywetgeving is alleen mogelijk als *iedereen* binnen de school daaraan meewerkt. | |
|  | |
| *Sleutelwoorden deel 1: GDPR, AVG, Privacywetgeving, verwerken, persoonsgegevens, verwerkingsverantwoordelijke, betrokkenen en de Autoriteit Persoonsgegevens.* | |
| **De volgende keer: Informatiebeveiliging en privacy (IBP)** | |
| *De serie IBP-berichten is mogelijk gemaakt door Kennisnet en de PO-Raad*  *Informatiebeveiliging en privacy goed geregeld  <naam schoolbestuur>* | |

|  |  |
| --- | --- |
| Logo | Informatiebeveiliging & privacy  goed geregeld! |
| ***Deel 2: Informatiebeveiliging en privacy (IBP) - hoe werkt dat?*** | |
| De AVG, informatiebeveiliging en privacy (IBP) - veelgehoorde termen, maar wat moet en kun je er eigenlijk mee in het onderwijs? In negen IBP-berichten met filmpjes ben je helemaal up-to-date! In deel 2: informatiebeveiliging en privacy.  [*Klik op het puzzelstukje voor een korte introductie!*](https://www.youtube.com/watch?v=-BBd9kBGTto&index=2&list=PLQI9hXCcoK1RYAfdrUXfFP4gXBN_GRhLf)  **Waar gaat IBP over?**  Op school maken we steeds meer gebruik van ict, zowel in de lessen als bij administratieve werkzaamheden. Daardoor zijn scholen steeds afhankelijker van ict en verwerken ze steeds meer privacygevoelige informatie, zoals persoonsgegevens in het leerlingvolgsysteem, zorgdossiers en rapporten.  De inzet van ict brengt nieuwe risico’s met zich mee zoals internet uitval door een DDos-aanval of een datalek door het verlies van een usb-stick met leerlinggegevens erop. Het is daarom belangrijk dat we samen zorgvuldig omgaan met persoonsgegevens van leerlingen en medewerkers. Als school moeten we de privacy van iedereen waarborgen en moet het onderwijs altijd door kunnen gaan.  De AVG geeft aan hoe we dat kunnen doen en binnen welke kaders we persoonsgegevens mogen verwerken. Daarbij stelt de AVG ook eisen aan de beveiliging van deze gegevens. Privacy kan niet gegarandeerd worden zonder informatiebeveiliging. | **Hoe werkt Informatiebeveiliging?**  Informatie moet:   * op het juiste moment voor handen zijn (beschikbaarheid) * juist zijn (integriteit) * alleen toegankelijke zijn voor de juiste personen (vertrouwelijkheid)     Doordat scholen zo afhankelijk zijn van informatie en ict, worden deze drie aspecten steeds belangrijker. Daarom nemen we als school maatregelen om beveiligingsincidenten te voorkomen en de eventuele gevolgen daarvan te beperken.  Meer weten over beschikbaarheid, integriteit en vertrouwelijkheid (BIV)? Lees dan het document [BIV classificatie](https://maken.wikiwijs.nl/userfiles/0990223a6857ccc182e5430bf19e25fef68a3c98.pdf)  **Wat is privacy ook alweer?**  Privacy is het recht om met rust te worden gelaten en om gegevens over jezelf (persoonsgegevens) te kunnen controleren.    Lees meer over privacy in IBP-bericht 1: de AVG |
| *“Privacy niet belangrijk vinden omdat je niets te verbergen hebt, is hetzelfde als niet geven om vrijheid van meningsuiting omdat je niets te zeggen hebt.”*  Edward Snowden | |
| **De AVG en IBP in de praktijk**  Door IBP goed te regelen kunnen we samen de privacy van iedereen (alle betrokkenen) waarborgen en de voortgang van het onderwijs en de bedrijfsvoering van de school garanderen.  De privacywetgeving helpt ons hierbij.  Artikel 5 van de AVG geeft een aantal basisregels voor het omgaan met persoonsgegevens. Deze kun je gemakkelijk onthouden aan de hand van 5 vuistregels.    Meer weten over de basisregels? Bekijk het document [‘De 5 vuistregels voor privacy 2.0.](https://www.kennisnet.nl/fileadmin/kennisnet/publicatie/Kennisnet-5-vuistregels-voor-privacy2.0.pdf) | In artikel 24 en 32 van de AVG staat dat we persoonsgegevens die we gebruiken ook moeten  beschermen met ‘passende technische en organisatorische maatregelen’ rond de beschikbaarheid, integriteit en vertrouwelijkheid van de (persoons)gegevens.  Deze maatregelen komen terug in afspraken en procedures die we hebben vastgelegd in een gedragscode. Voorbeelden daarvan komen in de volgende IBP-berichten terug. |
| Als medewerkers van <naam schoolbestuur>vraagt dit van ons dat we weten:   * waar IBP voor staat en waarom het belangrijk is om dit samen goed op te pakken. * wat de basisregels zijn als we persoonsgegevens verwerken. Bij het verzamelen, registreren en verwerken van persoonsgegevens gebruiken we altijd de 5 vuistregels. * wat passende technische en organisatorische maatregelen zijn. Deze komen terug in de afspraken, protocollen en procedures die we op school hebben gemaakt en vastgelegd. * dat we van elkaar kunnen verwachten dat we deze afspraken nakomen en waar nodig de procedures volgen. | |
|  | |
| *Sleutelwoorden deel 2: IBP, informatiebeveiliging, privacy, ‘5 vuistregels’, beschikbaarheid, integriteit, vertrouwelijkheid* | |
| **C:\Kennisnet\Puzzel awareness\nieuwe vorm puzzelstukjes\drive-download-20180923T082535Z-001\Datalekken.png**  **De volgende keer: Datalekken** | |
| *De serie IBP-berichten is mogelijk gemaakt door Kennisnet en de PO-Raad*  *Informatiebeveiliging en privacy goed geregeld  <naam schoolbestuur>* | |

|  |  |
| --- | --- |
| Logo | Informatiebeveiliging & privacy  goed geregeld! |
| ***Deel 3: Hoe voorkom je een datalek?*** | |
| De AVG, informatiebeveiliging en privacy (IBP) - veelgehoorde termen, maar wat moet en kun je er eigenlijk mee in het onderwijs? In negen IBP-berichten met animatiefilmpjes ben je helemaal up-to-date! In deel 3: datalekken.  [*Klik op het puzzelstukje voor een korte introductie!*](https://www.youtube.com/watch?v=KMokn46yHe8&index=3&list=PLQI9hXCcoK1RYAfdrUXfFP4gXBN_GRhLf)  **Waarom moet ik iets weten over datalekken?**  In de vorige IBP-berichten heb je ontdekt wat de AVG en IBP inhouden en dat we persoonsgegevens goed moeten beschermen. Dat betekent ook dat we  ervoor zorgen dat deze niet in verkeerde handen vallen.  Wanneer dat wel gebeurt, dan spreken we van het ‘lekken’ van persoonsgegevens. In dat geval hebben we de verplichting om een datalek te melden bij de Autoriteit Persoonsgegevens (AP) - deze meldplicht datalekken geldt voor alle organisaties, dus ook voor scholen.  In sommige gevallen moet het datalek ook gemeld worden bij de betrokkenen - degenen van wie de persoonsgegevens zijn ‘gelekt’. | **Een datalek, wat is dat eigenlijk?**  Een datalek is een inbreuk op de informatiebeveiliging waarbij persoonsgegevens verloren gaan of in handen komen van derden die geen toegang tot die gegevens mogen hebben.  Dat is soms lastig vast te stellen, daarom is de bewijslast omgedraaid. Het is dus een datalek als toegang door onbevoegden niet uitgesloten kan worden.  **Datalek ontdekt? Meld het!**  Je ontdekt, veroorzaakt of vermoed een datalek - waar moet je dit melden? Dit kan bijvoorbeeld via het daarvoor bestemde e-mailadres of bij je directe leidinggevende. In de gedragscode van de school staat dit precies beschreven. Maak altijd melding van een (mogelijk) datalek! We gaan dan kijken hoe het lek is ontstaan en hoe we het in toekomst kunnen voorkomen. Met de juiste maatregelen kunnen we daarna (verdere) schade beperken. Als schoolbestuur moeten we een datalek direct (liefst binnen 72 uur) melden aan de Autoriteit Persoonsgegevens. |
| Wat is bijvoorbeeld een datalek?   * Het verlies van een usb-stick of laptop met daarop persoonsgegevens van leerlingen of medewerkers. * Het verlies van een smartphone. Deze geeft toegang tot veel informatie zoals de gesynchroniseerde e-mail van school, notities of een automatische inlog in schoolsystemen. * ‘Offline’ datalekken zoals documenten met persoonsgegevens in de papierbak, leerlingverslagen op het bureau of meegenomen dossiers uit een kwijtgeraakte tas. * Een computer thuis, die gehackt of gestolen wordt waarop bijvoorbeeld een Excelbestand met leerlinggegevens staat. Gehackte bestanden, een DDoS-aanval of inbraak in een databestand. * Een e-mail met persoonsgegevens verstuurd naar de verkeerde persoon of personen.   Meer weten over hoe een DDoS-aanval werkt en wat je er tegen kunt doen? Bekijk het dossier [‘DDoS-aanval op school’](https://www.kennisnet.nl/artikel/ddos-aanvallen-op-school-dit-kan-je-er-tegen-doen/) van Kennisnet. | |
| **De AVG en datalekken in de praktijk**  Het is niet de vraag óf een school te maken krijgt met een datalek, maar eerder wanneer. Met technische maatregelen kunnen we veel datalekken voorkomen, maar de menselijke factor blijft altijd belangrijk. Iedereen heeft de verantwoordelijkheid om bewust en zorgvuldig met persoonsgegevens om te gaan.  We hebben afspraken over het veilig werken met persoonsgegevens, vastgelegd in een gedragscode. Hiermee kunnen we samen het risico op datalekken beperken. Waar moet je bijvoorbeeld op letten?   * Verstuur geen persoonsgegevens per e-mail, WhatsApp of andere sociale media. Niet mailen, maar delen! * Beveilig apparatuur met een wachtwoord en vergrendel je pc als je even weg gaat. * Vraag geen toegang tot meer gegevens dan je voor je werk nodig hebt. * Laat je devices buiten de school nooit onbeheerd achter, ook niet in een auto die op slot zit. * Sla persoonsgegevens niet op, op je eigen pc, laptop of telefoon. * Houd je school e-mail en privé e-mail gescheiden. | Dat klinkt allemaal logisch, maar vraagt wel om meer alertheid. Help elkaar om hier aan te denken. Zo kunnen we er samen voor zorgen dat persoonsgegevens veilig blijven - zowel van leerlingen, ouders, docenten als directieleden en bestuurder.  [*Klik hier voor ‘6x zorgvuldig*](https://www.kennisnet.nl/fileadmin/kennisnet/publicatie/Datalek_posterIBP.pdf)  Ieder datalek kan grote nadelige gevolgen hebben voor leerlingen (en hun ouders), medewerkers, maar ook voor onze school. Datalekken kunnen rekenen op flinke (negatieve) media-aandacht en veroorzaken imagoschade. Daarnaast staan er hoge boetes op datalekken of het niet tijdig melden ervan . |
| Als medewerker van <naam schoolbestuur> vraagt dit van ons dat we weten:     * wat een datalek is en welke afspraken er binnen <naam schoolbestuur> zijn om het risico daarop te verkleinen. * dat we een (mogelijk) datalek altijd moet melden via het afgesproken e-mailadres of aan de directe leidinggevende. * wat de gevolgen kunnen zijn als we bijvoorbeeld onze school e-mail synchroniseren met een ander apparaat. We weten welke stappen we moeten en kunnen nemen bij het verlies van het device. | |
|  | |
| *Sleutelwoorden deel 3: Meldplicht, datalek, afspraken e-mail en gebruik persoonsgegevens* | |
| **C:\Kennisnet\Puzzel awareness\nieuwe vorm puzzelstukjes\Sociale media.png**  **De volgende keer: sociale media** | |
| *De serie IBP-berichten is mogelijk gemaakt door Kennisnet en de PO-Raad*  *Informatiebeveiliging en privacy goed geregeld  <naam schoolbestuur>* | |

|  |  |
| --- | --- |
| Logo | Informatiebeveiliging & privacy  goed geregeld! |
| ***Deel 4: hoe ga je om met sociale media?*** | |
| De AVG, informatiebeveiliging en privacy (IBP) - veelgehoorde termen, maar wat moet en kun je er eigenlijk mee in het onderwijs? In negen IBP-berichten met animatiefilmpjes ben je helemaal up-to-date! In deel 4: sociale media.  [*Klik op het puzzelstukje voor een korte introductie!*](https://www.youtube.com/watch?v=-Bot8YM85Ms&index=4&list=PLQI9hXCcoK1RYAfdrUXfFP4gXBN_GRhLf)  **Wat zijn sociale media eigenlijk?**  ‘Sociale media’ is een verzamelnaam voor alle internettoepassingen waarmee je leuk en eenvoudig met elkaar kunt communiceren en informatie met elkaar kunt delen, bijvoorbeeld:   * tekst: nieuws, artikelen of chatberichten. * geluid: podcasts, muziek of spraakberichten. * beeld: foto’s, video of animaties.   Denk bij sociale media onder meer aan Instagram, YouTube, Facebook, Twitter, WhatsApp, LinkedIn en Snapchat.  Belangrijk om hierbij te onthouden is dat wat je deelt via sociale media vaak een eigen leven gaat leiden, waardoor je niet langer meer de enige eigenaar of verspreider ervan bent. Wat je deelt kun je dus niet meer ongedaan maken. | **Hoe ga je verantwoord om met sociale media?**  De school heeft afspraken over het gebruik van sociale media in de gedragscode vastgelegd. Het uitgangspunt is dat je je op school, zowel online als offline, aan dezelfde gedragsregels moet houden.  Wil je iets delen via sociale media, vraag je dan steeds af in welke rol je dat doet en wat de  afspraken er over zijn.    Meer weten? Lees de publicatie [‘Sociale media en schoolmedewerkers: de valkuilen.’](https://www.kennisnet.nl/fileadmin/kennisnet/publicatie/Sociale-media-en-schoolmedewerkers.pdf)  **Sociale media in de klas en mediawijsheid**  Om goed met sociale media om te gaan op school heb je mediawijsheid nodig. Je bent mediawijs wanneer je je online kritisch en bewust gedraagt. En als leraar draag je deze vaardigheden ook over op je leerlingen. Mediawijsheid helpt je bewust te zijn van zowel de valkuilen als voordelen van sociale media. Gaat er toch iets mis? Meld dit dan, zodat we samen naar een oplossing kunnen zoeken. |
| **Mediawijsheid en de inzet van sociale media in het onderwijs**  Het verantwoord inzetten van sociale media in het onderwijs leer je vooral via nieuwe vaardigheden, zoals digitale geletterdheid en mediawijsheid. Meer weten over mediawijsheid en sociale media, lees hier verder:   * [Het competentiemodel mediawijsheid van Mediawijzer](https://www.mediawijsheid.nl/competentiemodel/) * De ‘[Monitor Jeugd en Media’ van Kennisnet 2017](https://www.kennisnet.nl/artikel/monitor-jeugd-en-media-2017-minder-digitaal-vaardig-dan-gedacht/) * [Het artikel 'Welk effect heeft overmatig gebruik van sociale media op leerlingen?' van Kennisnet](https://www.kennisnet.nl/artikel/welk-effect-heeft-overmatig-gebruik-van-sociale-media-op-leerlingen/) * [Het artikel 'Wat kun je doen met sociale media in de klas?' van Leraar2](https://www.leraar24.nl/wat-kun-je-doen-met-sociale-media-in-de-klas/) * [Het artikel 'Hoe maak je leerlingen mediawijs?' van Leraar24](https://www.leraar24.nl/hoe-maak-je-leerlingen-mediawijs/) * [Brochures over de omgang met terreur op sociale media, van Kennisnet](https://www.kennisnet.nl/artikel/omgaan-met-terreur-op-sociale-media/) | |
| **De AVG en sociale media in de praktijk**  Ouders beslissen over de privacy van hun kinderen als deze jonger zijn dan 16 jaar. De AVG stelt dat ouders in een aantal gevallen toestemming moeten geven als hun kind gebruik maakt van bepaalde  digitale diensten, zoals sociale media en apps.    Wil je deze digitale diensten in de les met leerlingen gebruiken, dan is hiervoor vooraf apart (per app of dienst) toestemming nodig van de ouders (of wettelijk vertegenwoordigers) van leerlingen jonger dan 16 jaar.  Houd er dus rekening mee dat dit gevolgen heeft voor de snelheid waarmee je deze diensten kunt inzetten. | Binnen <naam schoolbestuur> hebben we afspraken over de inzet van sociale media en apps in de les vastgelegd in de gedragscode. Digitale diensten, zoals sociale media, worden binnen onze school niet ingezet zonder overleg en goede afwegingen vooraf. Houd er rekening mee dat ouders niet in alle gevallen toestemming zullen geven.  **Er is een uitzondering:**  Voor het gebruik van digitale leermiddelen van de  diverse uitgevers gelden andere regels. Hiervoor sluit de school aparte verwerkersovereenkomsten af om de privacy van de leerlingen en de beveiliging van de persoonsgegevens te waarborgen. Hierover meer in IBP-bericht 5. |
| Als medewerker van <naam schoolbestuur> vraagt dit van ons dat we weten:   * wat sociale media zijn en welke voor- en nadelen ze hebben. * dat mediawijsheid en sociale media hand in hand gaan. Mediawijsheid geeft ons en de leerlingen de kennis en vaardigheden om leuk en veilig met sociale media om te kunnen gaan. * welke afspraken over sociale media er in de gedragscode van de school staan. * dat voor de inzet van sociale media in de klas vooraf een juiste afweging, onderbouwing én toestemming van de ouders nodig is bij leerlingen jonger dan 16 jaar. | |
|  | |
| *Sleutelwoorden deel 4: sociale media, rol, mediawijsheid, sociale media en 16-jarigen, digitale diensten, toestemming ouders* | |
| **C:\Kennisnet\Puzzel awareness\nieuwe vorm puzzelstukjes\drive-download-20180923T082535Z-001\Cloud.png**  **De volgende keer: de Cloud** | |
| *De serie IBP-berichten is mogelijk gemaakt door Kennisnet en de PO-Raad*  *Informatiebeveiliging en privacy goed geregeld  <naam schoolbestuur>* | |

|  |  |  |  |
| --- | --- | --- | --- |
| Logo | | Informatiebeveiliging & privacy  goed geregeld! | |
| ***Deel 5: Hoe ga je om met werken in de cloud?*** | | | |
| De AVG, informatiebeveiliging en privacy (IBP) - veelgehoorde termen, maar wat moet en kun je er eigenlijk mee in het onderwijs? In negen IBP-berichten met animatiefilmpjes ben je helemaal up-to-date! In deel 5: de cloud.  [*Klik op het puzzelstukje voor een korte introductie!*](https://www.youtube.com/watch?v=7QfSKeB_o1I&index=5&list=PLQI9hXCcoK1RYAfdrUXfFP4gXBN_GRhLf)  **Wat is de cloud eigenlijk?**  Als je in de cloud werkt heb je via je device toegang tot je werkbestanden en applicaties via het internet. Schoolgegevens en digitaal lesmateriaal zijn hierdoor overal, op elk moment en met verschillende devices te gebruiken.  Het is niet altijd zichtbaar of duidelijk waar precies de gegevens staan, daarom wordt de term cloud gebruikt. Alle gegevens staan opgeslagen op een server (van bijvoorbeeld de leverancier) in een datacenter, die via het internet te bereiken is. | | Cloud computing heeft naast veel voordelen ook aandachtspunten. Met leveranciers van clouddiensten moet je contracten afsluiten en afspraken maken over de beveiliging van de (privacygevoelige) gegevens. Werken in de cloud stelt ook eisen aan je internetverbinding. Verder moet je er rekening mee houden dat elke clouddienst zijn eigen helpdesk heeft. Dit kan soms onhandig zijn wanneer je snel een probleem op moet lossen.  **De cloud en privacy afspraken**  Op school gebruiken we steeds vaker digitaal lesmateriaal dat via de cloud beschikbaar is. Leerlingen en medewerkers loggen online in met hun e-mailadres, gebruikersnaam of persoonsgebonden nummer om toegang te krijgen.  (Persoons)gegevens worden dan buiten de deur verwerkt en opgeslagen. Maar het bevoegd gezag (de bestuurder) is en blijft volgens de AVG altijd verantwoordelijk voor de bescherming van die persoonsgegevens. Daarom zijn we verplicht om met alle leveranciers van online-lesmateriaal afspraken te maken over:   * welke persoonsgegevens zij in opdracht van ons mogen verwerken. * de beveiliging van deze gegevens   Voor elke leverancier leggen we die afspraken vast in een zogenaamde verwerkersovereenkomst.  Meer weten over verwerkersovereenkomsten?  Bekijk dan [Het privacyconvenant](https://www.privacyconvenant.nl/) | |
| **Dataopslag in de cloud**  Als je (persoons)gegevens opslaat in een eigen clouddienst zoals Dropbox of je persoonlijke Google Drive, hebben we als school geen controle meer over het gebruik en de beveiliging ervan. Daarom is het opslaan van schoolgegevens waaronder persoonsgegevens in privé dropboxen en persoonlijke Google Drives binnen het <naam schoolbestuur> niet toegestaan.  Sla school- en persoonsgegevens altijd op de daarvoor afgesproken plaatsen op. Dit kan het eigen netwerk of een eigen private cloud van de school zijn. Zie hiervoor de afspraken die zijn vastgelegd in de gedragscode verantwoord gebruik bedrijfsmiddelen. | | | |
| **De AVG en cloud in de praktijk**  De AVG bepaalt ook dat persoonsgegevens alleen opgeslagen en uitgewisseld mogen worden met de EU-lidstaten, plus Noorwegen, Liechtenstein en IJsland. Met andere landen, de zogenaamde ‘derde landen’, mogen we alleen gegevens uitwisselen als deze landen een passend beschermingsniveau hebben.  De Verenigde Staten hebben bijvoorbeeld géén  passend beschermingsniveau. Persoonsgegevens doorgeven aan of opslaan bij een organisatie in de Verenigde Staten mag alleen als die organisatie is aangesloten bij het EU-VS Privacy Shield.  Meer weten? Bekijk de lijst van organisaties die aangesloten zijn bij [Privacy Shield.](https://www.privacyshield.gov/list)  **Waar je aan moet denken voor het gebruik van**  **online digitaal lesmateriaal**  Voordat je in de klas gebruik kan maken van online digitaal lesmateriaal, educatieve apps of niet-educatieve apps heb je toestemming nodig van de school. Bijvoorbeeld via de ict-coördinator of je directe leidinggevende. Mogelijk zijn er aanvullende maatregelen nodig voor het gebruik. Zoals controle waar de data komt te staan, aanschaf van een licentie of het afsluiten van een verwerkersovereenkomst. Hiervoor hebben we een stappenplan en een aanvraagformulier gemaakt. Beide documenten zijn terug te vinden op <plaats document> | | **Register met alle verwerkingen**  Als school moeten we naast het naleven van de AVG ook kunnen aantonen dat we dit doen. We zijn bijvoorbeeld wettelijk verplicht om vast te leggen welke persoonsgegevens we zelf verwerken en welke gegevens we door andere organisaties in onze opdracht laten verwerken. Daarbij moeten we ook aangeven in welk land de persoonsgegevens worden opgeslagen.  Onder deze organisaties vallen naast de grote leveranciers van digitaal lesmateriaal ook de aanbieders van bijvoorbeeld (gratis) apps. Het is daarom belangrijk dat we van te voren weten welke persoonsgegevens een cloudapplicatie gebruikt en waar deze worden opgeslagen. | |
| Als medewerkers van <naam schoolbestuur> vraagt dit van ons dat we weten:   * wat werken in de cloud precies is en welke voor- en nadelen het heeft. * dat we het gebruik van digitaal lesmateriaal en apps altijd moet aanvragen en/of melden volgens de afgesproken procedure. Hierdoor kunnen we vooraf de juiste maatregelen nemen, zoals het afsluiten van een eventuele verwerkersovereenkomst en het vastleggen in het dataregister. * waar we werkgerelateerde (persoons)gegevens bij <naam schoolbestuur> wel en niet mogen opslaan. * dat we altijd veilig, tijd-, plaats- en device-onafhankelijk kunnen werken in de ‘private cloud’ van onze school. | | | |
|  | | | |
| *Sleutelwoorden deel 5: cloud computing, verwerkersovereenkomst, public cloud, private cloud, aanvragen digitaal lesmateriaal, EU-VS Privacy Shield. register van verwerkingen.* | | | |
| **C:\Kennisnet\Puzzel awareness\nieuwe vorm puzzelstukjes\drive-download-20180923T082535Z-001\Werkplek.png**  **De volgende keer: de werkplek** | | | |
| *De serie IBP-berichten is mogelijk gemaakt door Kennisnet en de PO-Raad*  *Informatiebeveiliging en privacy goed geregeld  <naam schoolbestuur>* | | | |
| Logo | | Informatiebeveiliging & privacy  goed geregeld! | |
| ***Deel 6: Hoe houd je je werkplek veilig?*** | | | |
| De AVG, informatiebeveiliging en privacy (IBP) - veelgehoorde termen, maar wat moet en kun je er eigenlijk mee in het onderwijs? In negen IBP-berichten met animatiefilmpjes ben je helemaal up-to-date! In deel 6: de werkplek.  [*Klik op het puzzelstukje voor een korte introductie!*](https://www.youtube.com/watch?v=xWc7-zBu4U4&index=6&list=PLQI9hXCcoK1RYAfdrUXfFP4gXBN_GRhLf)  **Bedrijfsmiddelen - wat zijn dat eigenlijk?**  Om je werk te kunnen doen krijg je van school de beschikking over bedrijfsmiddelen zoals:   * een device (een computer, laptop) * software (het leerling administratiesysteem, outlook en digitaal lesmateriaal) * gegevens van leerlingen of medewerkers * netwerkfaciliteiten zoals internet     In de gedragscode van de school hebben we afspraken over het gebruik hiervan vastgelegd, de werkplek is hier onderdeel van. Op je werkplek zorg je ervoor dat anderen geen (onbedoelde) toegang kunnen krijgen tot gegevens en bedrijfsmiddelen waar ze geen rechten voor hebben. | | De volgende elementen zijn daar onderdeel van:  **Gebruik een veilig wachtwoord en deel deze nooit**  Een gebruikersnaam en wachtwoord geven je toegang tot de gegevens en applicaties die je nodig hebt om je werk te doen. Een wachtwoord is persoonlijk en mag absoluut niet gedeeld worden.    Meer weten over wachtwoorden? Bekijk het filmpje: [‘Hoe kraakt iemand mijn wachtwoord?](https://www.youtube.com/watch?v=sCMotoEV3TY)’  **Vermijd usb-sticks**  Een usb-stick lijkt handig om bestanden mee naar huis te nemen of bijvoorbeeld door te geven aan collega’s. Helaas kleven er aan het gebruik van usb-sticks grote risico’s. Zo kan er een virus op staan of kun je een usb-stick met leerlinggegevens verliezen.  Als die gegevens niet versleuteld zijn, wordt dit gezien als een datalek. We kunnen dan niet uitsluiten dat onbevoegden toegang hebben gekregen tot de gegevens op de usb-stick. Zo’n verlies moet je daarom altijd melden via het daarvoor bestemde e-mailadres of via je directe leidinggevende.    Meer weten? Bekijk IBP-Bericht 3: datalekken.  Het gebruik van een usb-stick is alleen toegestaan als alle bestanden op de usb-stick ‘versleuteld’ zijn, ook wel encryptie genoemd. Een voorbeeld in Windows 10 is Bitlocker. | |
| **Vergrendel je computer**  Koffie halen of even de klas uit? Vergrendel je computer!  In Windows doe je dit bijvoorbeeld door de toetsencombinatie **WINDOWSTOETS + L**  Zo voorkom je dat onbevoegden toegang kunnen krijgen tot je bestanden of ten onrechte persoonsgegevens kunnen zien en/of bewerken.    *LET OP*:  Clean desk (een leeg bureau) is net zo belangrijk als clear screen (een leeg beeldscherm). Laat daarom geen papieren documenten, zoals leerlingdossiers, op je bureau liggen. | | | |
| **De AVG en je werkplek in de praktijk**  Om verantwoord en volgens de AVG te werken met persoonsgegevens hebben we een aantal basisvaardigheden nodig. Het is belangrijk dat alle medewerkers, maar ook leerlingen en ouders, zich bewust zijn van de risico’s rondom privacy en het gebruik van persoonsgegevens. Dat begint bij het zorgvuldig omgaan met persoonsgegevens op de werkplek. Dit is handig samengevat in ‘Bewust 6x Zorgvuldig’. | | Let op de extra afspraken rond een eigen device  Gebruik je je eigen device (BYOD - bring your own device) om voor school werkzaamheden te doen? Zoals een smartphone, iPad, laptop of je pc thuis? Dan hebben we hiervoor aanvullende afspraken gemaakt in onze gedragscode. Dit zijn onder meer:   * een eigen device moet in ieder geval beveiligd zijn met een goed wachtwoord. * je mag geen bestanden met persoonsgegevens van leerlingen en/of medewerkers opslaan op de harde schijf van je eigen device. * je moet ervoor zorgen dat je antivirus programma up-to-date is en dat alle Windows-updates zijn bijgewerkt. * je moet op een eigen device altijd via de private cloud van de school werken. Je kunt daardoor overal veilig bij je schoolwerk. Usb-sticks of het mailen van bestanden is daarmee overbodig. | |
| Als medewerkers van <naam schoolbestuur> vraagt dit van ons dat we weten:   * waar een goed wachtwoord aan voldoet, we vervangen dat regelmatig en bewaren het op een veilige plek. We geven ons wachtwoord nooit aan iemand anders. * waar we (persoons)gegevens van de school zorgvuldig kunnen opslaan. Daarvoor gebruiken we de private cloud van de school (zeker via BYOD en thuis) en geen usb-sticks. * hoe we als medewerker onze werkplek veilig en verantwoord gebruiken. We vergrendelen onze pc of device als we er niet achter zitten. Niet alle informatie is voor iedereen bestemd. * dat we papieren documenten niet laten slingeren. Hebben we ze niet meer nodig dan vernietigen we ze met de papierversnipperaar. Clean desk is net zo belangrijk als clear screen. | | | |
|  | | | |
| *Sleutelwoorden deel 6: Werkplek, bedrijfsmiddelen, wachtwoord, usb-stick, versleuteld, encryptie, Windows-logotoets+L , clear screen/ clear desk, bewust 6x zorgvuldig, BYOD* | | | |
| **C:\Kennisnet\Puzzel awareness\nieuwe vorm puzzelstukjes\drive-download-20180923T082535Z-001\Veilig online.png**  **De volgende keer: veilig online** | | | |
| *De serie IBP-berichten is mogelijk gemaakt door Kennisnet en de PO-Raad*  *Informatiebeveiliging en privacy goed geregeld  <naam schoolbestuur>* | | | |

|  |  |
| --- | --- |
| Logo | Informatiebeveiliging & privacy  goed geregeld! |
| ***Deel 7: Hoe blijf je veilig online?*** | |
| De AVG, informatiebeveiliging en privacy (IBP) - veelgehoorde termen, maar wat moet en kun je er eigenlijk mee in het onderwijs? In negen IBP-berichten met animatiefilmpjes ben je helemaal up-to-date! In deel 7: veilig online.  [*Klik op het puzzelstukje voor een korte introductie!*](https://www.youtube.com/watch?v=Ly460GwEjNo&list=PLQI9hXCcoK1RYAfdrUXfFP4gXBN_GRhLf&index=7)  **Veilig online - wat betekent dat?**  Iedereen is via allerlei devices, steeds meer online.  Daar zitten veel voordelen aan: je beschikt op elk moment snel over informatie vanaf elk device. Maar er kleven ook nadelen aan. Let daarom goed op wat je online doet, vooral wanneer je privé en werk combineert op dezelfde devices.  Wil je een app gebruiken, dan moet je meestal inloggen met een gebruikersnaam of e-mailadres met een wachtwoord. Op websites moet je cookies accepteren. Zo laat je een online voetafdruk met veel (persoonlijke) informatie achter. En die gegevens zijn geld waard. | Meer weten over hoe een online voetafdruk werkt? Bekijk filmfragment van [‘Dave, een fantastische waarzegger.’](https://www.youtube.com/watch?v=E8gBOSsMwZw)  **Persoonsgegevens online delen**  Als je persoons gegevens (online) deelt met anderen, dan moet je erop kunnen vertrouwen dat de ontvanger er zorgvuldig mee om gaat. Ook ouders verwachten dat wij als medewerkers van <naam schoolbestuur> zorgvuldig omgaan met de persoonsgegevens van hun kinderen. Hiervoor heb je kennis en vaardigheden nodig om met de digitale wereld om te gaan.  **Onbeveiligde netwerken**  Best gemakkelijk dat je wifi hebt zonder dat je hoeft in te loggen? Dat is dus een onbeveiligd netwerk. Voor hackers wordt het zo heel eenvoudig om je smartphone, tablet of computer voor de gek te houden. Met speciale apparatuur kan een netwerk aangemaakt worden met de naam van het openbare wifi-netwerk (zoals de bibliotheek, een café of de trein) waar je apparaat vervolgens verbinding mee maakt. Hierna kan een hacker meekijken met wat je doet of gegevens stelen, zoals werkgegevens van de school. Vermijd daarom gratis openbare wifi-netwerken. |
| **Klik niet klakkeloos**  Heb je ooit een Phishing mail gehad?  Phishing (afgeleid van vissen en hengelen) is een vorm van internetfraude. Je wordt, via bijvoorbeeld een link in een mailtje, naar een valse website gelokt met bijvoorbeeld het verzoek om je inloggegevens te controleren. Als je hier – nietsvermoedend – je inlognaam en wachtwoord of je creditcardnummer invult, krijgt de fraudeur achter de schermen de beschikking over deze gegevens met alle gevolgen van dien. De fraudeur doet zich hierbij vaak voor als een vertrouwde instantie of persoon, zoals een bank, het postkantoor of zelfs een familielid. | |
| **Wat zijn cookies eigenlijk?**  Een cookie is een tekstbestandje dat door een server op uw computer, smartphone of tablet kan worden geplaatst. Cookies onthouden dat je bent ingelogd op een site, welke artikelen er in je winkelmandje zitten, je voorkeursinstellingen en worden gebruikt voor statistieken.  Dat kan handig zijn, maar wil je het altijd? Daarvoor is er de cookiewet die eist dat je duidelijk geïnformeerd wordt en expliciet toestemming moet geven voor NIET-noodzakelijke cookies, die jouw privacy kunnen schenden. De beslissing is aan jou. | **Hoe veilig ben jij online?**  Weet jij waar malware vandaan komt? En of je automatische updates op je pc altijd moet goedkeuren? Doe de zelf-check via [Nederland Veilig Online!](http://www.nederlandveiligonline.nl/quiz/)  Als je zelf de valkuilen kent en hoe je daarmee om moet gaan, dan kun je ook leerlingen helpen ‘online bekwaam’ te worden. |
| Als medewerkers van <naam schoolbestuur> vraagt dit van ons dat we weten:   * welke risico’s er online zijn en dat we terughoudend moeten zijn met het online plaatsen van (persoons)gegevens (niet alleen op school, maar ook thuis). * wat de gevolgen kunnen zijn van het gebruik van openbare wifi-netwerken. * wat malware en phishing zijn en hoe we het kunnen herkennen. * welke maatregelen we zelf kunnen nemen om veilig online te zijn. | |
|  | |
| *Sleutelwoorden deel 7: online gegevens, cookies, onbeveiligde netwerken, openbare netwerken, malware, phishing* | |
| **C:\Kennisnet\Puzzel awareness\nieuwe vorm puzzelstukjes\drive-download-20180923T082535Z-001\Delen _ Mailen.png**  **De volgende keer: delen & mailen** | |
| *De serie IBP-berichten is mogelijk gemaakt door Kennisnet en de PO-Raad*  *Informatiebeveiliging en privacy goed geregeld  <naam schoolbestuur>* | |

|  |  |
| --- | --- |
| Logo | Informatiebeveiliging & privacy  goed geregeld! |
| ***Deel 8: Liever delen dan mailen!*** | |
| De AVG, informatiebeveiliging en privacy (IBP) - veelgehoorde termen, maar wat moet en kun je er eigenlijk mee in het onderwijs? In negen IBP-berichten met animatiefilmpjes ben je helemaal up-to-date! In deel 8: delen en mailen.  [*Klik op het puzzelstukje voor een korte introductie!*](https://www.youtube.com/watch?v=Z3XlbduEPQA&list=PLQI9hXCcoK1RYAfdrUXfFP4gXBN_GRhLf&index=8)  **Wanneer deel je gegevens?**  We delen allemaal, bewust of onbewust, steeds meer informatie over onszelf, leerlingen en hun ouders. Herken je het telefoontje waarin even tussendoor gevraagd wordt om de geboortedatum en het land van herkomst van een leerling? Of dat mailtje dat je stuurt naar collega’s, met daarin de namen van een aantal dyslectische leerlingen?  **Persoonsgegevens - wanneer mag je ze delen?**  Het is belangrijk dat je weet welke gegevens je mag vastleggen, met wie je die mag delen en op welke manier. Je mag bijvoorbeeld niet zomaar persoonsgegevens doorgeven aan de gemeente, een collega-school, de leerplichtambtenaar of zelfs je collega’s.  Soms hebben we een wettelijke plicht om een aantal persoonsgegevens te delen. Bijvoorbeeld met DUO. DUO is ook verwerkingsverantwoordelijke, net als de school, en is dan ook zelf verantwoordelijk voor de bescherming van die persoonsgegevens. | Maar we delen ook persoonsgegevens met leveranciers van digitaal lesmateriaal of een app waarbij je inlogt met een e-mailadres en wachtwoord. In die gevallen blijft de school eindverantwoordelijk voor wat de andere partij met de persoonsgegevens doet. De school maakt dan afspraken met de leverancier over het gebruik en beveiliging van de persoonsgegevens.  Meer weten over hierover? Bekijk IBP-bericht 5: de cloud.  **Wanneer mail je gegevens?**  Het lijkt misschien gemakkelijk om die collega die erom vroeg, even de lijst te mailen met dyslectische leerlingen. Helaas is e-mail geen veilige manier om persoonsgegevens te delen. Deel privacygevoelige informatie daarom nooit via de mail, ook niet intern.  **Hoe deel je gegevens dan wel?**  De vuistregel is: liever delen dan mailen. Om je collega’s toegang te geven tot bepaalde informatie stuur je een link naar het bestand in bijvoorbeeld de beveiligde cloud- of netwerkomgeving van de school. Daarmee weet je dat alleen iemand met de link én de juiste toegangsrechten bij het bestand kan.  Steeds vaker kun je documenten via een beveiligde verbinding uploaden naar een andere organisatie. Een beveiligde verbinding kun je herkennen aan ‘https’ in het webadres en het slotje ervoor.  Je mag persoonsgegevens alleen mailen als je het bestand beveiligd met een wachtwoord. Spreek af dat je het wachtwoord op een andere manier doorgeeft, bijvoorbeeld telefonisch. Dat verkleint ook het risico op datalekken.  Meer weten over datalekken? Bekijk IBP-bericht 3. |
| *Uit* [*Do’s en don’ts*](https://maken.wikiwijs.nl/userfiles/4ea179414c1d5fec3476193dd8135d01d02a0805.pdf) *van Kennisnet* | |
| **Delen & mailen en de AVG in de praktijk**  Wanneer je persoonsgegevens wilt delen met anderen, denk dan eerst na of dit wel zomaar mag.  De AVG stelt dat je niet meer gegevens mag delen dan strikt noodzakelijk zijn voor het beoogde doel.  Deel bijvoorbeeld niet alle NAW-gegevens van een leerling als alleen de woonplaats gevraagd wordt. En misschien is het voldoende als je de gegevens anoniem maakt. Dataminimalisatie is een belangrijke basisregel bij het verzamelen, opslaan en delen van persoonsgegevens. | Weet jij wat persoonsgegevens zijn en welke bijzondere persoonsgegevens extra beschermd worden door de privacywetgeving?  Persoonsgegevens delen begint met je bewust zijn van de basisregels voor het verantwoord omgaan met persoonsgegevens.  Meer weten over de AVG en de basisregels, de 5 vuistregels? Bekijk IBP-bericht 1 en 2. |
| Als medewerkers van <naam schoolbestuur>vraagt dit van ons dat we weten:   * hoe we zorgvuldig persoonsgegevens kunnen delen, met wie we ze mogen delen en op welke manier. Eerst denken dan delen en bij twijfel navragen! * dat e-mail geen veilige manier is om (gevoelige)persoonsgegevens in welke vorm dan ook te delen. * welke afspraken er over het gebruik van e-mail en het delen van (persoons)gegevens bij <naam schoolbestuur> zijn gemaakt. | |
|  | |
| *Sleutelwoorden deel 8: eerst denken dan delen, grondslagen, afspraken e-mailgebruik, dataminimalisatie, zorgvuldig en verantwoord.* | |
| C:\Kennisnet\Puzzel awareness\nieuwe vorm puzzelstukjes\drive-download-20180923T082535Z-001\Beeldmateriaal.png  **De volgende keer: beeldmateriaal** | |
| *De serie IBP-berichten is mogelijk gemaakt door Kennisnet en de PO-Raad*  *Informatiebeveiliging en privacy goed geregeld  <naam schoolbestuur>* | |

|  |  |
| --- | --- |
| Logo | Informatiebeveiliging & privacy  goed geregeld! |
| ***Deel 9: Hoe ga je om met beeldmateriaal?*** | |
| De AVG, informatiebeveiliging en privacy (IBP) - veelgehoorde termen, maar wat moet en kun je er eigenlijk mee in het onderwijs? In negen IBP-berichten met animatiefilmpjes ben je helemaal up-to-date! In deel 9: beeldmateriaal.  [*Klik op het puzzelstukje voor een korte introductie!*](https://www.youtube.com/watch?v=tQo09LDfCgY&list=PLQI9hXCcoK1RYAfdrUXfFP4gXBN_GRhLf&index=9)  **Moet je altijd toestemming vragen?**  Schoolfeestje of excursie en meteen de foto’s en filmpjes online zetten? Hoewel het goed bedoeld is en zelden een probleem vormt, mag het niet zomaar. Beeldmateriaal van personen zijn persoonsgegevens, daarom stelt de privacywetgeving eisen aan het verwerken ervan. Voor het openbaar publiceren van beeldmateriaal van leerlingen, is vooraf toestemming nodig. Bij leerlingen jonger dan 16 jaar komt de toestemming van de ouders en als de leerling 16 jaar of ouder is moet deze zelf toestemming geven.    Zonder aantoonbare toestemming mogen er geen foto’s en video’s van leerlingen gebruikt worden. | **Hoe kun je beeldmateriaal wel delen?**  Wanneer er toestemming is, moet de school ook zorg dragen voor het veilig delen van beeldmateriaal.  Een openbaar fotoalbum mag bijvoorbeeld niet meer. Ook werkgerelateerde foto’s of filmpjes (met leerlingen of collega’s erop) op je eigen sociale media profielen plaatsen, is niet toegestaan.  Foto’s worden daarom op een beveiligd deel van de schoolwebsite geplaatst waar ouders moeten inloggen. Ook hier mogen alleen foto' s van kinderen geplaatst worden waarvan we als school kunnen aantonen dat er toestemming voor gegeven is.  **Filmen en fotograferen door ouders**  Het aantal ouders dat met camera’s en smartphones foto's maakt of filmt op school is in de afgelopen jaren flink toegenomen. Ook dit beeldmateriaal komt al snel op Facebook of YouTube terecht. Dat verbieden, is lastig. Maar we kunnen als school hierover wel afspraken maken met ouders. De school is niet zomaar een openbare plaats waar iedereen mag komen. We moeten ervoor zorgen dat de school een veilige omgeving is waarin leerlingen, ouders en collega’s niet ongewild gefotografeerd of gefilmd worden. |
| Wanneer een ouder een foto kopieert vanuit de beveiligde omgeving van de school en deze zelf (publiek) deelt op bijvoorbeeld Facebook, draagt de ouder daar verantwoordelijkheid voor. De school kan dit helaas niet verbieden.  Meer weten over beeldmateriaal en privacy? Bekijk het [Persbericht beeldmateriaal leerlingen](https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-roept-scholen-op-zorgvuldig-om-te-gaan-met-beeldmateriaal-van-leerlingen) van de Autoriteit Persoonsgegevens. | |
| **De AVG en beeldmateriaal in de praktijk**  De AVG stelt duidelijke eisen aan het gebruik van beeldmateriaal. Zonder toestemming mogen er geen foto’s en video’s van leerlingen gebruikt worden.  Bij het vragen om toestemming zijn drie punten van belang:   * het moet in vrijheid gegeven worden. Het moet geweigerd kunnen worden zonder dat leerlingen daardoor benadeeld zouden worden. * het moet 'ondubbelzinnig' zijn. Toestemming mag bijvoorbeeld niet verborgen zijn in schoolregels. Er mag niet van uitgegaan worden dat ouders toestemming geven als zij niet reageren. Ouders of verzorgers moetenexpliciet kunnen aangeven waar ze wel of geen toestemming voor verlenen. En de school moet de toestemming altijd kunnen aantonen. | * het moet specifiek zijn. Het moet duidelijk zijn waar toestemming voor gegeven wordt en met welk doel.   Vraag apart toestemming voor het gebruik van beeld:   * op de website * in de schoolgids * in de nieuwsbrief * op sociale media   LET OP:  Een leerling of ouder moet de gegeven toestemming altijd kunnen intrekken of op een later moment alsnog toestemming kunnen geven.  Als beeldmateriaal geplaatst is met toestemming, dan heeft het intrekken van de toestemming geen gevolgen voor de inmiddels geplaatste foto’s. |
| Als medewerkers van <naam schoolbestuur>vraagt dit van ons dat we weten:   * hoe we zorgvuldig moeten omgaan met beeldmateriaal en wanneer, waarvoor en van wie er foto’s en video’s gebruikt mogen worden. Bij twijfel eerst navragen! * dat zonder aantoonbare toestemming gebruik van beeldmateriaal niet is toegestaan. We hebben hiervoor een duidelijke werkwijze afgesproken. | |
|  | |
| *Sleutelwoorden deel 9: beeldmateriaal, toestemming, jonger dan 16 jaar, fotograferen en ouders, intrekken van toestemming* | |
| C:\Kennisnet\Puzzel awareness\nieuwe vorm puzzelstukjes\Puzzelstukjes_Totaal2.png  *Weet je het even niet meer, twijfel je of heb je vragen?*  *Lees dan de IBP-berichten eens terug of bekijk de filmpjes nog een keer.*  *Kom je er niet uit? Neem dan contact op met <.....> van <naam schoolbestuur>* | |
| *De serie IBP-berichten is mogelijk gemaakt door Kennisnet en de PO-Raad*  *Informatiebeveiliging en privacy goed geregeld  <naam schoolbestuur>* | |