scholengroep opron

Privacy: Passende maatregelen op jouw school

1. Inleiding

Scholen maken steeds beter en meer gebruik van ICT. Daardoor neemt niet alleen het aantal persoonsgegevens dat scholen gebruiken toe. Ook brengt de afhankelijkheid van ICT nieuwe risico's met zich mee, zoals cybercrime en datalekken. Het beschermen van de persoonsgegevens van leerlingen en medewerkers en daarmee het waarborgen van de privacy, wordt dan ook steeds belangrijker. Schoolbestuurders zijn volgens de wet verplicht om privacy goed te regelen.

Wetgeving bepaalt niet alleen onder welke voorwaarden persoonsgegevens gebruikt mogen worden, maar geeft ook aan dat er passende technische en organisatorische maatregelen genomen moeten worden om de persoonsgegevens te beschermen. Informatiebeveiliging is een belangrijke voorwaarde voor privacy, terwijl omgekeerd het zorgvuldig omgaan met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar, en zijn van elkaar afhankelijk.

2. AVG IBP-Beleidsplan OPRON

Het schoolbestuur is verantwoordelijk om informatiebeveiliging en privacy(IBP) te regelen. Het regelen van IBP begint dan ook met een goedgekeurd en bij iedereen bekend gemaakt IBP-beleid. Dat is de basis, de kapstok, om processen, richtlijnen en procedures rondom IBP uit te werken.

- *Actie: AVG IBP beleidsplan OPRON op de website zetten*
- *Actie: AVG IBP beleidsplan OPRON op het intranet www.opronnet.nl zetten*

3. Bewustwording

Beleid en maatregelen zijn niet voldoende om risico's op het gebied van informatiebeveiliging en privacy uit te sluiten. Meestal speelt de mens een belangrijke rol als er beveiligingsincidenten of datalekken zijn ontstaan. Daarom is het erg belangrijk om het bewustzijn bij de medewerkers te vergroten en aan te scherpen.

Zorg ervoor dat alle medewerkers weten wat een beveiligingsincident of een datalek is, en waar ze een beveiligingsincident moeten melden. Medewerkers moeten weten dat zij niet alleen het verlies van een usb-stick, een gestolen laptop et cetera met daarop persoonsgegevens van leerlingen en/of medewerkers moeten melden, maar ook melding moeten doen van die verstuurde e-mail naar de verkeerde geadresseerde.

- *Actie: elke medewerker neemt kennis van de online workshop: https://maken.wikiwijs.nl/99972/Bewustwording_IBP_voor_medewerkers_po_en_vo*

4. Privacyreglement

Iedere school verwerkt persoonsgegevens van personeel en leerlingen. In het privacyreglement leg je vast voor welke doelen je persoonsgegevens registreert. Het gaat hierbij niet alleen om gewone persoonsgegevens zoals naam, geboortedatum en overige contactgegevens, maar soms ook om bijzondere persoonsgegevens met betrekking tot bijvoorbeeld gezondheid, afkomst en godsdienst.

- *Actie: Privacyreglement OPRON op de website zetten*
- *Actie: Privacyreglemet OPRON op het intranet www.opronnet.nl zetten*

5. Privacyverklaring

In de privacyverklaring legt de school uit welke persoonsgegevens worden verzameld en gebruikt en met welk doel.

- *Actie: Privacyverklaring op de website zetten*
- *Actie: Privacyverklaringen van alle scholen OPRON op het intranet www.opronnet.nl zetten*

6. Gebruik beeldmateriaal leerlingen

Schoolfeestje, gezellig! En nu die filmpjes en foto's gelijk op de website... Nee dus. Foto's en video's van leerlingen zijn persoonsgegevens, daarom gelden er vanuit de privacywetgeving eisen voor het gebruik van beeldmateriaal.

6.1. Toestemming vragen:

Het gebruiken van beeldmateriaal, het delen van foto's en video's van leerlingen door scholen, vormt zelden een probleem en is meestal goedbedoeld. Toch eist de wetgever dat de school vooraf toestemming vraagt aan ouders voor het gebruik van beeldmateriaal van leerlingen als de leerling jonger is dan 16 jaar. Als de leerling 16 jaar of ouder is moet hij/zij zelf toestemming geven. Zonder die toestemming mag je geen foto's en video's van leerlingen gebruiken.

Bij het vragen van toestemming zijn drie punten van belang:

De toestemming moet in **vrijheid** gegeven worden; toestemming moet geweigerd kunnen worden zonder dat leerlingen daardoor benadeeld zouden worden.
De toestemming moet **'ondubbelzinnig'** zijn. Toestemming mag niet verborgen zijn in schoolregels en er mag niet van uitgegaan worden dat ouders toestemming geven als zij niet reageren. Ouders/verzorgers moeten expliciet kunnen aangeven waar ze wel of geen toestemming voor verlenen. De school moet de toestemming altijd kunnen aantonen.
De toestemming moet **specifiek** zijn. Het moet duidelijk zijn waar toestemming voor gegeven wordt en met welk doel. Zorg voor gelaagde toestemming: wil je toestemming voor foto's op de website, in de schoolgids, nieuwsbrief of in sociale media? De keuze moet duidelijk aan te geven zijn, bijvoorbeeld door een kruisje in een vakje te zetten bij bepaalde type media (foto's/film) of bij bepaalde uitingen (website, schoolkrant, etc.).

- *Actie: zeer specifiek toestemming aan ouders vragen voor gebruik beeldmateriaal. https://maken.wikiwijs.nl/bestanden/725652/Voorbeeldbrief_toestemming_gebruik_beeldmateriaal.docx (voorbeeld aanpassen aan schoolbehoefte)*

6.2. De wet

Privacy wordt in Nederland geregeld in de Wet bescherming persoonsgegevens. Deze wet wordt op 25 mei 2018 vervangen door strengere Europese privacywetgeving (Algemene Verordening Gegevensbescherming). Foto's en video's van leerlingen zijn persoonsgegevens en vallen daarmee onder deze wet. Daarom gelden er eisen voor het gebruik van beeldmateriaal. Het gaat om alle vormen van gebruik, zoals:

- foto's die je als school in de nieuwsbrief plaatst;
- foto's die je deelt of op sociale media plaatst;
- een video die je vertoont op de website van de school.

Wil je als school via de website of sociale media foto's of video's van leerlingen verspreiden, dan moet je daar altijd toestemming voor vragen. En als ouders willen dat je een foto verwijdert, moet je daar altijd toestemming voor geven.

6.3. Foto's veilig delen

Naast toestemming vragen is de school ook verantwoordelijk voor het veilig delen van beeldmateriaal. Een openbaar fotoalbum mag niet meer. Plaats daarom foto's op een beveiligde site waarbij ouders moeten inloggen. Hou er wel rekening mee dat ook hier alléén foto's komen van kinderen waarvan de ouders toestemming hebben gegeven om foto's te delen!

- *Actie: foto's plaatsen alleen met toestemming.*
- *Actie: beveiligd fotoalbum in mijnschool aanleggen*

6.4. Filmen/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 deze foto's komen al snel op Facebook of YouTube. En wat als een ouder de foto van de beveiligde site kopieert en zelf deelt?

Ook hier geldt dat een school voor álle kinderen een veilige omgeving moet zijn, en niet een plek waar zij (en hun ouders) het risico lopen ongewenst gefotografeerd te worden. Maar het maken van foto's en video's door ouders op school kun je moeilijk verbieden. En als een ouder de foto kopieert en zelf deelt neemt de ouder daar de verantwoordelijkheid voor. De school kan niet verbieden dat ouders die foto's overnemen en verder delen (zelfs niet als dat bijvoorbeeld publiek op Facebook is)... Je kan er wel afspraken over maken, want een school is niet zomaar een openbare plaats waar iedereen toegang toe krijgt.

7. Communiceer!

Het met regelmaat praten over het belang van informatiebeveiliging en privacy helpt om het bewustzijn bij iedereen te vergroten.

8. Afspraken over sociale media

Iedere school heeft wel positieve en negatieve verhalen te vertellen over het gebruik van sociale media door leerlingen (en medewerkers!). Om de online veiligheid van iedereen op school te verbeteren stellen scholen protocollen op, organiseren ze informatieavonden of sluiten ze bepaalde diensten af.

Met een protocol voor gebruik van sociale media (en internet) kun je als school afspraken maken over het gebruik hiervan, zodat voor iedereen duidelijk is wat de regels zijn. Je kunt er voor kiezen om voor leerlingen andere afspraken te maken dan voor medewerkers. Een belangrijk punt hierbij is om te bepalen of medewerkers, die namens of voor de school communiceren, hun eigen sociale media-accounts mogen gebruiken.

Er is geen wettelijke verplichting om zo'n reglement of protocol te maken, maar het helpt wel om bewust om te gaan met sociale media binnen je school en draagt bij aan een sociaal veilig klimaat. Let er wel op dat een protocol of reglement weer de instemming vereist van de (G)MR.

- *Actie: De volgende documenten kunnen helpen bij het maken van afspraken over sociale media bij jou op school.*
  https://maken.wikiwijs.nl/bestanden/729030/Social%20media%20reglement.docx (leerlingen)
  https://maken.wikiwijs.nl/bestanden/729032/social%20media%20protocol%20medewerkers.pdf (medewerkers)
  Voorbeelden naar behoefte per school aanpassen.
- *Ouders (aan het begin van het schooljaar) een toestemmingsformulier laten ondertekenen voor foto's op ouderportaal, Facebook, website.*
- *Ouders verzoeken op school geen foto's te maken en op Facebook te zetten. Bijvoorbeeld tijdens een musical of een schoolfeest.*
- *Internetafspraken met leerkrachten/ ouders en leerlingen.*

9. Uitwisselen van gegevens

9.1. Passend Onderwijs

Als leerlingen extra zorg of begeleiding nodig hebben, legt een school extra persoonsgegevens over de leerling vast, bijvoorbeeld over gezondheid of gedrag. Deze informatie ziet de wet als bijzondere persoonsgegevens. Een school moet extra zorgvuldig omgaan met deze gegevens.

Aparte afspraken
Op het moment dat de school gegevens wil uitwisselen met een andere organisatie, bijvoorbeeld een onderwijskundige, pedagoog of psycholoog, dan moet je daar aparte afspraken over maken. Deze afspraken leg je vast in een verwerkersovereenkomst waarin vertrouwelijkheid van de gegevens centraal staat. Let er ook op dat je bij het inschakelen van een externe deskundige zoals een psycholoog ook de toestemming nodig hebt van de wettelijk verzorgers (ouders).

Soms lukt het niet om de juiste begeleiding op de school zelf te regelen. Dan schakel je het samenwerkingsverband passend onderwijs (afgekort: swv) in, bijvoorbeeld voor een toelaatbaarheidsverklaring passend onderwijs.

Samenwerkingsverband passend onderwijs (Swv)
Het swv is een zelfstandige organisatie. De wet beschrijft dat het swv een zelfstandige wettelijke taak heeft. In privacytermen is het swv een ‘verwerkingsverantwoordelijke’, en dus zelf verantwoordelijk voor de gegevens van leerlingen. Zodra de school leerlinggegevens aanlevert aan het swv, is het swv verantwoordelijk voor de privacybescherming. Het swv is dus géén verwerker voor de school. Een schoolbestuur sluit dus géén verwerkersovereenkomst af met het swv. De wet regelt dat de school gegevens mag uitwisselen met het swv. De vijf vuistregels blijven uiteraard wél van toepassing.

- *Actie: gegevens versleutelen indien overdracht plaatsvindt via mailverkeer! In Office365 wordt bovenschools een knop ‘beveiliging’ toegevoegd aan de mail!*
- *Actie: toestemming vragen aan ouders voor gegevensoverdracht*

Jeugdhulpverlening
Het kan voorkomen dat een leerling extra ondersteuning nodig heeft, dat er thuis problemen zijn of dat een leerling met politie en justitie in aanraking is gekomen. In al deze gevallen wissel je gevoelige gegevens uit over leerlingen. Omdat de school gegevens uitwisselt met andere organisaties, moet duidelijk zijn hoe iedereen omgaat met de privacy van de leerlingen.

Basiszorg
De basiszorg voor jeugd en gezin is meestal per gemeente geregeld. Om gegevens met deze organisaties uit te kunnen wisselen is het belangrijk om afspraken te maken in een convenant (‘privacyconvenant sociale wijkteams’), en om in een privacyreglement te beschrijven wat ieders rechten en plichten zijn.

Externe partners
Het Nederlands Jeugdinstituut heeft een handreiking gemaakt voor scholen die samenwerken met externe partners. Deze handreiking geeft informatie en praktische tips over hoe je om moet gaan met privacy en wat wel en niet mag binnen de kaders van de wet.

Gezondheidsprojecten
Scholen krijgen regelmatig de vraag om mee te werken aan onderzoeken over de gezondheid van leerlingen.

- *Actie: Alleen als de ouders of leerlingen expliciet toestemming hebben gegeven, mogen de gemeenten de gezondheidsgegevens verwerken. Toestemming vragen.*
- *Actie: mailverkeer versleutelen!*

9.2. Uitwisseling leerlingdossiers en OKR

9.2.1. Primair onderwijs

Om ervoor te zorgen dat leerlingen in het basisonderwijs op hun nieuwe school de juiste ondersteuning en begeleiding krijgen, is in de 'Wet primair onderwijs' geregeld dat de basisschool de nieuwe school voorziet van een onderwijskundig rapport (okr). Bij de overstap naar de middelbare school noemt men dit ook wel het overstapdossier. Na overleg met het onderwijzend personeel stelt de directie dit rapport op. Het rapport moet een goede, doorlopende leerlijn voor elke leerling garanderen.

Voor de uitwisseling van het okr tussen de basisschool en de nieuwe school (po of vo), is geen toestemming van de ouders nodig. Ouders kunnen dan ook geen bezwaar maken tegen de uitwisseling van die informatie: de school moet de informatie hoe dan ook uitwisselen. Wel hebben ouders het recht op inzage van het overstapdossier vóórdat dit wordt uitgewisseld. Inzage heeft geen aanpassing van het rapport tot gevolg. Bezwaren en opmerkingen van de ouders worden apart vastgelegd en toegevoegd aan het dossier. De school moet de mogelijkheid tot inzage van ouders schriftelijk vastleggen in het leerlingdossier. Hiermee maakt de school het controleerbaar dat de informatieplicht is nageleefd. Deze informatieplicht ligt immers wettelijk vast.

9.2.2. Voortgezet onderwijs

Ook de 'Wet voortgezet onderwijs' kent een overstapdossier. Het gaat daarbij om het contact met een andere school of instelling voor ander onderwijs, ten behoeve van de in- en uitschrijving van de leerling. Onder dit contact vallen alle uitwisselingen van leergegevens en de direct met het leren samenhangende begeleidingsgegevens.

Het uitgangspunt van het okr is dat de scholen alleen gegevens overdragen die zij relevant vinden voor de nieuwe school.

De oude school mag dus niet het gehele leerlingdossier ongezien doorsturen, maar alleen die gegevens die nodig zijn om de leerling op de nieuwe school goed te begeleiden en te laten leren.

- *Actie: toepassing naar behoefte indien nodig*

9.3. Leerplicht en verzuim

Nederland is verdeeld in 39 Regionale Meld- en Coördinatiepunten (RMC) voor voortijdig schoolverlaters (vsv'ers). Elke RMC-regio heeft een contactgemeente die de melding en registratie van voortijdig schoolverlaters coördineert en zorg draagt voor mogelijkheden van doorverwijzing en herplaatsing in het onderwijs.

9.3.1. Wat mag een leerplicht-/RMC-ambtenaar nu eigenlijk opvragen?

Belangrijk uitgangspunt bij het delen van informatie is:

- Wat regelt de wet (grondslag)
- Dataminimalisatie.

1. Leerplichtambtenaren hebben vanuit de Leerplichtwet een wettelijk recht op informatie, waarbij het vooral gaat om verzuiminformatie.
2. Een leerplichtambtenaar heeft alleen recht op die informatie die hij/zij strikt noodzakelijk nodig heeft voor de uitoefening van het werk. Een leerplichtambtenaar hoeft niet te zien dat een voorbeeldige leerling één uur mist…

9.3.2. Een leerplicht-/RMC-ambtenaar mag geen andere persoonsgegevens verwerken dan:

1. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens van de leerplichtige;
2. een administratienummer dat geen andere informatie bevat dan bedoeld onder a;
3. nationaliteit en geboorteplaats;
4. gegevens als bedoeld onder 1, van de ouders, voogden of verzorgers van de leerplichtige;
5. gegevens met betrekking tot de inschrijving of afschrijving van de leerplichtige;
6. gegevens ten aanzien van het schoolverloop, het schoolverzuim en van het beroep op een vrijstelling van de leerplicht;
7. andere dan de onder 1 tot en met 6 bedoelde gegevens waarvan de verwerking is vereist of noodzakelijk is met het oog op de toepassing van de Leerplichtwet 1969 of een andere wet.

Andere informatie delen mag niet. Een account in een leerlingvolgsysteem (Magister, Parnasys , SOMtoday, enz) mag dan ook niet! (Daar mag een ambtenaar van gemeente of RMC zelfs niet eens om vragen!)

- *Actie: toepassing naar behoefte indien nodig*

10. Wie mogen gegevens inzien?

Wie mogen eigenlijk de gegevens op school inzien? De vuistregel dataminimalisatie zegt het volgende:

- Je gebuikt niet meer persoonsgegevens dan strikt noodzakelijk.
- Je zorgt ervoor dat niet meer mensen toegang hebben tot die persoonsgegevens dan nodig is.

Een conciërge zal niet altijd hoeven te weten welke leerlingen extra begeleiding nodig hebben, en de cijfers van wiskunde zijn niet altijd relevant voor een aardrijkskundedocent.

Dat betekent dat vastgelegd moet worden met wie persoonsgegevens uitgewisseld en intern gedeeld worden, wie toegang heeft tot bepaalde persoonsgegevens in de verschillende informatiesystemen. Zodat het inzichtelijk is wie, of welke rol, geautoriseerd is om bepaalde verwerkingen van (persoons)gegevens te doen. De (informatie)systemen die de school gebruikt, moeten zijn ingericht op basis van deze rolverdeling.

Het is van belang om (informatie)systemen zo in te richten, dat alleen die medewerkers geautoriseerd zijn om bepaalde persoonsgegevens te verwerken, die dat voor hun werkzaamheden nodig hebben.

- *Actie: deKlas.nu/ MOO voorzien van de juiste autorisaties. (Bijv. Administratie niet op de Leerkrachtschijf)*
- *Actie: LVS: juiste autorisaties geven.* ***LET OP! Het mag werkbaar blijven!*** *Totale afscherming is niet nodig. De Autoriteit persoonsgegevens moet hier nog uitspraken over doen.*
- *Actie: afspraken maken over het beheer van fysieke leerlingdossiers.*

11. D)DoS, wat moet ik weten...

Een (D)Dos-aanval op school: dit kan iedereen overkomen. Je systemen liggen plat, je netwerk is traag en iedereen belt je met vragen. En jij vraagt je af: Wat moet ik doen?
Wat is een DDoS-aanval?
Een (distributed) denial-of service of (D)DoS-aanval is één van de bedreigingen, die de continuïteit van het onderwijs steeds vaker in gevaar brengen. De aanval heeft als doel om de beschikbaarheid van een systeem te onderbreken. Het zorgt er bijvoorbeeld voor dat de website of de geplande digitale toets niet bereikbaar is. Dit gebeurt meestal door het versturen van meer verzoeken dan het systeem kan afhandelen. Wanneer een aanval vanaf meerdere computers (soms wel duizenden tegelijk) wordt uitgevoerd, dan is er sprake van een DDoS-aanval. Vaak wordt gebruik gemaakt van een zogenaamd botnet, een verzameling van computers die onder de controle van de aanvaller(s) zijn gekomen. Het is dan ook belangrijk om maatregelen tegen deze bedreiging te nemen, zodat het onderwijs door kan gaan.

DDoS-aanval op school: wat nu?
Het is niet eens de vraag of je als school te maken krijgt met een DDoS-aanval, maar meer wanneer. Wees er op voorbereid. Kennisnet heeft, in samenwerking met politie, scholen en leveranciers, een handig informatiedossier opgesteld over DDoS-aanvallen op school. In dit dossier vind je meer informatie over dit onderwerp.

Behalve informatie over DDoS-aanvallen, behandelt het dossier ook de maatregelen die bestuurders, ict-coördinatoren en technisch medewerkers moeten nemen vooraf en tijdens een aanval. Zij zijn tenslotte samen verantwoordelijk voor de continuïteit van goed werkende en veilige ict-toepassingen op school. In de drie stappen herkennen, aanpak en preventie, wordt per takenpakket uitgelegd hoe jij jouw school zo goed mogelijk kan beschermen tegen DDoS-aanvallen en/of de gevolgen daarvan.

- Actie: bekijk het dossier http://kn.nu/ddos-op-school

12. Maatregelen op Teamniveau

12.1. Aandachtspunten

- Wees terughoudend met het gebruik van USB-sticks. (lees: gebruik GEEN USB-sticks!) Mocht je hier persoonsgegevens op willen slaan, zorg dan dat deze versleuteld zijn en het wachtwoord alleen bij jou en de eventuele rechtmatige ontvanger bekend zijn.
- Gebruik in plaats van USB sticks liever de beveiligde cloud-omgevingen die OPRON in gebruik heeft (Office365, MOO, ESIS/Leerwinst, Cito, Basispoort, etc.) voor het opslaan of delen van persoonsgegevens.
- Delen vanuit Office365 is toegestaan.
- Mailen naar meerdere personen? Gebruik :BCC
- Gebruik MOO-bestanden om gegevens op te slaan.
- Gebruik Onedrive in jouw Office365-account om gegevens op te slaan.
- Gebruik geen gezamenlijke inlogaccounts en wachtwoorden. Zorg dat iedereen een eigen account heeft dat toegang geeft tot wat hij/zij echt nodig heeft.
- Mail op persoonlijke titel en niet vanuit groepsmail-accounts.
- Gebruik groepsmailaccounts (bijv. groep3@.....school.nl) voor inkomende mail. Uitgaande mail dus via een persoonlijk account versturen!
- Persoonsgegevens via de mail ALTIJD met toestemming versleuteld versturen.
- Indien je jouw werkplek verlaat, zorg dan dat anderen geen gebruik kunnen maken van jouw gegevens. (afmelden of vergrendelen (**Windows-toets + L**)
- Laat geen papieren leerlinggegevens slingeren in de klas.
- Klassenmap zo mogelijk sluiten. Zeker aan het eind van een werkdag.
- Beheer je eigen inloggegevens en geef deze niet af.
- Geen wachtwoorden laten slingeren.
- Discreet omgaan met kopiëren, kopieën en scannen.
- Maak 2 à 3 invaller-accounts aan in deKlas.nu/ MOO.
- Persoonlijke fysieke documenten (rapport) ook persoonlijk meegeven.

13. Maatregelen op Leerlingenniveau

13.1. Dialoog met leerlingen

Ook leerlingen maken steeds meer gebruik van digitale middelen om te leren en te communiceren. Als je bedenkt dat 95% van de leerlingen in groep 8 een smartphone heeft en een groot deel actief is op sociale media, is het helemaal niet gek om in de klas het gesprek aan te gaan over hoe zij hun privacy kunnen bewaken en hoe zij met de privacy van mede-leerlingen omgaan. Want mag je je wachtwoord met iemand delen? Maar ook: Hoe gaan we met elkaar om op sociale media?

Naast slachtoffer op internet kunnen jongeren ook dader zijn door bijvoorbeeld de schoolwebsite te hacken of het systeem plat te leggen met een DDos-aanval. Wanneer er anti-pestregels zijn, een anti-pestcontract of een gedragscode ict- en internetgebruik, wordt dit meestal klassikaal besproken. Maar hoe praat je nu eigenlijk in de klas over informatiebeveiliging en privacy?

13.2. Hoe ga je het gesprek aan met leerlingen over IBP?

- Actie: hulpvragen voor les informatiebeveiliging https://maken.wikiwijs.nl/bestanden/716457/25%20hulpvragen%20informatiebeveiliging.pdf
- Actie: hulpvragen voor les privacy https://maken.wikiwijs.nl/bestanden/716456/25%20hulpvragen%20privacy.pdf
- Actie: ook de Autoriteit Persoonsgegevens heeft een aantal lessen gemaakt over privacy om in de klas te gebruiken https://primaindeklas.nl/lesson/index/314?hash=46c9614f

13.3. Aandachtspunten

- Laat leerlingen zo veel mogelijk persoonlijk inloggen in deKlas.nu/ MOO.
- Zorg dat leerlingen hun eigen MOO- wachtwoord zélf instellen.

DO'S EN DON'TS

Zo bewaakt u de privacy

Met enige regelmaat verschijnen er in het nieuws berichten over het uitlekken van persoonlijke gegevens. Wachtwoorden, gebruikersnamen: het ligt dan allemaal op straat. Een school wil dit natuurlijk écht niet op haar geweten hebben. Neem daarom de juiste voorzorgsmaatregelen om de gegevens van de leerlingen te beschermen. Hieronder vindt u een aantal do's en don'ts over privacy, opgesteld door Kennisnet. TEKST JOB VOS

DO'S

Zorg voor dataminimalisatie
Verzamel alleen de gegevens die nodig zijn om het beoogde doel te bereiken en bewaar ze niet langer dan nodig is voor dat doel.

Ga verstandig om met wachtwoorden Houd wachtwoorden geheim en verander ze regelmatig. Op die manier voorkomt u dat iemand kan rondneuzen in bestanden met privacygevoelige informatie.

Denk na voordat u handelt
Wetgeving op het gebied van privacy is ingewikkeld, maar daar is een goede reden voor: privacy is een grondrecht dat bescherming vereist. Denk dus na wanneer u aan de slag gaat met privacygevoelige gegevens.
Stel uzelf de vraag: hoe zou ik het vinden als het om mijn gegevens zou gaan?

Bij twijfel: niet doen
Twijfelt u over het gebruik van privacygevoelige gegevens? Gebruik ze dan niet en win eerst informatie in over wat wel en niet mag.

Blijf kritisch
Iedereen heeft zijn eigen belangen. Wees u hiervan bewust wanneer er privacygevoelige gegevens in het spel zijn. Een leverancier die zegt dat er geen bewerkersovereenkomst nodig is, heeft misschien geen zin in rompslomp. Maar het kan ook zijn dat hij de persoonsgegevens zelf ergens voor wil gebruiken.

DON'TS

Gegevens verzamelen zonder doel
Verzamel niet zomaar gegevens of informatie. Stel eerst vast wat uw doelen zijn. Zorg dat uw gegevensverzamelingen in overeenstemming zijn met uw privacybeleid en privacyreglement.

Eerder verzamelde gegevens gebruiken voor een ander doel
Eerder verzamelde gegevens mogen niet zomaar voor een compleet ander doel worden gebruikt. Wil uw school gegevens gebruiken die niet verzameld zijn voor het geven van onderwijs, dan is daar toestemming voor nodig. Een voorbeeld: een foto op een toegangspasje is noodzakelijk om de leerling toegang te geven tot het schoolgebouw. Een foto voor het online smoelenboek is niet noodzakelijk voor het geven van onderwijs, maar slechts een extraatje. De foto die is verstrekt voor de schoolpas, mag zonder aparte toestemming niet worden gebruikt voor het smoelenboek.

Ervan uitgaan dat iemand toestemming geeft De wet eist soms dat toestemming nodig is voor het gebruik van persoonsgegevens. U mag mensen niet dwingen om toestemming te geven. Ook het 'aannemen' van die toestemming is niet hetzelfde als toestemming vragen. De school mag bijvoorbeeld niet melden: 'we gaan er van uit dat u toestemming geeft voor het gebruik van de foto's van uw kinderen in de nieuwsbrief. Als u dat niet wilt, moet u maar...'. Dit noemen we een 'opt-out', en dat is niet toegestaan wanneer actieve toestemming nodig is (opt-in).

Gele memo's gebruiken
De toegang tot digitale systemen moet goed zijn beveiligd tegen verlies, beschadiging en diefstal van persoonsgegevens. Het is niet verstandig om het wachtwoord van de leerlingenadministratie op een geel briefje te schrijven en aan de monitor te plakken. U legt uw bankpas toch ook niet direct naast het briefje waar u de pincode op heeft geschreven?

Op de website van Kennisnet (www.kennisnet.nl) vindt u meer informatie over het thema privacy.