Toepassing van de Wet Bescherming Persoonsgegevens, protocol Datalekken Kindante

Versiebeheer

Versienummer	Auteur	Wijziging/aanpassing
1.0	E.Toussaint	20 januari 2017
1.1	E.Toussaint	28 februari 2017
1.2	E.Toussaint	1 april 2017
1.3	E.Toussaint	19 april 2017

Inhoud

Privacywetgeving wordt steeds belangrijker, Informatie t.b.v. privacy waarborging in het Primair Onderwijs:

Convenant Digitale Onderwijsmiddelen en Privacy – Leermiddelen en toetsen

Digitale leermiddelen zijn niet meer weg te denken in het onderwijs. Het is belangrijk dat bij het gebruik van deze leermiddelen de privacy van leerlingen is beschermd. Daarom sluiten de scholen, vertegenwoordigd door de PO- en de VO-raad, en aanbieders van dit type diensten en producten een convenant.

Het convenant is ondertekend door de volgende partijen:

- PO-raad
- VO-raad
- GEU (branche-organisatie voor aanbieders van leermiddelen, toetsen en educatieve dienstverlening
- KBb-E (brancheverenigingvan distributeurs in de educatieve keten)
- VDOD (brancheverenigingvan leveranciers van digitale onderwijsdiensten)

Het convenant vertaalt de Wet bescherming persoonsgegevens naar de onderwijspraktijk. Het bevat afspraken over hoe wordt omgegaan met persoonsgegevens bij het gebruik van digitale leermiddelen en toetsen. Zo weten scholen en aanbieders wat ze over en weer van elkaar mogen verwachten, zijn de afspraken werkbaar in de praktijk en heeft iedereen dezelfde gemeenschappelijke uitleg bij deze afspraken.

Regie bij de school

Bij de afspraken staat voorop dat de school de regie heeft. De school is verantwoordelijk voor de zorgvuldige omgang met de persoonsgegevens van de leerlingen en de communicatie naar ouders. Hierbij hoort ook het maken van goede afspraken met leveranciers. Een school staat hier niet alleen in. De partijen bij het convenant hebben een gemeenschappelijke en gedeelde zorg om de school in staat te stellen deze verantwoordelijkheid vorm te geven.

De afspraken in de praktijk

De brancheorganisaties en de PO- en VO-raad zijn hard aan de slag met de implementatie van de afspraken uit het convenant en de Model Bewerkersovereenkomst, die als bijlage bij het convenant hoort. De PO- en de VO-raad zullen samen met de brancheorganisaties de scholen informeren over wat zij kunnen verwachten en hen daarbij hulp bieden.

De succesvolle route om te komen tot deze afspraken wordt voortgezet. De partijen die zich verbinden aan het convenant blijven met elkaar in gesprek over de toepassing en naleving van de afspraken in praktijk.

Richtlijnen en procedures voor Kindante en haar scholen

De school vindt in bijlage 3 het "werkdocument voor scholen" dat binnen het juridisch kader een werkdocument is om gemakkelijk te beschrijven hoe de school omgaat met privacygevoelige gegevens van leerlingen en de wijze waarop de school transparant met ouders communiceert over hoe met deze gegevens op school wordt omgegaan.

De inhoud van het document wordt met ouders die een kind aanmelden gecommuniceerd. Ouders moeten weten welke gegevens van hun kind op school worden opgeslagen, verwerkt of doorgegeven aan derden en hoe de school de privacy van gegevens volgens de Wet Bescherming Persoonsgegevens waarborgt.
Voor alle bestaande ouders van kinderen op school wordt dit document zorgvuldig gecommuniceerd en in ieder geval opgenomen in de schoolgids.

Voldoen aan de wet (de Wet Bescherming Persoonsgegevens)) betekent meer dan het hebben van een vastgesteld document. Alle personeelsleden van Kindante moeten weten welk gedrag voorwaardelijk is in het kader van bescherming van privacygevoelige gegevens. De gezamenlijke afspraken moeten voor iedereen die met privacygevoelige gegevens van leerlingen omgaan duidelijk zijn.
Voor veel uitgeverijen en bedrijven waarmee gegevens worden uitgewisseld, was de totstandkoming van de wet sneller, dan het ontwerpen van een bewerkersovereenkomst.
Voor de grote uitgeverijen verenigd in de "GEU" (Gemeenschappelijke Educatie Uitgevers) en Basispoort zijn standaard bewerkersovereenkomsten i.s.m. Kennisnet en de PO-Raad ontwikkeld.
Voor alle andere partners op Kindanteniveau, zijn bewerkersovereenkomsten getekend, of zullen getekend worden zodra de desbetreffende partners hun overeenkomsten gereed hebben. Op dit moment zijn er op Kindanteniveau bewerkersovereenkomsten getekend met: Unilogic, ISY, Gynzy, Afas, Ecsplore, Cupella, Basispoort, Snappet, Rovict, Cito, ONZEleerling, Cogix en Nieuwsbegrip.
Voor alle partijen waarmee individuele scholen leerlinggegevens digitaal uitwisselen dienen scholen zelf in contact te treden en bewerkersovereenkomsten af te sluiten, om gegevensuitwisseling met het oog op privacywetgeving te waarborgen.

Binnen de wet bescherming persoonsgegevens werden in de decembermaand van 2015 aanvullend "de meldplicht datalekken" gepubliceerd. Met hoge boetes voor iedereen, die geen melding maakt van een eventueel "datalek". Ook scholen moeten weten, welke criteria hier gelden: het verlies of diefstal van een laptop, tablet of memorystick waarop privacygevoelige gegevens staan moet worden gemeld aan de Autoriteit Persoonsgegevens en in bepaalde gevallen ook aan de betrokkene. Als eerste aanspreekpunt voor datalekken binnen Kindante geldt, dat er contact wordt gezocht met domein ICT Kindante.

Het Privacyreglement Kindante

Dit reglement is overgenomen van de PO-raad (modeldocument) en in die zin aangepast, dat niet alle scholen dit afzonderlijk opstellen, maar het op bestuursniveau is gedefinieerd.

1. Aanhef Dit reglement is bestemd voor Stichting Kindante.

2. Definities

Persoonsgegevens	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
Verwerking van persoonsgegevens	Eke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
Bijzonder persoonsgegeven	Een persoonsgegeven dat iets zegt over iemand zijn godsdienst, levensovertuiging, ras, politieke gezindheid of zijn gezondheid;
Betrokkene	Degene op wie een persoonsgegeven betrekking heeft al dan niet vertegenwoordigd door diens wettelijk vertegenwoordiger. In dit reglement gaat het om de leerlingen en medewerkers.
Wettelijk vertegenwoordiger	Indien de betrokkene de leeftijd van zestien jaren nog niet heeft bereikt, wordt de betrokkene vertegenwoordigd door zijn wettelijk vertegenwoordiger. Meestal zal dit een ouder zijn maar het kan hier ook gaan om een voogd;
Verantwoordelijke	De verantwoordelijke stelt vast welke persoonsgegevens er verwerkt worden én wat het doel is van die verwerking. Dat wil zeggen de rechtspersoon waar de school onder valt: het bevoegd gezag. Wanneer in dit reglement gesproken wordt over de verantwoordelijke dan wordt daarmee het bevoegd gezag van Kindante bedoeld.
Bewerker	Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen;
Derde	Ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken;
Stichting Kindante	Het bevoegd gezag.

3. Reikwijdte en doelstelling

1. Dit reglement stelt regels over de verwerking van persoonsgegevens van leerlingen en medewerkers van Kindante.
2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door Kindante worden verwerkt. Dit reglement heeft tot doel:
    a. de persoonlijke levenssfeer van de betrokkene te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens;
    b. vast te stellen welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt;
    c. de zorgvuldige verwerking van persoonsgegevens te waarborgen;
    d. de rechten van betrokkene te waarborgen.

4. Doelen van de verwerking van persoonsgegevens

Bij de verwerking van persoonsgegevens houdt Kindante zich aan de relevante wetgeving waaronder de Wet Bescherming Persoonsgegevens (WBP).

Doelen

De verwerking van persoonsgegevens vindt slechts plaats voor de doelen als genoemd bij de volgende categorieën in het Vrijstellingsbesluit Wet bescherming persoonsgegevens:

a. onderwijs;

b. arbeid en pensioen;

5. Vrijstelling meldingsplicht

De in artikel 4 genoemde gegevensverwerkingen vallen onder het vrijstellingsbesluit WBP en hoeven niet worden aangemeld bij de toezichthouder Autoriteit persoonsgegevens (AP).

6. Doelbinding

Persoonsgegevens worden uitsluitend gebruikt voor zover dat gebruik verenigbaar is met de omschreven doelen van de verwerking. Kindante verwerkt niet meer gegevens dan noodzakelijk is om die vastgestelde doelen te bereiken.

7. Soorten gegevens

De gebruikte categorieën van persoonsgegevens worden met betrokkenen gecommuniceerd.

8. Grondslag verwerking

Verwerking van persoonsgegevens gebeurt alleen op grond van:

a. Toestemming: in het geval de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend
b. Overeenkomst: in het geval de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst
c. Wettelijke verplichting: in het geval de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan Kindante onderworpen is
d. Publiekrechtelijke taak: in het geval de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt

9.Bewaartermijnen

Kindante bewaart de gegevens niet langer dan dat zij noodzakelijk zijn voor het vervullen van het doel waarvoor zij zijn verkregen, tenzij er een andere wettelijke verplichting is die het langer bewaren van de gegevens verplicht stelt.

10. Toegang

Kindante verleent slechts toegang tot de in de administratie en systemen van de school opgenomen persoonsgegevens aan:

a. de bewerker en de derde die onder rechtstreeks gezag van Kindante staat;
b. de bewerker die gemachtigd is om persoonsgegevens te verwerken;'
c. derden die op grond van de wet toegang moet worden verleend, waarbij alleen toegang wordt verleend aan de gegevens waartoe volgens de wet toegang toe moet worden gegeven.

11. Beveiliging en geheimhouding

a) Kindante neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden

beschadigd, verloren gaan of onrechtmatig worden verwerkt. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.

b) Kindante zorgt dat medewerkers niet meer inzage of toegang hebben tot de persoonsgegevens dan zij strikt noodzakelijk nodig hebben voor de goede uitoefening van hun werk.

c) Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek en de kosten van de tenuitvoerlegging. Daarbij houdt Kindante rekening met de concrete risico's die van toepassing kunnen zijn op de verwerkte persoonsgegevens.

d) Iedereen die betrokken is bij de uitvoering van dit reglement, en daarbij de beschikking krijgt over persoonsgegevens die vertrouwelijk zijn of geheim moeten worden gehouden (zoals bijvoorbeeld zorggegevens), en voor wie niet reeds uit hoofde van beroep, functie of wettelijk voorschrift een geheimhoudingsplicht geldt, is verplicht tot geheimhouding van die persoonsgegevens daarvan.

12. Verstrekken gegevens aan derden

Wanneer daartoe een wettelijke plicht bestaat kan Kindante de persoonsgegevens verstrekken aan derden. Het verstrekken van persoonsgegevens aan derden kan ook plaats vinden na toestemming van de betrokkene.

13. Sociale media

Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt in de gedragscode van Kindante of herleidingen hiervan in het protocol op school.

14. Rechten betrokkenen

De WBP geeft de betrokkene een aantal rechten. Kindante erkent deze rechten en handelt in overeenstemming met deze rechten.

Inzage

a. Elke betrokkene heeft recht op inzage van de door Kindante verwerkte persoonsgegevens die op hem/haar betrekking hebben. Kindante kan vragen om een geldig identiteitsbewijs ter verificatie van de identiteit van de verzoeker

Verbetering, aanvulling, verwijdering en afscherming

b. Betrokkene kan een verzoek doen tot verbetering, aanvulling, verwijdering of afscherming van zijn persoonsgegevens, tenzij dit onmogelijk blijkt of een onredelijke inspanning zou vergen.

Verzet

c. Voor zover Kindante persoonsgegevens gebruikt op de grond van artikel 8 onder d, kan de betrokkene zich verzetten tegen verwerking van persoonsgegevens op basis van diens persoonlijke omstandigheden.

Termijn

d. Kindante dient binnen een termijn van 4 weken na ontvangst van een verzoek hieraan schriftelijk gehoor te geven dan wel dit schriftelijk, gemotiveerd af te wijzen. Kindante kan de betrokkene laten weten dat er meer tijd nodig is en deze termijn verlengen met maximaal 4 weken.

Uitvoeren verzoek

e. Indien het verzoek van de betrokkene wordt gehonoreerd, draagt Kindante zorg voor het zo spoedig mogelijk doorvoeren van de verzochte wijzigingen.

Intrekken toestemming

f. Voor zover voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming te allen tijde door de wettelijk vertegenwoordiger worden ingetrokken.

15. Transparantie

1. Kindante informeert de betrokkene over de verwerking van zijn persoonsgegevens. Indien het type verwerking dat vraagt, informeert de school iedere betrokkene apart over de details van die verwerking.
2. Kindante informeert de betrokkene – op hoofdlijnen – ook over de afspraken die gemaakt zijn met derden en bewerkers die persoonsgegevens van de betrokkene ontvangen.

16. Klachten

1. Wanneer u van mening bent dat het doen of nalaten van Kindante niet in overeenstemming is met de WBP of zoals dat is uitgewerkt in dit reglement is, dan dient u zich te wenden tot het bevoegd gezag van Kindante
2. Overeenkomstig de WBP kan de betrokkene zich eveneens wenden tot de rechter of de Autoriteit Persoonsgegevens.

17. Onvoorziene situatie

Indien zich een situatie voordoet die niet beschreven is in dit reglement dan neemt de verantwoordelijke de benodigde maatregelen.

18. Wijzigingen reglement

De verantwoordelijke heeft het recht dit reglement, na instemming van de (G)MR te wijzigen.

19. Slotbepaling

Dit reglement wordt aangehaald als “het privacyreglement” van Kindante en treedt in werking op 1 augustus 2016.

Ten behoeve van ouders:

Welke gegevens bewaart de school van mijn kind ?

De basisschool bewaart verschillende gegevens over uw kind in een leerlingdossier. U en de school mogen deze leerlinggegevens inzien. In speciale gevallen mogen derden dat ook.

Leerlinggegevens
De basisschool houdt van elke leerling een leerlingdossier bij. Daarin bewaart de school:

- gegevens over inschrijving en uitschrijving;
- gegevens over afwezigheid;
- adresgegevens;
- gegevens die nodig zijn om het leerlinggewicht vast te stellen.

Ook de volgende gegevens mag de school bewaren:

- gegevens over de ondersteuningsbehoefte, als uw kind die heeft;
- gegevens over de gezondheid die nodig zijn voor eventuele speciale begeleiding of voorzieningen;
- gegevens over de vorderingen en de resultaten van uw kind.

De school mag de meeste gegevens nog 2 jaar bewaren nadat uw kind van school is gegaan.

De basisschool moet langer bewaren:

- gegevens over verzuim en in- en uitschrijving (5 jaar nadat de school uw kind heeft uitgeschreven);
- gegevens over een leerling die naar een school voor speciaal onderwijs is doorverwezen (3 jaar na vertrek van de leerling).

Adresgegevens van (oud-)leerlingen mag de school bewaren voor het organiseren van reünies.

Inzage en correctie leerlinggegevens

Als ouder heeft u het recht om de gegevens over uw kind in te zien (inzagerecht). U maakt hiervoor een afspraak met de school. Terwijl u de gegevens inziet, blijft iemand van de school aanwezig. Als ouder heeft u ook correctierecht. U kunt de school verzoeken verkeerde gegevens in het leerlingdossier van uw kind te verbeteren of te verwijderen.

Heeft u geen ouderlijk gezag meer, bijvoorbeeld na een echtscheiding? Ook dan moet de school u inzage geven in de leerlinggegevens over uw kind. Dit staat in het Burgerlijk Wetboek. U moet dan zelf de directie van de school om deze informatie vragen.

Inzage leerlinggegevens door derden

Soms is de school verplicht om gegevens aan bepaalde professionals te geven. Bijvoorbeeld bij:

- de overgang naar een andere school, zoals het voortgezet onderwijs (vo) of het speciaal basisonderwijs (sbo);
- inzage door de Inspectie van het Onderwijs (IvhO);
- vermoedens van kindermishandeling;
- noodsituaties.

In andere gevallen moet u als ouder eerst toestemming geven, voordat derden de gegevens van uw kind mogen inzien.

Bijvoorbeeld:

a. naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie bedoelde gegevens van de betrokkene;

b. het persoonsgebonden nummer (BSN);

c. nationaliteit;

d. gegevens als bedoeld onder a, van de wettelijk vertegenwoordiger of verzorger van de leerling;

e. gegevens betreffende de gezondheid of het welzijn van de leerling voor zover die noodzakelijk zijn voor de ondersteuning;

f. gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor de school, het onderwijs of de te geven ondersteuning;

g. gegevens betreffende de aard en het verloop van het onderwijs en ondersteuning, alsmede de behaalde studieresultaten;

h. schoolgegevens (waaronder naam school, naam zorgcoördinator/mentor/ intern begeleider, klas/groep waarin de leerling zit, tijdstip van inschrijving bij deze school, naam van de indiener van de aanmelding bij het samenwerkingsverband, schoolloopbaan en rapportage vanuit primair en voortgezet onderwijs);

i. aanleiding voor de aanmelding bij het samenwerkingsverband, relevante screenings- en onderzoeksgegevens en omschrijving van de problematiek die aan de orde is;

j. activiteiten die door de school zijn ondernomen rond de betreffende leerling, alsmede de resultaten hiervan;

k. bestaande of (relevante) afgesloten hulpverleningscontacten en de namen van contactpersonen;

l. relevante persoonsgegevens die door externe partijen worden verstrekt met betrekking tot de aangemelde problematiek van de betreffende leerling;

m. relevante financiële gegevens over bijvoorbeeld schoolgeld;

Welke gegevens mogen worden uitgewisseld met OSO (Overstapservice Onderwijs)

Jaarlijks stappen ruim 175 duizend leerlingen over van het PO naar het VO. Het is wettelijk bepaald dat hierbij leer- en begeleidingsgegevens moeten worden uitgewisseld. Dit Overstapdossier bevat veel gevoelige gegevens over de leerlingen. Ouders hebben het recht om het rapport voor uitwisseling in te zien. In de wet is ook vastgelegd welke leer- en begeleidingsgegevens uitgewisseld mogen worden.

- gegevens over in- en uitschrijving;
- gegevens over afwezigheid;
- adresgegevens;
- gegevens die nodig zijn om te berekenen hoeveel geld de school krijgt;
- het onderwijskundig rapport;
- gegevens over de gezondheid die nodig zijn voor speciale begeleiding of voorzieningen;
- gegevens over de vorderingen en de resultaten van de leerling;
- verslagen van gesprekken met de ouders;
- de resultaten van eventueel psychologisch onderzoek.

(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.)

Om deze gegevens veilig uit te wisselen is een digitale service ontwikkeld door de PO- en VO-raad, waarmee de gegevens rechtstreeks tussen de administratiesystemen van scholen uitgewisseld kunnen worden. Deze service, de Overstapservice Onderwijs (OSO) genaamd, wordt door veel schoolbesturen gebruikt. In de praktijk gebeurt het echter ook nog vaak dat gegevens op papier worden uitgewisseld. Dit kost de scholen veel extra tijd, omdat de gegevens handmatig ingevoerd dienen te worden in de administratiesystemen. Met OSO kan ook de privacy beter beschermd worden, omdat gewerkt wordt met de laatste beveiligings- en gegevensstandaarden waaraan leveranciers moeten voldoen. De huidige DOD-koppeling die ook nog wel gebruikt wordt, wordt daarom uit gefaseerd. Het gebruik van OSO vraagt echter wel om goede (regionale) afspraken tussen scholen over de gegevens die aangeleverd moeten worden en de momenten waarop dit moet gebeuren. Alle scholen van Kindante zijn gecertificeerd voor OSO en alle managementassistenten zijn bekend met de werkwijze. Voor Kindante is OSO een standaard. Er wordt nauw samengewerkt met het VO in de regio en uiteraard met de samenwerkingsverbanden.

Meer informatie over OSO: klik hier.

Format Kindante t.b.v. toestemming van ouders voor publicatie van foto’s en video’s

Op scholen worden ten behoeve van informatievoorziening en communicatie op de website, in nieuwsbrieven of ouderportalen ook foto’s of video’s getoond waarop kinderen en personeel van scholen is te zien. Hiervoor dient vooraf en ieder schooljaar opnieuw, toestemming te worden verleend door ouders.
Een format, waar ouders een akkoordverklaring kunnen tekenen is te vinden in bijlage 4.

Protocol datalekken Kindante

Inleiding

Sinds 1 januari 2016 is de meldplicht datalekken van kracht. De meldplicht vormt een toevoeging aan de Wet Bescherming Persoonsgegevens (Wbp): zowel bedrijven als overheden moeten voortaan direct melding doen als er een datalek heeft plaatsgevonden, bijvoorbeeld in geval van een hack of diefstal van een USB met belangrijke informatie.

Kindante heeft haar beleid in het kader van de Wet op Bescherming Persoonsgegevens beschreven in het document "Toepassing van de Wet op Privacy Persoonsgegevens op Kindantescholen". Hierin worden de kaders voor onze scholen beschreven, die de privacy van kind – en oudergegevens moeten waarborgen. Belangrijk hierbij is de informatieplicht naar betrokkenen en volledige transparantie over wat scholen vanuit hun professie met welke gegevens doen en met wie zij deze gegevens delen. Daarnaast kiest Kindante voor het vaststellen van een privacyreglement (blz. 6 e.v.) voor privacygevoelige gegevens van kinderen én alle Kindantepersoneel.

Belangrijke richtsnoeren hierbij zijn :

- Rekening houden met wettelijke bewaartermijnen
- Gegevens moeten toereikend zijn, niet overmatig worden verzameld
- De gegevens moeten juist en nauwkeurig zijn
- Met de gegevens moet vertrouwelijk worden omgegaan
- De gegevens moeten goed beveiligd zijn

In dit document beschrijft Kindante volgens de richtlijnen van de "Autoriteit Persoonsgegevens" hoe we als organisatie preventief en curatief om wensen te gaan met het voorkomen en beheersen van "datalekken".

Van groot belang, is het kweken van bewustzijn onder alle betrokkenen voor "datalekken en bescherming van iemands privacygevoelige gegevens". Dit is niet een taak van bijvoorbeeld de ICT-afdeling, of loonadministratie of schooldirecteur, maar is een zaak die goed op het netvlies van alle personeelsleden van Kindante moet komen! Regels en procedures zijn relatief gemakkelijk vast te stellen, maar de mens is in alle beveiligingsissues hier betrekking op hebbende de zwakste schakel!

Wat is een datalek?

Een datalek is het verkrijgen van toegang tot, vernietiging, wijziging of vrijkomen van persoonsgegevens (van kinderen, ouders of medewerkers) bij Kindante als organisatie, zonder toestemming van de Kindanteorganisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook over onrechtmatige verwerking van gegevens.

Meldplicht

Als er sprake is van inbreuken op de beveiliging van persoonsgegevens (een datalek dus), dan moeten deze inbreuken niet alleen worden doorgegeven in het geval van kwaadwillende hackers, maar in alle gevallen waarbij een aanzienlijke kans bestaat op nadelige gevolgen voor de privacy van personen.

De inbreuk moet daarvoor wel 'ernstig' van aard zijn. Ernstig betekent in dit verband dat er kans is op verlies of onrechtmatige verwerking van persoonsgegevens. Dit blijft een case-by-case inschatting die de school en het bureau Kindante zelf zal moeten maken, maar bijvoorbeeld het "kwijtraken" van een zorgdossier van een kind of een personeelsdossier moet worden gezien als ernstig!

De meldplicht is bovendien tweeledig. Er moet gemeld worden aan de Autoriteit Persoonsgegevens en in sommige gevallen aan alle betrokkenen. De melding van een datalek moet zo spoedig mogelijk na het voorval worden gedaan (binnen 72 uur!). Mocht het datalek ongunstige gevolgen hebben voor de levenssfeer van betrokkenen, dan dient men naast de Autoriteit Persoonsgegevens ook de betrokkenen in te lichten. De maximale boete voor het niet op tijd melden is in de nieuwe wet maar liefst 810.000 euro of maximaal 10% omzet.

In de praktijk

Bovenstaande betekent in de praktijk dat moet worden opgelet in ten minste deze gevallen:

Verlies of diefstal van o.a. een USB-stick, een computer, laptop, tablet, telefoon, documenten (aktentas, schooltas) of van wachtwoorden waarmee privacygevoelige informatie is te achterhalen.

Privacygevoelige informatie is o.a.: Burger Service Nummers (BSN), kopieën van identiteitsbewijzen, informatie over iemands godsdienst, levensovertuiging, seksuele geaardheid, strafrechtelijke gegevens, salarisgegevens, schulden, politieke overtuiging, prestaties op school of werk- of relatieproblemen.

Situaties waarbij er niet veilig wordt omgegaan met persoonsgegevens, die kunnen leiden tot een datalek:

- Niet afgesloten dossierkasten die voor onbevoegden toegankelijk zijn
- Formulieren of documenten die op bureaus rondslingeren (clean desk policy dient overal te gelden!)
- Niet opgehaalde afdrukken op de printer/kopieerapparaat
- 'Openstaande' beeldschermen van de computer bij afwezigheid (op school/kantoor, maar ook extern via telewerk-omgeving)
- Werken in een open(bare) Wifi-verbinding
- Wachtwoorden die op het bureau of thuis makkelijk te vinden zijn (op papier/in agenda)
- Wachtwoorden die door derden worden afgekeken
- Inloggegevens die worden uitgeleend
- Foutief geadresseerde e-mails
- Mailen van kindgegevens

Bepaling datalek

Bij de beslissing of je een gebeurtenis die zich heeft voorgedaan moet melden aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene, moet je een aantal afwegingen maken.

Dit schema geeft deze afwegingen weer:

Beveiligingslek:
Heeft zich een beveiligingslek voorgedaan?

Zijn bij het beveiligingsincident persoonsgegevens verloren gegaan, of is onrechtmatige verwerking redelijkerwijs niet uit te sluiten?

Beveiligingsincident!  **Datalek!**

Gaat het om persoonsgegevens van gevoelige aard, of is er om een andere reden sprake van (een aanzienlijke kans op) ernstige nadelige gevolgen voor de bescherming van de verwerkte persoonsgegevens?

Melden aan Autoriteit Persoonsgegevens

Waren niet alle gelekte gegevens (goed) versleuteld, of heeft het datalek om andere redenen waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene?

Melden aan de betrokkene

Waar moet ik een datalek melden?

Als er sprake is van een datalek (of men vermoedt een datalek) zoals in voorgenoemde tekst besproken, neem dan direct telefonisch contact op met

Bureau Kindante, Domein ICT via Ed Toussaint (046-4588776) of Claudia de Rooij (046-4007605).

Zij zullen in overleg met de melder bepalen of er sprake is van een datalek zoals de Autoriteit Persoonsgegevens dat bedoelt en zij zullen een melding maken volgens de procedure op de site: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

BIJLAGEN

Bijlage 1: Model bewerkersovereenkomst Versie 2.0 te vinden op:
https://www.privacyconvenant.nl/convenant/

Bijlage 2: Het convenant digitale onderwijsmiddelen is terug te vinden op : https://www.poraad.nl/nieuws-en-achtergronden/privacy-in-onderwijs-steeds-verder-verstevigd

Bijlage 3: Werkdocument voor scholen

Bijlage 4: Format Kindante t.b.v. toestemming van ouders voor publicatie van foto's en video's

Bijlage 5: Informatieplicht aan ouders

Bijlage 6: Wat doet Kindante in het kader van veiligheid van het netwerk en hardware?

Bijlage 3: Werkdocument voor scholen : "Transparantie over privacy"

Vooraf:
m.b.t. de implementatie van deze herziene wetgeving moeten Kindantescholen z.s.m. voldoen aan de letter van de wet, om transparantie in communicatie naar ouders over privacy en de omgang met privacy gevoelige gegevens van leerlingen volgens de wet te borgen.
Belangrijk hierbij is, dat alle personeelsleden op school goed geïnformeerd raken over de inhoud van deze materie. Ook de medezeggenschapraden van scholen moeten hierin worden meegenomen. De nadruk moet niet liggen op het "in orde hebben van documenten" , maar in de toepassing van de privacybescherming van leerlinggegevens in de dagelijkse schoolpraktijk !

Werkdocument Transparantie over privacy

(Alle Geel gemarkeerde teksten kunnen door de school naar eigen situatie worden aangepast)

Transparantie over privacy
Als school hebben we informatieplicht en moeten we uitleggen hoe er met de gegevens over leerlingen wordt omgegaan. Ouders hebben recht op volledige transparantie van ons daarover. Dit document informeert ouders over privacy op school. Dit document wordt opgenomen in onze schoolgids.

Privacy
Op [naam school] gaan wij zorgvuldig om met de privacy van onze leerlingen. Dit is vastgelegd in het privacyreglement van ons bestuur Kindante, dat is opgenomen in bijlage …. De gegevens die over leerlingen gaan, noemen we persoonsgegevens. Wij maken alleen gebruik van persoonsgegevens als dat nodig is voor het leren en begeleiden van onze leerlingen, en voor de organisatie die daarvoor nodig is. Een overzicht van deze categorieën en officiële bewaartermijnen vindt u in bijlage….
In het privacyreglement van Kindante kunt u precies lezen wat voor onze school de doelen zijn voor de registratie van persoonsgegevens. De meeste gegevens ontvangen wij van ouders (zoals bij de inschrijving op onze school). Daarnaast registreren leraren en ondersteunend personeel van onze school gegevens over onze leerlingen, bijvoorbeeld cijfers en vorderingen. Soms worden er bijzondere persoonsgegevens geregistreerd als dat nodig voor de juiste begeleiding van een leerling, zoals medische gegevens (denk aan dyslexie of ADHD). In verband met de identiteit van onze school, willen wij graag de geloofsovertuiging registreren zodat wij daar – zo mogelijk – tijdens het onderwijs rekening mee kunnen houden, maar het geven van deze informatie aan de school is niet verplicht.

De leerlinggegevens worden opgeslagen in ons (digitale) administratiesysteem Esis en indien noodzakelijk m.b.t. digitale toetsen in het computerprogramma van CITO .De vorderingen van de leerlingen worden vastgelegd in ons leerlingvolgsysteem Esis en indien noodzakelijk m.b.t. digitale toetsen in het computerprogramma van CITO. Deze programma's zijn beveiligd en toegang tot die gegevens is beperkt tot medewerkers van onze school. Omdat [naam school] onderdeel uitmaakt van het schoolbestuur Kindante, worden ook met Kindante bepaalde gegevens gedeeld in het kader van de gemeenschappelijke administratie, verantwoording naar inspectie en het plaatsingsbeleid.

Tijdens de lessen maken wij gebruik van een aantal digitale leermaterialen. Hiervoor is een beperkte set met persoonsgegevens nodig om bijvoorbeeld een leerling te kunnen identificeren als die inlogt. Wij hebben met deze leveranciers duidelijke afspraken gemaakt over de gegevens die ze van ons krijgen. De leverancier mag de leerling gegevens alleen gebruiken als wij daar toestemming voor geven, zodat misbruik van die informatie door de leverancier wordt voorkomen. De educatieve software die wij betrekken van Heutink Primair Onderwijs BV, de Rolf Groep, L.C.G. Malmberg b.v. , Noordhoff uitgevers, Reinders Oisterwijk, ThiemeMeulenhoff en uitgeverij Zwijsen wordt ontsloten middels de portal van Basispoort.

Ouders hebben het recht om de gegevens van en over hun kind(eren) in te zien. Als de gegevens niet kloppen, moet de informatie gecorrigeerd worden. Als de gegevens die zijn opgeslagen niet meer relevant zijn voor de school, mag u vragen die specifieke gegevens te laten verwijderen. Voor vragen of het uitoefenen van uw rechten, kunt u contact opnemen met de leraar/lerares van uw kind, of met de schooldirecteur.

Als er leerlinggegevens worden uitgewisseld met andere organisaties, vragen we daar vooraf de toestemming van de ouders, tenzij we volgens de wet *verplicht zijn* om die informatie te verstrekken. Dat kan het geval zijn als de leerplichtambtenaar om informatie vraagt of als het ministerie van Onderwijs, Cultuur en Wetenschap informatie nodig heeft..

Voor het gebruik van foto's en video-opnames van leerlingen op bijvoorbeeld de website, social media van de school of in de nieuwsbrief, vragen wij altijd vooraf uw toestemming. Ouders mogen altijd besluiten om die toestemming niet te geven, of om eerder gegeven instemming in te trekken. Als u toestemming heeft gegeven, blijven wij natuurlijk zorgvuldig met de foto's en filmpjes omgaan en wegen wij per keer af of het verstandig is een foto of filmpje te plaatsen. Voor vragen over het gebruik van foto's en video's kunt u terecht bij de leraar/lerares van uw kind, of bij de schooldirecteur. Zie hiervoor het voorbeeld/format op blz. 10 in dit document.

Basispoort
Om leerlingen eenvoudig toegang te geven tot digitaal leermateriaal van de school, maakt [naam school] gebruik van Basispoort. Deze software maakt het geven van onderwijs op maat via gedigitaliseerde leermiddelen mogelijk. Het maken van bijvoorbeeld een online toets of oefenen in een online-omgeving van een uitgever, is alleen mogelijk als de docent weet welke leerling de antwoorden heeft ingevoerd. Hiervoor zijn leerlinggegevens nodig. De school heeft met Basispoort een overeenkomst gesloten waarin afspraken zijn gemaakt over het gebruik van de leerlinggegevens. Basispoort maakt gebruik van de volgende set met gegevens: een identificatienummer van Basispoort, voornaam, achternaam, tussenvoegsel, geboortedatum, leerlingkey, groepskey, groepsnaam, jaargroep, geslacht en het identificatienummer van de school. Via Basispoort worden er dus geen leer- of toetsresultaten opgeslagen en/of uitgewisseld.
Basispoort geeft op haar eigen website ook informatie (http://info.basispoort.nl/privacy).

Als u wilt weten hoe de uitgevers van digitale leermiddelen omgaan met leerlinggegevens, dan kunt u dat nalezen in de privacy bijsluiters die horen bij de leermiddelen die de school gebruikt. Meer informatie is te vinden op de site van de PO-Raad (https://www.poraad.nl/nieuws-en-achtergronden/privacy-in-onderwijs-steeds-verder-verstevigd). Hier zijn 2 belangrijke documenten te vinden: het convenant privacy voor digitale leermiddelen en toetsen en de modelbewerkersovereenkomst.
Veel Nederlandse (educatieve) uitgeverijen zijn verenigd in de organisatie die de naam GEU draagt: (Gemeenschappelijke Educatieve Uitgevers). Leden van de GEU onderschrijven de uitgangspunten en afspraken in zoals die op de site van de PO-raad te vinden zijn. Informatie over de GEU kunt u vinden op hun site: https://www.geu.nuv.nl/leermiddelen-in-nederland/

Inschrijfformulier

De schoolgids en de website van de school, zijn belangrijke informatiebronnen voor ouders die op zoek zijn naar een school voor hun kind(eren). Als het uiteindelijk tot een aanmelding en/of inschrijving komt, wil de school graag beschikken over de juiste informatie. De ouders worden gevraagd om informatie te verstrekken. Daarvoor wordt er meestal gebruik gemaakt van een of meerdere (digitale) formulieren. Gemakshalve noemen we formulieren 'inschrijfformulier'. Bij het vragen naar informatie over het kind en diens ouders, is het belangrijk om transparant te zijn wat de school doet met de verstrekte informatie.
Het is lastig om voor alle scholen een zelfde en eenvormig modelformulier te gebruiken. Iedere school heeft behoefte aan zijn eigen specifieke vragen. Hierna is daarom een algemene tekst opgenomen die u zelf kunt aanvullen.

Bijgaand (of op blz. xxx van onze schoolgids, of op onze website) treft u het inschrijfformulier aan van [onze school]. U ontvangt een bevestiging van uw inschrijving. [nadere uitleg inschrijvingsproces etc. etc.].

De meeste vragen op het formulier spreken voor zich. Een aantal vragen zijn wij wettelijk verplicht aan u te stellen. Zo vragen wij naar uw opleidingsniveau. Dit heeft te maken met de wettelijke 'gewichtenregeling': het aantal leerkrachten aan onze school is mede afhankelijk van het totaal van het 'leerlinggewicht' van onze leerlingen.

De gegevens die u heeft ingevuld op het inschrijfformulier, worden opgeslagen in de leerlingadministratie Esis van onze school. Uiteraard worden deze gegevens vertrouwelijk behandeld. Op onze administratie is de Wet bescherming persoonsgegevens van toepassing. Dit betekent onder andere dat de gegevens door ons worden beveiligd, en dat de toegang tot de administratie is beperkt tot alleen personeel die de gegevens strikt noodzakelijk nodig heeft. U heeft als ouder het recht om de door ons geregistreerde gegevens in te zien (voor zover die informatie betrekking heeft op uw kind). Als de gegevens niet kloppen, dan mag u van ons verwachten dat wij – op uw verzoek - de informatie verbeteren of aanvullen.

Voor meer informatie over de omgang met de privacy van uw kind(eren), verwijzen wij u naar het privacyreglement van Kindante.(blz. 6 e.v.)

Telefoonlijst
Op basisscholen worden er vaak klassenlijsten of telefoonlijsten uitgedeeld met namen, adressen en telefoonnummers (van ouders) van leerlingen. Maar het verstrekken van een dergelijke lijst valt onder de wettelijk beschermde privacy van de leerling en diens ouders. Het goed kunnen geven van onderwijs is niet afhankelijk van deze klassenlijst. Het is dus verstandig om de ouders (vooraf) toestemming te vragen om een klassenlijst te mogen maken en te laten delen met andere ouders in de klas. Hoe praktisch deze lijst ook is: steeds vaker zijn er ouders die er bezwaar tegen hebben dat hun privégegevens met de hele klas worden gedeeld.

Bij het gebruik van een adressenlijst kan de volgende lijst gebruikt worden:

Op onze school wordt er, per klas, een klassenlijst gemaakt met de adressen van leerlingen. Deze lijst met contactgegevens is erg praktisch om te overleggen met andere ouders, als de kinderen (buiten schooltijd) willen afspreken of als er vragen zijn rondom school, overblijf of bijvoorbeeld huiswerk. Wij vragen hierbij uw toestemming om de naam van uw kind, diens adres en uw telefoonnummer te mogen delen met de andere (ouders van de) klasgenootjes van uw kind. Als u er bezwaar tegen heeft, wordt de naam van uw kind niet gedeeld (en moet u daar zelf voor zorgen). Deze informatie op de klassenlijst mag uitsluitend gebruikt worden voor persoonlijk gebruik onderling, en dus niet voor bijvoorbeeld reclame.

Hierbij maak ik, wel / geen * bezwaar tegen het in de klas van mijn kind verspreiden van een klassenlijst met de naam van mijn kind, adres en telefoonnummer.
* doorhalen wat niet van toepassing is.

Toelichting Informatieplicht

De helderheid die scholen over privacy moeten geven, gaat over twee belangrijke thema's:
informatie over het privacy-beleid. Hierin wordt beschreven hoe de school in het algemeen omgaat met privacy. Dit is meestal vastgelegd in een privacyreglement en/of mediaprotocol;
over de (concrete) uitwisselingen van gegevens met andere organisaties en bedrijven, zoals met leveranciers van digitaal leermateriaal of leveranciers van leerling-informatiesystemen.
Deze informatie is meestal opgenomen op de website en/of in de schoolgids. Het is ook mogelijk deze informatie (jaarlijks) aan ouders te verstrekken.

Volgens de Wet bescherming persoonsgegevens (WBP) moet de school degene over wie de persoonsgegevens gaan (de betrokkene) op de hoogte stellen van uw identiteit (schooldirecteur, bestuur en/of bevoegd gezag) en voor welk doel(en) u de persoonsgegevens verzamelt. Als de betrokkene jonger dan 16 jaar is, dan mogen volgens de WBP alleen de wettelijke vertegenwoordigers (ouders) beslissen over de privacy van de betrokkene. Gemakshalve gebruiken we hierna 'ouders'.

De Wbp eist dat een school de ouders extra informeert als:
de verwachting van de ouders anders is: als de school persoonsgegevens gebruikt op een manier die ouders redelijkerwijs niet verwachten, is dit een reden om ouders extra informatie te geven;
de omstandigheden waaronder de school persoonsgegevens krijgt: ouders zijn er niet altijd van op de hoogte dat de school via een andere organisatie nieuwe persoonsgegevens heeft gekregen, het is dan noodzakelijk ouders daarvan (en indien mogelijk: persoonlijk) op de hoogte te stellen;
Het gebruik dat u van de gegevens gaat maken: als de gevolgen van het gebruik van de persoonsgegevens voor de leerling (of diens ouders) groter zijn dan anders, is extra informatieverstrekking noodzakelijk;
de aard van de gegevens: hoe gevoeliger de aard van de gegevens is die u van de leerling gebruikt, hoe meer reden er is om de ouders hierover gedetailleerd te informeren, denk hierbij aan het gebruik van medische gegevens.

De informatie moet vooraf aan de ouders bekend zijn gemaakt. Dat hoeft niet persoonlijk en mag dus via de website, nieuwsbrief of schoolgids. Ouders moeten ten minste zijn geïnformeerd op het moment dat de school de gegevens gaat gebruiken. De school moet er wel rekening mee houden dat de informatie iedereen moet kunnen bereiken: niet iedereen ontvangt bijvoorbeeld de digitale nieuwsbrief of heeft toegang tot (het afgesloten deel van) de website.

De informatieplicht geldt niet als:
de school weet dat alle ouders volledig zijn geïnformeerd. Vermoeden is niet genoeg;
het onevenredig veel inspanning kost om iedereen (persoonlijk) te informeren, is een alternatief voldoende (dus geen persoonlijke brief of gesprek maar bijvoorbeeld via de nieuwsbrief of website).

Bedenkingen over transparantie
Uit gesprekken met docenten en bestuurders blijkt dat scholen soms huiverig zijn om transparant te zijn: informatie geven aan ouders geeft hen misschien wel aanleiding om extra (lastige) vragen te stellen. In de praktijk lijkt dit gelukkig mee te vallen. Een school hoeft zich natuurlijk geen zorgen te maken als ze aan de wet voldoet: daar kunnen ouders niet tegen zijn. En daar komt bij dat de ervaring is dat ouders tegenwoordig mondiger zijn en ook zonder die transparantie kritische vragen stellen. En waarom zou een school de ouders een extra vraag in handen spelen door níet volledige transparantie te geven, zoals de wet dat van scholen vraagt?

Bijlage 4: Format Kindante t.b.v. toestemming van ouders voor publicatie van foto's en video's

[Plaats], [maand] [jaar]

Beste ouder/verzorger,

Op onze school laten wij u met foto's en video's zien waar we mee bezig zijn. Opnames worden gemaakt tijdens verschillende gelegenheden. Bijvoorbeeld tijdens activiteiten, schoolreisjes en lessen. Ook uw zoon/dochter kan op deze foto's (en soms in video's) te zien zijn. Ook ons bestuur (Kindante) publiceert op haar internetpagina soms foto's van kinderen die op een van de 42 scholen zitten.

Natuurlijk gaan we zorgvuldig om met foto's en video's. Wij plaatsen geen foto's waardoor leerlingen schade kunnen ondervinden. We plaatsen bij foto's en video's geen namen van leerlingen. Toch vinden we het belangrijk om uw toestemming te vragen voor het gebruik van foto's en video's van uw zoon/dochter. Het is goed mogelijk dat u niet wilt dat foto's van uw kind op internet verschijnen.

Met deze brief vragen we daarom uw toestemming voor het gebruik van beeldmateriaal van uw zoon/dochter. Wilt uw deze brief of antwoordstrook met uw kind meegeven naar school?

Uw toestemming geldt alleen voor foto's en video's die door ons, of in onze opdracht worden gemaakt. Het kan voorkomen dat andere ouders foto's maken tijdens schoolactiviteiten. De school heeft daar geen invloed op, maar wij gaan ervan uit dat deze ouders ook terughoudend zijn bij het plaatsen van foto's en video's op internet.

Wilt u uw toestemming samen met uw zoon/dochter bespreken? We merken dat oudere leerlingen soms zelf een keuze willen maken om foto's te gebruiken. Als u uw keuze thuis bespreekt, dan weten ze zelf waarom het gebruik van foto's en video's wel of niet mag.

U mag natuurlijk altijd terugkomen op de door u gegeven toestemming. Ook mag u op een later moment alsnog toestemming geven.

Alvast bedankt voor uw medewerking!

Met vriendelijke groet,

[naam ondertekenaar]

Hierbij verklaart ondergetekende, ouders/verzorger van …….. groep ……..

dat foto's en video's door [SCHOOL] gebruikt mogen worden:
in de schoolgids of schoolbrochure of schoolkalender, op de website van de school , in de (digitale) nieuwsbrief , op sociale-media accounts van de school, op ouderportaal of ISY of Klasbordapp en eventueel door ons bestuur Kindante voor communicatiedoeleinden, of voor onderzoeksdoeleinden (achteraf bekijken van een gegeven les door een stagiaire).

Datum: .....

Naam ouder/verzorger: .....

Handtekening ouder/verzorger: .....

Toelichting gebruik formulier toestemming

Een toelichting op het gebruik van foto's en video's op school, is te vinden in hoofdstuk 7 van de brochure 'Privacy in 10 stappen'. Deze brochure kunt u lezen en downloaden via kn.nu/privacy.

Er is geen toestemming van ouders nodig voor het gebruik van foto's en video's in de klas en les voor onderwijskundige doeleinden. Ook is er geen toestemming nodig voor het plaatsen van een foto op een schoolpas of voor gebruik van een foto in het administratiesysteem.
Wel gelden voor het gebruik van dat beeldmateriaal de gewone privacyregels (zoals dataminimalisatie: terughoudend omgaan met foto's en video's van leerlingen).

In het toestemmingsformulier is aparte toestemming opgenomen voor verschillende categorieën. De wetgever eist dat een ouder een goedgeïnformeerde beslissing kan nemen, die ook specifiek is. Het vragen van toestemming 'voor gebruik van foto's door de school' is dat zeker niet. Als school mag je je het dus niet zo formuleren: 'als u niet wilt dat we foto's van uw kind gebruiken, moet u dat maar zeggen'. Dit is een 'opt-out', en dit is in strijd met de wet.

Foto's maken door ouders op school
Het kan voorkomen dat ouders het vervelend vinden dat andere ouders foto's maken van hun kinderen.

Meestal overleggen deze ouders samen over het maken en gebruik van die foto's. Soms komen ouders er samen niet uit en dan wordt de school gevraagd om iets te regelen.

De school wil voor álle kinderen een veilige omgeving zijn, en niet een plek waar kinderen (en hun ouders) bang hoeven te zijn steeds te worden gefotografeerd. Het maken van foto's en video's op school kan moeilijk worden verboden, maar kan wel aan banden worden gelegd. Door bijvoorbeeld verwachtingen uit te spreken naar ouders over fotograferen tijdens een schoolactiviteit, of door ouders in de nieuwsbrief te vragen terughoudend te zijn met het maken en publiceren van foto's. Mocht dat niet het gewenste effect hebben, dan kan de school regels voor het maken van foto's op school vastleggen in het privacyreglement of in een aparte gedragscode of een protocol . Een schoolgebouw is niet zomaar een openbare plaats waar iedereen toegang toe heeft. De school kan aan het verlenen van toegang dus voorwaarden verlenen zoals de (extreme) regel dat fotograferen van leerlingen tijdens de les of in klas alleen is toegestaan door docenten.

Toestemming geven door één of twee ouders
Het is de vraag is de toestemmingsverklaring door één of beide ouders moeten worden ondertekend.

Als leerlingen jonger zijn dan 16 beslissen de wettelijk vertegenwoordigers (de ouders) over de privacy. De wet gaat ervan uit dat je als school mag vertrouwen op de mededelingen van één ouder. Als dat vertrouwen terecht is, dan is de andere ouder ook gebonden aan die mededeling. Bij het ondertekenen van de toestemmingsverklaring, mag de school dus vertrouwen op de toestemming als één ouder die geeft. Alleen als de school weet dat de andere ouder (die niet getekend heeft) tegen de toestemming is, mag de school niet uitgaan van die ene ondertekening. Dan moet de school van beide ouders toestemming hebben. Vooral bij gescheiden ouders kan het verstandig zijn om de toestemming van beide ouders te vragen. Voor het intrekken van toestemming is de mededeling van één ouder ook voldoende.

Bij twijfel is het beter om te vertrouwen op twee handtekeningen, of om de foto dan maar niet te gebruiken.

Bijlage 5: Informatieplicht aan ouders

SITUATIE	ALLE INFORMATIE	BEPERKTE INFORMATIE (ALTIJD IN OVERLEG MET CVB)	GEEN INFORMATIE (ALTIJD IN OVERLEG MET CVB)
Ouders die met elkaar getrouwd zijn en beide het gezag hebben.	Beide ouders. Zij bepalen welke andere personen alle informatie mogen verkrijgen (bijv. niet gezaghebbende ouder, pleegouders, grootouders).		
Ouders die getrouwd zijn waarvan één ouder het gezag heeft en één ouder het kind erkend heeft.	De ouder die gezag heeft. Deze bepaalt welke andere personen alle informatie mogen verkrijgen (bijv. niet gezaghebbende ouder, pleegouders, grootouders).	De ouder die het kind erkend heeft, heeft recht op beperkte informatie waar hij/zij zelf om moet vragen. Het betreft alleen belangrijke feiten en omstandigheden dus informatie over schoolvorderingen en evt. sociaal-pedagogische ontwikkelingen op school tenzij de veiligheid van het kind niet gewaarborgd kan worden (bijv. signalen van kindermishandeling / huiselijk geweld)***	
Ouders die getrouwd zijn waarvan 1 ouder het gezag heeft en 1 ouder geen gezag heeft en zijn kind niet erkend heeft.	De ouder die gezag heeft. Deze bepaalt welke andere personen alle informatie mogen verkrijgen (bijv. niet gezaghebbende ouder, pleegouders, grootouders).		De ouder die geen gezag heeft en het kind niet erkend heeft.
Ouders die getrouwd zijn waarvan beide ouders het gezag niet hebben maar wel hun kind erkend hebben. Er is een voogd toegewezen*.	De voogd. Deze bepaalt welke andere personen alle informatie mogen verkrijgen (bijv. leefgroep, niet gezaghebbende ouder, pleegouders, grootouders).	De ouders hebben recht op beperkte informatie waar zij zelf om moet vragen. Het betreft alleen belangrijke feiten en omstandigheden dus informatie over schoolvorderingen en evt. sociaal-pedagogische ont-wikkelingen op school tenzij de veiligheid van het kind niet gewaarborgd kan worden (bijv. signalen van kindermishandeling/ huiselijk geweld)***	

Ouders die gescheiden zijn, waarvan beide ouders het gezag hebben.	Beide ouders. Zij bepalen welke andere personen alle informatie mogen verkrijgen (bijv. niet gezaghebbende ouder, pleegouders, grootouders).	Indien er signalen zijn van kindermishandeling/huiselijk geweld.	
Ouders die gescheiden zijn, waarvan 1 ouder het gezag heeft en 1 ouder het kind erkend heeft.	De ouder die gezag heeft. Deze bepaalt welke andere personen alle informatie mogen verkrijgen (bijv. niet gezaghebbende ouder, pleegouders, grootouders).	De ouder die het kind erkend heeft, heeft recht op beperkte informatie waar hij/zij zelf om moet vragen. Het betreft alleen belangrijke feiten en omstandigheden dus informatie over schoolvorderingen en evt. sociaal-pedagogische ontwikkelingen op school tenzij de veiligheid van het kind niet gewaarborgd kan worden (bijv. signalen van kindermishandeling / huiselijk geweld)***	
Ouders die gescheiden zijn, waarvan 1 ouder het gezag heeft en 1 ouder het kind niet erkend heeft.	De ouder die gezag heeft. Deze bepaalt welke andere personen alle informatie mogen verkrijgen (bijv. niet gezaghebbende ouder, pleegouders, grootouders).		De ouder die geen gezag heeft en het kind niet erkend heeft.
Ouders die gescheiden zijn, waarvan beide ouders geen gezag hebben en het kind erkend hebben. Er is een voogdijmaat-regel* uitgesproken door de rechter.	De voogd. Deze bepaalt welke andere personen alle informatie mogen verkrijgen (bijv. leefgroep, niet gezaghebbende ouder, pleegouders, grootouders).	De ouders hebben recht op beperkte informatie waar zij zelf om moet vragen. Het betreft alleen belangrijke feiten en omstandigheden dus informatie over schoolvorderingen en evt. sociaal-pedagogische ont-wikkelingen op school tenzij de veiligheid van het kind niet gewaarborgd kan worden (bijv. signalen van kindermishandeling/ huiselijk geweld)***	

*****In Nederland staan alle minderjarigen (kinderen onder de 18 jaar) onder gezag. Meestal hebben de ouders samen het gezag: het “ouderlijk gezag”. Het gezag kan ook worden uitgeoefend door een ouder en een niet-ouder samen (bijvoorbeeld de partner van een vader of moeder). Dit wordt “gezamenlijk gezag” genoemd.

Als ouders scheiden behouden zij in principe beiden het gezag over het kind. Als een ander dan de ouder(s) het gezag uitoefent wordt dit “voogdij” genoemd. De voogdijmaatregel wordt uitgesproken door de kinderrechter. Dit betekent dus ook dat de ouders geen gezag meer hebben.

Wanneer er een OTS (onder toezicht stelling) wordt uitgesproken door de kinderrechter betekent dit dat de ouders (of een van de ouders) nog steeds het ouderlijk gezag heeft, maar onder toezicht staan. Er wordt dan een gezinsvoogd toegewezen.

***** Hierbij zijn twee uitzonderingen:**

1) de informatie wordt niet verstrekt als de school de informatie niet op dezelfde manier aan de ouder met het ouderlijk gezag zou verstrekken;
2) de informatie wordt niet verstrekt als het belang van het kind zich tegen het verschaffen van de informatie verzet.

Voor meer info: https://onderwijsgeschillen.nl/thema/informatieverstrekking-aan-gescheiden-ouders#wettelijke

Bijlage 6: Wat doet Kindante in het kader van veiligheid van het netwerk en hardware ?

Data

Laten we als eerste benoemen dat het hacken van software en netwerken nooit 100% uitgesloten kan worden. Maar de kans wordt aanzienlijk verkleind als je bij een gerenommeerd, ISO gecertificeerd datacentrum bent aangesloten. Unilogic beheert ons netwerk en onze data op professionele wijze en wij vertrouwen als stichting op de expertise en beveiliging van dit bedrijf. Unilogic is ISO gecertificeerd en dient zich te houden aan de 'ISO 27001 Informatiebeveiliging'. Zij voeren zelf voortdurend risicoanalyses uit en handelen dienovereenkomstig volgens de wet.

Data op het netwerk wordt afgeschermd door medewerkers een persoonlijk account te geven met voor hun toepasselijke rechten op de dataschijven. E.e.a. wordt afgedekt door identity-management middels de tool EDUgrip.

Datamappen met bestanden waarin privacygevoelige of vertrouwelijke gegevens zijn op het Bureau, net als op scholen van Kindante alleen maar toegankelijk voor de personeelsleden die expliciet toegang hebben verkregen tot deze datamappen.
Alle personeelsleden van Kindante kunnen extern via elk apparaat toegang krijgen tot het netwerk van Kindante via de applicatie 'Verbinding maken via extern bureaublad'. Zij moeten daar met hun persoonlijk inloggegevens inloggen.

Door herhaalde nieuwsberichten voor alle Kindantepersoneel en voortdurende aandacht voor dit thema tijdens bijvoorbeeld directieberaden en Kenniskringen van Kindante, blijven we inspanningen leveren om op het netvlies van personeelsleden te houden, dat we veilig dienen om te gaan met data en privacygevoelige gegevens. De zwakste schakel is immers de mens zelf.

Hardware

Hardware waarmee toegang wordt verkregen tot het netwerk van Kindante moet worden gecertificeerd en geïnstalleerd door Unilogic. Alleen dan kan een apparaat op het netwerk inloggen. Omdat het netwerk en alle hardware door dezelfde partij op professionele wijze is geconfigureerd en up-to-date wordt gehouden, wordt de kans op hacken aanzienlijk verkleind.

Aangezien al onze data staat opgeslagen in het datacenter van Unilogic is het fysiek beveiligen van onze computers in feite geen issue. Als een computer zou worden meegenomen is dit vervelend maar geen datalek, want er staat geen informatie op de harde schijven. Dit wordt door de installatie van Unilogic onmogelijk gemaakt.
Bij een laptop wordt vaak wel de harde schijf gebruikt, dus als deze wordt ontvreemd of verloren is er wél kans op een datalek.

Accountbeleid

Het aanmaken van netwerkaccounts wordt door de Helpdesk van Unilogic gedaan of door de ICT-er op school. Daar is een procesdocument voor gemaakt dat voor iedereen toegankelijk is via ons intranet. Het beheer van deze accounts ligt op schoolniveau. Voor het Bureau wordt dit gedaan door Domein ICT. Zij kunnen ook, indien noodzakelijk, alle andere accounts van Kindante beheren (en dus acuut blokkeren, mocht dat nodig zijn). Door steekproeven wordt toegezien op het correct uitvoeren van handelen op schoolniveau m.b.t. accountbeheer: is een personeelslid werkzaam geworden op een andere Kindantelocatie in een ander ICT-technisch domein, dan dient het bestaande account te worden geblokkeerd, c.q. verwijderd !
Er zijn strikte protocollen met works-arounds opgesteld door domein ICT, waarin vermeld staat wat m.b.t. accountbeheer (toegang van tot het netwerk en diverse softwarepakketten) moet worden aangepast in geval van

- Een uitdiensttreding van een directielid of personeelslid van bureau Kindante
- Een wisseling van school door een directielid
- Het sluiten van een school
- Een fusie van scholen

Intern beleid stimuleert mensen om regelmatig hun wachtwoord te wijzigen. Ze zijn het echter (nog) niet verplicht, daar wordt wel over nagedacht omdat dit een mogelijk risico vormt. Mensen die hun wachtwoord niet meer weten kunnen via de helpdesk van Unilogic een nieuw wachtwoord vragen, de helpdesk hanteert daarbij de werkwijze dat ze het tijdelijke wachtwoord mailen naar een directe collega van de persoon, zodat ze zeker weten dat het op de juiste locatie terecht komt. Telefonisch worden nooit wachtwoorden verstrekt.
Voor alle overige wijzigingen wordt een autorisatietabel bijgehouden door Domein ICT op het Bureau. Alleen de mensen in deze tabel mogen bepaalde wijzigingen op school aanvragen. Deze tabel wordt in elk geval jaarlijks, en indien nodig vaker, bijgewerkt.

Onbeheerde computers worden op het bestuurskantoor na 10 min inactiviteit vergrendeld. Mensen worden echter gestimuleerd om zélf hun computer te vergrendelen als ze hun werkplek verlaten om een datalek' te voorkomen. Op scholen wordt de automatische vergrendeling nog niet toegepast omdat p.c.'s van leerkrachten vaak zijn verbonden aan digitale borden en dus ook daar een zwart scherm wordt getoond bij uitblijvende activiteit op de p.c. Het verdient voortdurende aandacht van allen, om elkaar aan te spreken op "openstaande beeldschermen" !
Het leerlingadministratie- en volgsysteem (ESIS) bevat veel privacygevoelige informatie over leerlingen (en ouders). Dit is een webapplicatie die overal ter wereld te benaderen is. In dit pakket is het momenteel verplicht voor iedere gebruiker om iedere 3 maanden het wachtwoord aan te passen. Dit is door een bovenschoolse supervisor ingesteld. Het wachtwoord moet voldoen aan de eisen die het pakket stelt. Ook heeft de applicatie de ingebouwde beveiliging dat mensen na 20 minuten inactiviteit worden uitgelogd.
Er zijn op dit moment 3 bovenschoolse personeelsleden in de rol van "supervisors" binnen de applicatie, die vanwege hun werkzaamheden toegang hebben tot Esis-data van alle scholen, zij werken allen op het Bureau van Kindante. Zij zijn allen gemachtigd om een account te blokkeren als dat nodig is.

De toegang tot Basispoort, en de programma's die daarachter zitten, wordt door de meeste scholen ook via ESIS geregeld. Als medewerkers worden toegevoegd in ESIS krijgen ze middels een koppeling automatisch toegang tot Basispoort. Als er medewerkers vertrekken is het de verantwoordelijkheid van de school om deze mensen weer te verwijderen. Unilogic heeft het voor onze scholen mogelijk gemaakt dat mensen via een single sign-on in Basispoort kunnen.

De personeels- en salarisadministratie wordt gedaan in AFAS. De medewerkers die toegang hebben tot deze gegevens werken allen op het Bureau en hebben voor hun werkzaamheden toegang tot AFAS Profit middels een eigen, voor hun werkzaamheden afgestemde, account. Alle andere medewerkers hebben alleen toegang tot AFAS InSite waarbij zij alleen voor hun toegankelijke en relevante informatie kunnen zien.

De veiligheid en toegang tot alle softwarepakketten wordt door de leveranciers bepaald. Voor alle pakketten is een bewerkersovereenkomst gemaakt of opgevraagd zodat de privacy van ‘onze’ leerlingen en medewerkers gewaarborgd is. Zie voor meer informatie “Toepassing van de Wet op Privacy Persoonsgegevens op Kindantescholen”.

Wat kan een medewerker doen om datalekken te voorkomen?

ICT-protocol
Iedere werknemer dient op de hoogte te zijn van de inhoud van het document “Gedragscode ICT”. Hierin staan richtlijnen voor een Kindantemedewerker hoe om te gaan met ICT-hardware, software en sociale media.

Data
Medewerkers van Kindante worden geacht om alleen maar te werken met kind- of personeelsgevoelige informatie op het netwerk van Kindante of binnen de webapplicaties die de school/stichting in gebruik heeft. Het is zeker niet de bedoeling om privacygevoelige informatie mee naar huis te nemen op USB-sticks/Cd-roms of naar privé-emailadressen te sturen en/of thuis op een eigen apparaat op te slaan! Personeelsleden die thuis willen werken moeten dit doen via de beveiligde optie ‘Verbinding via extern bureaublad’.

Als een medewerker vermoedt dat hij of zij te veel rechten heeft gekregen op het netwerk en daardoor privacygevoelige informatie kan inzien, dan behoort hij of zij dit aan de leidinggevende te melden.

Personeelsleden worden geacht hun wachtwoorden niet af te geven aan anderen, mensen niet te laten meekijken bij het intypen van wachtwoorden en wachtwoorden regelmatig aan te passen, ook al dwingt het systeem je daar niet toe.

Hardware
PC’s die in gebruik zijn dienen te worden vergrendeld als de gebruiker zijn werkplek verlaat.
Laptops behoren nooit onbeheerd achtergelaten te worden. Bij vervoer van hardware dat eigendom is van school moet dit zo veel mogelijk onzichtbaar (bv in een kofferbak) gebeuren. Kantoren en lokalen waarin zich hardware bevindt dienen niet toegankelijk te zijn voor buitenstaanders als er geen werknemers aanwezig zijn.