Informatiebeveiliging en privacy beleid (IBP) Kindante,

volgens de AVG (Algemene Verordening Gegevensbescherming)

Versie	Status	Datum	Auteur	Omschrijving
1.0	Vastgestelde versie door CvB	11-01-2018	Ed Tous-saint	
1.1		22-02-2018	Ed Tous-saint	Bijlage 9 toegevoegd: Protocol rollen en rechten in Esis
1.2		27-03-2018	Ed Tous-saint	Hoofdstuk 10: uitwisseling leerlinggegevens, toegevoegd: beschermde datamappen en implementatie Cryptshare
1.3		03-04-2018	Ed Tous-saint	Lijst bewerkersovereenkomsten geüpdatet
1.4		17-04-2018	Ed Tous-saint	Update protocol Esis rollen en rechten

INHOUD

1 Samenvatting

Deze beleidsnotitie gaat over de consequenties van de Europese wet AVG voor Kindante en haar scholen : De Algemene Verordening Gegevensbescherming die met ingang van 1 mei 2018 van kracht wordt.
Kindante heeft afspraken en procedures vastgesteld in de eerder verschenen beleidsnotitie in relatie tot de WBP: Wet bescherming Persoonsgegevens. Deze is nu aangepast aan de nieuwe AVG – wetgeving. Daarmee komt de beleidsnotitie vanuit de WBP te vervallen.

In het kort de **belangrijkste** punten:

- Een school communiceert transparant naar ouders over welke gegevens van kinderen worden vastgelegd, met welk doel en hoe ze worden beveiligd.
  Hierbij zijn de vuistregels in hoofdstuk 4.2 bindend: Doelbepaling, Doelbinding, Grondslag, Dataminimalisatie, Transparantie en Data-integriteit.

- Ouders moeten weten dat zij als “eigenaar” van die gegevens op ieder moment inzage mogen hebben in die gegevens en waar toegestaan die mogen wijzigen. Het gaat dan met name over het leerlingdossier, en n.a.w.-gegevens. (Transparantie)

- Ouders moeten ieder jaar opnieuw toestemming geven of de school foto – of filmmateriaal mag gebruiken waarop hun kind is afgebeeld.

- Er zijn bewerkersovereenkomsten getekend met alle partijen die digitale gegevens bewaren en/of verwerken. Op hoofdlijnen zijn die getekend op bestuursniveau met b.v. alle grote uitgevers van educatieve software en andere partijen. Zijn er andere partijen dan in de lijst in bijlage 5, dan moet de school zelf met die partij een bewerkersovereenkomst afsluiten.

- Alle medewerkers moeten zich bewust zijn/worden van privacygevoelige informatie, die voor de uitoefening van het beroep noodzaak zijn, maar die voor andermans ogen niet is bestemd! Privacy is een recht!
  In bijlage 7 wordt duidelijk wat dat in de dagelijkse schoolpraktijk betekent.

- In een organisatiestructuur wordt duidelijk gemaakt hoe Kindante het continu proces van Beveiliging en Privacy waarborgt. (Hoofdstuk 6)

- Uitgelegd wordt hoe Kindante controleert en rapporteert ook in het geval van bijvoorbeeld een datalek. (Hoofdstuk 7)

- Kindante heeft een vastgestelde Privacyreglement geldend voor alle leerlingen en medewerkers. (Hoofdstuk 8)

- Kindante legt uit welke procedures en work-arounds worden gehanteerd in het kader van veiligheid van het netwerk en hardware. (o.a. accountbeheer)

- Kindante legt uit hoe leerlinggegevens digitaal uitgewisseld dienen te worden in (Hoofdstuk 10)

2 Inleiding

Het onderwijsveld is in toenemende mate afhankelijk van informatie en (meestal geautomatiseerde) informatievoorzieningen. Ook neemt de hoeveelheid informatie toe door educatieve softwareontwikkelingen . Deze afhankelijkheid van ICT en gegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het is van belang om adequate maatregelen te nemen op het gebied van informatiebeveiliging en privacy (IBP) om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.

Toelichting informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten van de informatievoorziening te garanderen. Deze aspecten zijn:

- Beschikbaarheid: de mate waarin gegevens en/of functionaliteiten beschikbaar zijn op de juiste momenten.
- Integriteit: de mate waarin gegevens en/of functionaliteiten juist en volledig zijn.
- Vertrouwelijkheid: de mate waarin de toegang tot gegevens en/of functionaliteiten beperkt is tot degenen die daartoe bevoegd zijn.

Onvoldoende informatiebeveiliging kan leiden tot onacceptabele risico's bij de uitvoering van onderwijs en bij de bedrijfsvoering van de instelling. Incidenten en inbreuken in deze processen kunnen leiden tot financiële schades en imagoverlies.

Toelichting privacy

Privacy gaat over persoonsgegevens. Persoonsgegevens dienen beschermd te worden conform huidige wet – en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die herleidbaar zijn tot een bepaald individu. Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens. De wet noemt als voorbeelden van verwerking: *het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekking door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, afschermen, uitwissen en vernietigen van gegevens.*

Vervlechting informatiebeveiliging en privacy

Uit voorgaande blijkt dat informatiebeveiliging een belangrijk onderdeel is van privacy, terwijl omgekeerd de zorgvuldige omgang met persoonsgegevens noodzakelijk is voor informatiebeveiliging. Beide begrippen staan naast elkaar, en zijn van elkaar afhankelijk. Het onderwerp informatiebeveiliging

en privacy wordt afgekort tot IBP. Dit beleid ligt ten grondslag aan de aanpak van informatiebeveiliging en privacy binnen de Stichting Kindante[1].

3 Doel en reikwijdte

Doel

Dit beleid heeft als doelen:

- Het waarborgen van de continuïteit van het onderwijs en de bedrijfsvoering.
- Het garanderen van de privacy van leerlingen en medewerkers waardoor beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen.

Dit beleid is erop gericht om de kwaliteit van de verwerking van informatie en de beveiliging van persoonsgegevens te optimaliseren waarbij een goede balans moet zijn tussen privacy, functionaliteit en veiligheid. Uitgangspunt is dat de persoonlijke levenssfeer van de betrokkene, met name van medewerkers en leerlingen, wordt gerespecteerd en Kindante voldoet aan relevante wet- en regelgeving.

Reikwijdte

- Het informatiebeveiligings- en het privacy beleid binnen Kindante geldt voor alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur / outsourcing), alsmede voor alle organisatieonderdelen. Onder dit beleid vallen ook alle devices van waar geautoriseerde toegang tot het schoolnetwerk verkregen kan worden.
- De nadruk van het beleid ligt op die toepassingen, die vallen onder de verantwoordelijkheid van Kindante. Het beleid heeft zowel betrekking op gecontroleerde informatie, die door de school zelf is gegenereerd en wordt beheerd. Daarnaast is het ook van toepassing op niet-gecontroleerde informatie waarop de school kan worden aangesproken, zoals uitspraken van medewerkers en leerlingen in discussies, op (persoonlijke pagina's van) websites.
- Het beleid heeft betrekking op het verwerken van persoonsgegevens van alle betrokkenen binnen Kindante waaronder in ieder geval alle medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers en externe relaties (inhuur/outsourcing), evenals op andere betrokkenen waarvan <naam school> persoonsgegevens verwerkt.
- In het beleid ligt de nadruk op de, geheel of gedeeltelijk, geautomatiseerde/systematische verwerking van persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van kindante evenals op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Het beleid is ook van toepassing op niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

[1] In dit beleidsstuk wordt onder "Stichting Kindante" verstaan: alle scholen, kantoren en betrokkenen binnen Kindante: medewerkers, leerlingen, ouders/verzorgers, (geregistreerde) bezoekers, externe relaties en andere betrokkenen.

- IBP-beleid binnen Kindante heeft raakvlakken met:
  - Algemeen veiligheids- en toegangsbeveiligingsbeleid; met als aandachtspunten bedrijfshulpverlening, fysieke toegang en beveiliging, crisismanagement, huisvesting en ongevallen
  - Medewerkers - en organisatiebeleid; met als aandachtspunten in- en uitstroom van medewerkers, functiewisselingen, functiescheiding en vertrouwensfuncties
  - IT-beleid; met als aandachtspunten aanschaf, beheer en gebruik van ict en (digitale) leermiddelen
  - Medezeggenschap van leerlingen, hun ouders/verzorgers en medewerkers
  - Beleid inzake aanschaf en gebruik van digitale leermiddelen

4 Uitgangspunten

Algemene beleidsuitgangspunten

De belangrijkste beleidsuitgangspunten bij Kindante zijn:

- Informatiebeveiliging en het privacy dient te voldoen aan alle relevante wet- en regelgeving, in het bijzonder aan de Wet bescherming persoonsgegevens en de Algemene Verordening Gegevensbescherming (die 25 mei 2018 in werking treedt).
- De verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondslagen. Waarbij een goede balans tussen het belang van Kindante om persoonsgegevens te verwerken en het belang van betrokkene om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn persoonsgegevens van belang is.
- Binnen Kindante is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort niet alleen het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie, maar ook van fysieke documenten.
- De school is als rechtspersoon eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd. Daarnaast beheert de school informatie, waarvan het eigendom (auteursrecht) toebehoort aan derden. Medewerkers en leerlingen moeten goed geïnformeerd worden over de regelgeving rond het gebruik van informatie.
- Informatie heeft een waarde: financieel, economisch maar zeker ook emotioneel. Er is een balans tussen de risico's van hetgeen we willen beschermen en de benodigde investeringen en maatregelen.
- Kindante sluit met alle leveranciers van digitale onderwijsmiddelen (zowel van educatieve als bedrijfsapplicaties) bewerkersovereenkomsten af als zij persoonsgegevens ontvangen van de school. Hierbij wordt gebruik gemaakt van de meest recente versie van het convenant 'Digitale leermiddelen privacy' (www.privacyconvenant.nl) en de bijbehorende model bewerkersovereenkomst. Dit geldt ook voor overheids- en andere instellingen indien er gegevens van leerlingen of medewerkers worden verstrekt, al dan niet op wettelijke basis.
- Er wordt van alle medewerkers, leerlingen, (geregistreerde) bezoekers en externe relaties verwacht dat zij zich 'fatsoenlijk' gedragen met een eigen verantwoordelijkheid. Het is niet acceptabel dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies. Kindante heeft hiervoor een gedragscode ICT en social mediaprotocol geformuleerd, vastgesteld en geïmplementeerd.

- Informatiebeveiliging en privacy is bij Kindante een continu proces, waarbij regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing gewenst is.
- Bij wijzigingen in de infrastructuur of de aanschaf van nieuwe (informatie)systemen, wordt bij Kindante vanaf de start rekening gehouden met informatiebeveiliging en privacy.

Uitgangspunten privacy

De vijf vuistregels met betrekking tot de omgang van persoonsgegevens bij Kindante zijn:

1. **Doelbepaling en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doelen waarvoor ze zijn verkregen.
2. **Grondslag**: verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen: toestemming, overeenkomst, de wet, publiekrechtelijke taak, vitaal belang van de betrokkene, of gerechtvaardigd belang.
3. **Dataminimalisatie**: bij de verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt: het type persoonsgegevens moet redelijkerwijs nodig zijn om het doel te bereiken; ze staan in verhouding tot het doel (= proportioneel). Het doel kan niet met minder, alternatieve of andere gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie**: de school legt aan betrokkenen (leerlingen, hun ouders en medewerkers) op transparante wijze verantwoording af over het gebruik van hun persoonsgegevens, alsmede over het gevoerde IBP-beleid. Deze informatievoorziening vindt ongevraagd plaats. Daarnaast hebben deze betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun Persoonsgegevens. Daarnaast kunnen betrokkenen zich verzetten tegen het gebruik van hun gegevens.
5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.

Persoonsgegevens moeten adequaat worden beveiligd volgens algemeen en breed geaccepteerde beveiligingsnormen.

Bij alle registraties op basis van toestemming, zal Kindante alle de betrokkenen (ouders, verzorgers) eenduidig informeren, dat de gegeven toestemming op ieder wenselijk moment kan worden ingetrokken.

5 Wet- en regelgeving

Kindante voldoet aan alle van toepassing zijnde relevante wet- en regelgeving, waaronder:

- Wet op het primair onderwijs en/of Wet voortgezet onderwijs
- Wet goed onderwijs en goed bestuur PO/VO
- Wet bescherming persoonsgegevens
- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Leerplichtwet
- Auteurswet
- Wetboek van Strafrecht

Hiernaast zijn de bepalingen van het convenant 'Digitale onderwijsmiddelen en privacy 2.0' leidend bij het maken van afspraken met leveranciers.

6 Organisatie

De organisatie van IBP gaat over processen, gewoontes, beleid, wetten en regels die van betekenis zijn voor de manier waarop mensen een organisatie sturen, besturen, beheren en controleren. Hierbij spelen de relaties tussen de verschillende betrokkenen en de doelen van de organisatie een rol. Dit hoofdstuk beschrijft hoe IBP binnen Kindante is georganiseerd. Er wordt daarbij onderscheid gemaakt tussen drie niveaus:

- Richtinggevend (strategisch)
- Sturend (tactisch)
- Uitvoerend (operationeel)

Voor elk niveau wordt beschreven welke rollen welke verantwoordelijkheden en taken hebben en wat de documenten zijn die daarbij passen

Rollen (functies) rondom IBP

Om informatiebeveiliging en privacy gestructureerd en gecoördineerd op te pakken worden bij Kindante een aantal rollen onderkend die aan medewerkers in de bestaande organisatie zijn toegewezen.

Richtinggevend

Eindverantwoordelijke
Het College van Bestuur is eindverantwoordelijk voor IBP en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging en privacy vast. De toepassing en werking van het IBP-beleid wordt op basis van regelmatige rapportages geëvalueerd. De inhoudelijke verantwoordelijkheid voor IBP is gemandateerd aan de manager IBP.

Sturend

Manager IBP
Manager IBP is een rol op sturend niveau. Hij/zij geeft terugkoppeling en advies aan de eindverantwoordelijke en stuurt de mensen aan op uitvoerend niveau. Deze rol is belegd bij de domeinverantwoordelijke ICT-Onderwijs binnen Kindante. De manager IBP moet:

- Het beleid vertalen naar richtlijnen, procedures, maatregelen en documenten voor de gehele instelling
- De uniformiteit bewaken binnen Kindante
- Het aanspreekpunt zijn voor incidenten op het gebied van informatiebeveiliging en privacy
- De verdere afhandeling van incidenten binnen Kindante coördineren

De manager IBP en de ICT-applicatiebeheerder van Kindante adviseren samen het College van Bestuur en zijn verantwoordelijk voor het organiseren van ICT en informatiebeveiliging binnen Kindante.

DPO Data Protection Officer
De Data Protection Officer, houdt binnen Kindante en collega-besturen toezicht op de toepassing en naleving van de AVG. De wettelijke taken en bevoegdheden van de DPO geven deze functionaris een onafhankelijke positie in de organisatie. De DPO zorgt voor het afhandelen van vertrouwelijke informatiebeveiligingsincidenten. De DPO heeft regelmatig overleg met manager IBP. De DPO is meestal ook de contactpersoon voor klachten en vragen van betrokkenen.

Domeinverantwoordelijke / proceseigenaar
Binnen Kindante BURO zijn er verschillende domeinen/processen, zoals ICT, Personeel (HRM, P&O), administratie, secretariële, facilitaire- en financiële zaken en onderwijs. Op scholen zijn Kindantemedewerkers in diverse functies en rollen binnen school werkzaam. Op elk van deze domeinen/processen, zowel op BURO als op scholen is iemand verantwoordelijk om te bepalen op welke wijze IBP daarbinnen wordt vormgegeven in richtlijnen, procedures en instructies.

Deze proceseigenaar is tevens verantwoordelijk voor de risico's die veroorzaakt worden doordat personen of applicaties ten onrechte toegang krijgen tot applicaties. Om deze risico's te verkleinen hebben proceseigenaren de volgende specifieke taken:

- Samen met het College van Bestuur stellen zij het beleid voor toegang vast.
- Samen met de manager IBP en de ICT-applicatiebeheerder zien zij erop toe dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten of applicaties waarvoor zij specifiek bevoegd zijn.
- Samen met de manager IBP en ICT-applicatiebeheerder beoordelen zij regelmatig de toegangsrechten van gebruikers.

Leidinggevenden hebben hierbij een voorbeeldrol ten opzichte van hun medewerkers.

Uitvoerend

Data Protection Manager
De Data Protection manager vormt een technisch aanspreekpunt inzake informatiebeveiliging voor de manager IBP, de applicatiebeheerder van Kindante, proceseigenaren (b.v. een ICT-er op school) en leidinggevenden (directieleden op school of domeinverantwoordelijken op het BURO).

Proceseigenaren
Vanuit de manager IBP en applicatiebeheerder van Kindante worden proceseigenaren en leidinggevenden voorzien van een ingevuld werkpakket, bestaande uit richtlijnen, procedures en instructies. Op basis hiervan voert hij zijn of haar taken uit. Op scholen bepaalt de leidinggevende wie deze taak/rol van functioneel beheer uitvoert, meestal vanwege het hoge “ICT-gehalte” de ICT-er op school).

Medewerker
Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging in hun dagelijkse werkzaamheden. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund met checklists en formulieren.

Medewerkers worden gevraagd om actief betrokken te zijn bij informatiebeveiliging. Dit kan door meldingen te maken van security incidenten, het doen van verbetervoorstellen en het uitoefenen van invloed op het beleid (individueel of via de (G)MR.
Voor alle medewerkers worden praktische voorbeelden, gerelateerd aan de AVG op een rijtje gezet (bijlage 7) en een gedragscode aangereikt inclusief sociale media-richtlijnen (bijlage 8).

Leidinggevende
Naleving van het informatiebeveiligingsbeleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende zowel op BURO als op scholen van Kindante heeft op uitvoerend niveau de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het beveiligingsbeleid;
- toe te zien op de naleving van het IBP-beleid door de medewerkers, waarbij hij/zij zelf een voorbeeldfunctie heeft;
- periodiek het onderwerp IBP onder de aandacht te brengen in werkoverleggen, beoordelingen etc.;
- als aanspreekpunt beschikbaar te zijn voor alle medewerkers gerelateerde IBP-onderwerpen.

De leidinggevende kan in zijn taak ondersteund worden door de manager IBP.

7 Controle en rapportage

Dit informatiebeveiligings- en privacybeleid wordt minimaal elke twee jaar getoetst en bijgesteld door de DPO,en manager IBP . Hierbij wordt rekening gehouden met:

- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's)
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan

Daarnaast kent Kindante een jaarlijkse planning en control cyclus voor informatiebeveiliging en privacy. Dit is een periodiek evaluatieproces waarmee de inhoud en effectiviteit van het informatiebeveiligings- en privacybeleid wordt getoetst.

Voor alle overlegmomenten geldt dat deze zoveel mogelijk ingepast worden in bestaande overlegvormen met hetzelfde karakter waarbij op:

- **strategisch** niveau richtinggevend wordt gesproken over organisatie en compliance, alsmede over doelen, scope en ambitie op het gebied van IBP. (Domeinoverleg BURO Kindante)
- **tactisch** niveau wordt de strategie vertaald naar plannen, te hanteren normen, evaluatiemethoden, e.d. Deze plannen en instrumenten zijn sturend voor de uitvoering. (Directieberaad Kindante)
- **operationeel** niveau worden de onderwerpen besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. Deze overlegvorm wordt decentraal georganiseerd, en indien nodig in elk organisatieonderdeel van kindante. (op schoolniveau of tijdens Kenniskringen ICT)

Voorlichting en bewustzijn

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom wordt bij kindante het bewustzijn van de individuele medewerkers voortdurend aangescherpt, zodat de kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, deelnemers en gasten. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van de manager IBP/ applicatiebeheerder ICT/ Data Protection Manager met het College van Bestuur als eindverantwoordelijke.

Classificatie en risicoanalyse

Voor zover bekend tijdens het vaststellen van dit document krijgen alle aandachtsgebieden binnen het kader van de wetgeving een plek. In het proces van verdere professionalisering, mede door de invulling van de functie van een Data Protection Manager, zullen classificering van gegevens, risicoanalyses en te nemen beveiligingsmaatregelen verder worden ontwikkeld. Daarbij zijn beschikbaarheid, integriteit en vertrouwelijkheid de kwaliteitsaspecten die van belang voor de informatievoorziening

Controle, naleving en sancties

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het IBP-proces. Van belang hierbij is dat leidinggevenden en proceseigenaren hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Bij Kindante wordt actief aandacht besteed aan IBP bij de aanstelling, tijdens functioneringsgesprekken, met een instelling brede gedragscode, met periodieke bewustwordingscampagnes, et cetera.
Voor de bevordering van de naleving van de Wet bescherming persoonsgegevens vervult de Data Protection Officer een belangrijke rol. De DPO wordt aangesteld door het College van Bestuur, en heeft een wettelijk omschreven en onafhankelijke toezichthoudende taak. De DPO werkt via een door het CvB vast te stellen reglement.
Mocht de naleving ernstig tekortschieten, dan kan Kindante de betrokken verantwoordelijke medewerkers een sanctie op leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.
Bij Kindante is het melden van beveiligingsincidenten en datalekken vastgelegd in een protocol.

8 Privacyreglement

In het privacyreglement (bijlage 2) legt Kindante uit, hoe zij omgaat met de persoonsgegevens van medewerkers en leerlingen.

9 Transparante informatie voor school en ouders

In bijlage 9 wordt uitgelegd welke gegevens door school worden bewaard en voor welke termijn. Dit is relevante informatie voor de ouders die in een schoolgids zou kunnen worden opgenomen.

10 Uitwisselen van leerlinggegevens

met OSO (Overstap Service 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;
- 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.

Met behulp van beschermde Datamappen

Kindante voorziet scholen en BURO in een dataschijf, waarop submappen zichtbaar zijn voor die (groepen) mensen, die geautoriseerd zijn om die map in te zien, of te bewerken. Medewerkers die vanuit leerlingenzorg (ambulant begeleiders, specialisten) privacy gevoelige data willen delen, kunnen dit hier in afgeschermde mappen binnen het beveiligde netwerk van Kindante.

Met behulp van Cryptshare

Kindante installeert voor alle accounts in het netwerk (dus voor alle medewerkers) de plug-inn Cryptshare in de bestaande Microsoft-outlookomgeving. In outlook wordt een knop zichtbaar van Cryptshare. Als deze wordt gebruikt, verzendt de gebruiker de mail die middels encryptie wordt verzonden, inclusief de eventuele bijlage(n). Verificatie is een optie, waarbij de ontvanger ook (per sms of app of samen afgesproken wachtwoord) de mail en bijlage(n) kan openen. Daarnaast kent iedere verzonden mail een expiratiedatum (max 7 dagen); na deze tijd is de ontvanger niet meer in staat de mail (link in een mail) te openen en dus de mail en eventuele bijlage(n) te openen.

11 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 medewerkers 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 3.
Wanneer scholen beeldmateriaal van leerlingen publiceren, moeten zij passende technische en organisatorische maatregelen treffen om deze te beschermen. Deze maatregelen moeten een bepaald beveiligingsniveau garanderen, zodat foto’s niet in verkeerde handen terecht komen. Een passende technische maatregel kan zijn om een portal op de website te plaatsen die alleen toegankelijk is voor leerlingen en hun ouders/voogd met bijvoorbeeld een persoonlijke inlognaam en wachtwoord.

Makkelijker is het, om kinderen niet direct herkenbaar met gezicht in beeld te filmen of te fotograferen !

12 Protocol Datalekken

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. Uit de praktijk: verlies of diefstal van een iPad, laptop, dossiertas, etc.

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

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

Wat kan een medewerker doen om datalekken te voorkomen?

Iedere werknemer dient op de hoogte te zijn van de inhoud van het document “Gedragscode ICT en Social Mediabeleid”. 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! Medewerkers 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.

Medewerkers 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.

Bijlage 1: Tabel IBP rollen en taken

Niveau	**Wie** **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren/ vastleggen**
Richtinggevend (strategisch)	Voorbeelden: Bestuur CvB Directeur	• Eindverantwoordelijk • IBP-beleidsvorming, -vastlegging en het uitdragen ervan • Verantwoordelijk voor het zorgvuldig en rechtmatig verwerken van persoonsgegevens • Evalueren toepassing en werking IBP-beleid op basis van rapportages • Organisatie IBP inrichten	• Informatiebeveiligings- en privacy beleid • Baseline/ basismaatregelen • Reglement FG vaststellen • Privacyreglement vaststellen

Sturend (tactisch)	Manager IBP	• Inhoudelijk verantwoordelijk voor IBP
		• IBP-planning en controle
		• Adviseert bestuur/CvB/directie over IBP
		• Voorbereiden uitvoeren IBP-beleid, Classificatie/risicoanalyse
		  • Hanteren IBP normen en wijze van toetsen
		  • Evalueren IBP-beleid en maatregelen
		  • Uitwerken algemeen beleid naar specifiek beleid op een uniforme wijze
			Processen, richtlijnen en procedures IBP, waaronder:
			
			• Activiteitenkalender
			• Protocol beveiligingsincidenten en datalekken
			• Bewerkersovereenkomsten regelen
			• Brief toestemming gebruik foto's en video
			• Opstellen informatie documentatie richting leerlingen, ouders/ verzorgers
			• Security awareness activiteiten

		• Schrijven en beheren van processen, richtlijnen en procedures om de uitvoering te ondersteunen	• Sociale media reglement • Gedragscode ICT en internetgebruik • Gedragscode medewerkers en leerlingen
	Functionaris voor Gegevensbescherming/ Privacy officer	• Toezicht op naleving privacywetgeving • Richtlijnen, kaders vaststellen en aanbevelingen doen t.b.v. verbeterde bescherming van verwerkingen van persoonsgegevens • Afwikkeling klachten en incidenten	• Privacyreglement, • Procedure IBP-incident afhandeling • Inrichten meldpunt datalekken
	Domeinverantwoordelijke/ Proceseigenaren waaronder: ict, personeel (HRM / P&O), Facilitair, onderwijs , financiën, inkoop en administratie	• **Classificatie/ risicoanalyse** in samenwerking met Manager IBP (Informatiemanager/ verantwoordelijke IBP/ Security officer) • Toegangsbeleid zowel fysiek als digitaal vaststellen en laten goedkeuren door *bestuur/CvB/directie* • *Samen met functioneel beheer en ICT beheer* er op toezien dat gebruikers alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn. • *Samen met functioneel beheer en ICT* beheer de toegangsrechten van gebruikers regelmatig beoordelen en controleren.	• Inventariseren waar persoonsgegevens van de school terechtkomen (leveranciers lijst) • Classificatie- en risicoanalyse documenten. Diverse aanvullende beleidsstukken, richtlijnen, procedures en protocollen, waaronder: • Toegangsmatrix diverse informatiesystemen en netwerk

Niveau	**Wie** **Rollen**	**Hoe** **Verantwoordelijkheid / taken**	**Wat** **Realiseren/ vastleggen** **Vanuit de Wiki**
Uitvoerend (operationeel)	Security officer Functioneel beheerder	• Incidentafhandeling (registreren en evalueren). • Technisch aanspreekpunt voor IBP-incidenten. • Uitvoeren taken conform gegeven richtlijnen en	

		procedures.	
	Medewerker Dagelijkse leiding/ leidinggevende/ directie	• Verantwoordelijk omgaan met IBP bij hun dagelijkse werkzaamheden. • Communicatie naar alle betrokkenen; ervoor zorgen dat medewerkers op de hoogte zijn van het IBP-beleid en de consequenties ervan. • Toezien op de naleving van het IBP-beleid en de daarbij behorende processen, richtlijnen en procedures door de medewerkers. • Voorbeeldfunctie met positieve en actieve houding t.a.v. IBP-beleid. • Implementeren IBP-maatregelen. • Periodiek het onderwerp informatiebeveiliging onder de aandacht te brengen in werkoverleggen, beoordelingen etc.; • Rapporteren voortgang m.b.t. doelstellingen IBP-beleid aan bestuur.	Communiceren, informeren en toezien op naleving van o.a.: • IBP in het algemeen • Regels passend onderwijs • Hoe omgaan met leerling dossiers • Wie mogen wat zien • Gedragscode • Omgaan met sociale media • Mediawijs maken

Bijlage 2: Privacyreglement

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 ver-

zochte 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.

Bijlage 3: Format Kindante: 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 onder-

tekenen 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 4: 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 sleden die expliciet toegang hebben verkregen tot deze datamappen.
Alle medewerkers 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 Kindante medewerkers en voortdurende aandacht voor dit thema tijdens bijvoorbeeld directieberaden en Kenniskringen van Kindante, blijven we inspanningen leveren om op het netvlies van medewerkers 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 medewerker 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 medewerker 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"!
Alle medewerkers hebben een code om beveiligd te kunnen printen op de locatie waar zij werken. Hiermee voorkom je dat privacygevoelige gegevens op een printer liggen die andere niet mogen zien.
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 medewerkers 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.
In bijlage 9 wordt in het protocol "Esis rechten en rollen" beschreven, hoe er op het accountmanagement wordt toegezien.

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 mede-

werkers 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”.

Bijlage 5: Lijst van leveranciers die persoonsgegevens verwerken met wie Kindante een bewerkersovereenkomst heeft afgesloten

AFAS
AVISION (Route 8)
Basispoort
Bloon
Cito
Clooser
Cogix
Cupella
Ecsplore
Ecsplore_Triade_GGD
Gynzy
Isy
Kwintessens
Lexima
Malmberg
Nieuwsbegrip
Noordhoff uitgevers
Oefenweb
Onderwijsmonitor Uni Maastricht
OnzeLeerling
OSO
Ouderportaal Basisonline
Robidus
Rovict
Snappet
Stimuliz
Thieme-Meulenhof
Unilogic
Zwijsen

Bijlage 6: Activiteitenkalender

Beleid Wet bescherming persoonsgegevens en protocol datalekken		Vastgesteld mei 2017
Privacyreglement		Vastgesteld mei 2017
Aanpassing Gedragscode ICT (2013)	Checken inhoudelijk op actualiteit/toevoeging Social Media protocol	Gereed en vastgesteld 1 september 2017
Aanvulling Privacyverklaring websites en cookie-beheer	Gereed voor kindante.nl 1-9-2017	Gecommuniceerd op 6 september 2017 naar organisatie
SLL-certificaten websites	Opgepakt september 2017	1 januari 2017
Lijst met bewerkersovereenkomsten op Kindanteniveau voor alle scholen getekend		Voor 95% compleet, deadline 1 januari 2018 : 100 %
Tekstuele inhoudelijke check/aanpassingen : van WBP-> naar AVG		gereed 1 januari 2018
Klankbordgroep directieleden;	Draagvlak en bewustwording creëren in Directieberaad ; delen in Kenniskringen ICT lijst van gepaste acties	gereed 1 februari 2018
Voorbereidingen aanstelling DPO (Data Protection Officer)	i.s.m. besturen MosaLira, Innovo, Movare en Kindante	i.s.m. besturen MosaLira, Innovo, Movare en Kindante. Nog in onderhandeling (1-4-2018)

Bijlage 7: Privacy in de dagelijkse praktijk

Acties	Frequentie
School	
Toestemming vragen aan ouders voor gebruik foto's kinderen voor publicatie	Jaarlijks
Toestemming vragen aan ouders voor afnemen testen Ecsplore en verwerken en delen van data	Jaarlijks
Communicatie gevolgen AVG in schoolgids + website	Jaarlijks
In de klas	
Schermbeveiliging aan als je je werkstation verlaat (Windowsknop + L)	Altijd
Geen wachtwoordenlijstjes fysiek in school aanwezig (op lessenaars, prikborden, onder pc's)	Altijd
Wachtwoorden worden nooit afgegeven aan derden (ook niet aan vervangers)	Altijd
Wachtwoorden die gebruikt worden moeten regelmatig vervangen worden. Automatisch vraagt het netwerksysteem hier halfjaarlijks om.	Regelmatig
Laat niemand meekijken bij het intypen van wachtwoorden.	Altijd
Dossiers in afgesloten kasten	Altijd
We hanteren een clean desk policy: b.v. dag-planningen met privacygevoelige informatie na werktijd opbergen (lade of kast)	Altijd
Thuis of onderweg	
Bij telewerken (of Remote Desktop applicatie) of gebruik van de omgeving van Esis of webmail is de gebruiker alert op bescherming van het device waarop hij/zij werkt	Altijd
Het is niet toegestaan gebruik te maken van USB-sticks, externe harde schijven of DVD's om privacygevoelige informatie te vervoeren.	Altijd
Bij verlies of diefstal van (mobile) devices en smartphones waarop gevoelige informatie is te ontsluiten wordt direct melding gedaan bij domein ICT (datalek)	Altijd
USB-sticks zijn verboden. Zo voorkom je dat je privacygevoelige gegevens bij verlies of diefstal openbaart (datalek!) en voorkom je verspreiding van virussen !	Altijd

Email

Het is niet toegestaan om gebruik te maken van privé mail om privacygevoelige informatie te versturen.	Altijd
Er worden nooit BSN's en andere privacygevoelige gegevens per mail verstuurd (b.v. kind dossiers)	Altijd
In een mail naar meerdere personen die elkaars emailadres niet hoeven te weten (b.v. ouders), worden alle adressen altijd in de "bcc" verstuurd	Altijd

Overig

Uitwisseling van kind-gegevens t.b.v. overstap of verhuizing naar een andere school (PO-VO) gebeurt veilig en alleen m.b.v. OSO (Overstap Service Onderwijs) ; met OSO wordt precies aangegeven WAT er mag worden overgedragen	Altijd
Check op welke gebruikers welke rechten hebben. B.v.: een leerkracht "ziet" afhankelijk van de schoolorganisatie alleen zijn eigen groep leerlingen in Esis	Altijd
Check op SSL certificaten op websites indien online invul modules gebruikt worden	Altijd

Gedragscode ICT en richtlijnen gebruik van Social Media

Versie 1: 2013
Versie 2: november 2016 (Claudia) kleine aanpassingen m.n. inhoud die niet meer relevant is.
Versie 3: augustus 2017; (Ed) update met verwijderen inhoud die niet meer van toepassing is en aanvulling social media (vastgesteld door CvB)

Inhoud

Inleiding
De gedragscode ICT van Kindante is een document dat geldt voor iedere medewerker van Kindante. In dit document wordt helder uiteengezet hoe er, in welke situatie, door medewerkers omgegaan dient te worden met:

- Het gebruik van e-mail en internet binnen het netwerk van Kindante
- Het gebruik van vaste telefonie binnen Kindante
- Het gebruik van mobiele (smart)telefonie binnen Kindante en andere mobiele apparaten
- Data (bestanden) die ontsloten worden binnen het netwerk van Kindante

Ook wordt beschreven hoe er, in welke situatie, beveiligingscontroles kunnen worden uitgevoerd op bovenstaand gebruik.
Deze gedragscode geldt voor iedereen die gebruik maakt van het netwerk van Kindante en/of zich in een Kindanteschool bevindt. In deze gedragscode wordt onder “medewerkers’ verstaan:

- Medewerkers met een arbeidsovereenkomst
- Stagiaires
- Uitzend – en freelancekrachten
- Vrijwilligers
- Ouders
- Leerlingen
- Externen

Uitgangspunt is dat iedere medewerker van Kindante de gelegenheid krijgt kennis te nemen van betreffende gedragscode. In de maatschappij zien we in toenemende mate het gebruik van:

- Smarttelefoons en tablets (met internettoegang) door kinderen en medewerkers op basisscholen
- Sms services, WhatsApp, berichten via social media
- Een fotocamera en/of videocamera op mobiele telefoonapparatuur
- Publiceren van filmpjes en fotomateriaal op vrij toegankelijke internetsites (You-Tube);
- Downloads (Lime Wire, Torrentz)
- Opslagcapaciteit en toenemend gebruik van mobiele gegevensdragers (memorysticks, externe harde schijven, Mp3-spelers, tablets, smartphones)
- Social Media zoals Facebook, LinkedIn, Twitter, Snapchat
- Chatomgevingen (Skype)

Duidelijkheid over wat mag en kan bij betreffende maatschappelijke ontwikkelingen is een vereiste om op een goede wijze om te gaan met deze voorzieningen.

Doel van deze gedragscode is:

- Handhaving van goede naam en integriteit
- Uitdragen van goede waarden en normen
- Tegengaan van “ongewenst gebruik”, seksuele intimidatie, discriminatie of ander onacceptabel gebruik
- Het in bescherming nemen van gebruikers
- Systeem en netwerkbeveiliging
- Kostenbeheersing

Kindante verwacht van medewerkers op het netwerk dat zij rekening houden met het voorgaande en daarom zorgvuldig omgaan met het ICT-netwerken van alle genoemde voorzieningen op de school en op de werkplek.
Als hoofdregel voor dagelijks gebruik geldt dan ook: gebruik de computer en de (mobiele) telefoon en/of voorzieningen in principe voor het werk en/of voor onderwijsdoeleinden. Ieder gebruik in strijd met het doel van deze gedragscode is niet toegestaan.

1. Privacy

Kindante hecht waarde aan privacy van medewerkers en kinderen. De Wet Bescherming Persoonsgegevens staat toe dat de werkgever controleert op onjuist gebruik dan wel misbruik van bedoelde voorzieningen. Deze controlemogelijkheden staan beschreven in deze gedragscode en geven aan op welke wijze en in welke situaties Kindante tot controle kan overgaan. Daarbij is het streven gericht op een goede balans tussen controle en privacybescherming.

2. Beheer

Het Kindante-netwerk wordt in eerste lijn “onderhouden” door de ICT-er op school. Het betreft hier op zeer kleine schaal het kunnen uitvoeren van handelingen, die voor het dagelijks gebruik noodzakelijk zijn. Op hoofdlijnen geschiedt alle onderhoud door Unilogic.
Indien er in deze gedragscode gesproken wordt over de netwerkbeheerder, dan wordt Unilogic Networks bedoeld. In alle andere gevallen wordt “de ICT-er op school” als terminologie gebruikt.

3. Algemene Uitgangspunten

Ieder computernetwerk kent een eigen vorm van kwetsbaarheid en beveiliging. In dit verband worden de gebruikers gewezen op het volgende:

- User-identificatie (inlognaam en wachtwoord) voor het netwerk, maar ook alle softwarepakketten waarvoor moet worden ingelogd, zijn persoonsgebonden en mogen niet aan derden worden doorgegeven.
- Het wordt aanbevolen om wachtwoorden elke drie maanden te veranderen.
- De inhoud en het onderhoud van de home-directory (het aan de gebruiker beschikbaar gestelde deel van de server) valt volledig onder de verantwoordelijkheid van de gebruiker, die deze voorziening zakelijk gebruikt en niet onnodig vult met ‘grote’ bestanden.
- Het up – en downloaden van niet aan onderwijs gerelateerde bestanden is niet toegestaan zonder uitdrukkelijke permissie van de netwerkbeheerder/ICT-er op school. Hier wordt dus niet het up – of downloaden van bestanden t.b.v. de intranetomgeving bedoeld.
- Een systeem waarop de gebruiker heeft ingelogd moet worden afgesloten op het einde van het gebruik; een systeem waarop is ingelogd mag door de gebruiker niet onbewaakt worden achtergelaten. Bij het verlaten van werkplek , wordt m.b.v. sneltoets combinatie windowstoets - L, de toegang tot het netwerk vergrendeld. Op het bestuursbureau worden pc’s na 10 minuten inactiviteit automatisch vergrendeld.
- Iedere gebruiker dient de aanwijzingen van de netwerkbeheerder/ICT-er op school in kwestie op te volgen.
- Bij constatering van storingen en/of andere onregelmatigheden aan computers of het net-

werk, inbreuken op beveiliging etc. dient de gebruiker dit terstond aan de netwerkbeheerder of ICT-er van de school te melden.

Het is verboden voor een gebruiker om:

- Zelf software te installeren zonder toestemming van de netwerkbeheerder/ICT-er op school;
- Niet geautoriseerde apparatuur aan te sluiten op het computernetwerk;
- Virussen te maken en/of te verspreiden. Hoewel het hele netwerk uiteraard is beveiligd d.m.v. anti-virusprogrammatuur en firewalls, is de kans aanwezig dat een flexibel ingezet werkstation (b.v. een laptop) , niet is voorzien van de laatste updates. In dat geval is het verplicht om eerst het antivirusprogramma te updaten en dan pas gebruik te maken van een in te pluggen gegevensdrager (b.v. usb-stick), om zo het netwerk niet te vervuilen met virussen, die b.v. van thuis zijn “meegenomen”;
- Het computernetwerk te gebruiken om toegang te krijgen tot gegevens die niet voor de gebruiker bestemd zijn, dan wel ander strafbaar gedrag. Dit geldt in de regel ook voor beheerders van het netwerk, ICT-ers op school, of anderen die als beheerder mogen inloggen;
- Opgeslagen bestanden op mobiele gegevensdragers (usb-sticks) die privacygevoelige informatie bevatten, onbeheerd achter te laten, of niet goed genoeg te beschermen tegen verlies of diefstal;
- Storingen of andere onregelmatigheden aan de computers of het netwerk zelf te verhelpen;
- Of op andere wijze te handelen, in strijd met het doel van deze gedragscode.

NB: het gebruik van memorysticks/usb-sticks wordt uit oogpunt van veiligheid afgeraden (i.v.m. verlies/diefstal en eventuele virusoverdracht). Alle data op het netwerk worden bij Unilogic opgeslagen en veilig geback-upt. Deze data en Outlook zijn benaderbaar via het extern bureaublad. Gebruikers worden aangeraden om het extern bureaublad te gebruiken zodat op een andere locatie veilig gewerkt kan worden.

4. Gebruik van Internet

- Gebruikers mogen via het netwerk van Kindante gebruik maken van internet in het kader van de functie-uitoefening of onderwijsactiviteit;
- Medewerkers mogen incidenteel en kortstondig internet gebruiken voor persoonlijke doeleinden, mits dit geen storende onderbreking vormt van de werkzaamheden;
- Het is verboden om auteursrechtelijk beschermde afbeeldingen (gedownload van internet) te verspreiden via bv websites, in nieuwsbrieven of e-mails. Bij schending van auteursrechten is er kans op een boete;
- Het is voor gebruikers verboden middels het netwerk van Kindante internet te gebruiken om:
    - ✓ Te winkelen voor een niet zakelijk doel
    - ✓ Te gokken of deel te nemen aan kansspelen
    - ✓ Niet zakelijke nieuwsgroepen of chatboxen te bezoeken
    - ✓ Websites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten en/of dit materiaal te bekijken of te downloaden
    - ✓ Aanstootgevende informatie waartoe men via internet toegang heeft verkregen zonder toestemming te downloaden, te veranderen, te verspreiden of te vernietigen
    - ✓ Afbeeldingen en videocommunities te bezoeken, die privé-materiaal van wereldburgers publiceert (b.v. You-Tube)
    - ✓ Te mailen met e-mailaccounts anders dan het account van Kindante (Hotmail, Gmail,

@Home etc.) en/of het Skype mailadres te gebruiken
- ✓ Social Media te gebruiken (zoals b.v. Twitter, Facebook, Instagram)

tenzij een van de bovengenoemde zaken een educatief doel dient, of rechtstreeks voortvloeit uit werkzaamheden, die met de functie op school te maken hebben, dan wel met permissie van de direct leidinggevende in kwestie.

5. Gebruik van e-mail

- Iedere medewerker van Kindante kan beschikken over een persoonlijk e-mailadres (leerlingen evt. vanaf groep 5) , om e-mails te ontvangen en te versturen;
- Volwassen gebruikers mogen incidenteel en kortstondig het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mail mits dit geen onderbreking vormt van de werkzaamheden;
- Het versturen van e-mail moet te allen tijde voldoen aan de volgende voorwaarden: correct taalgebruik en een correcte vermelding van de afzender, een duidelijke en ter zake doende inhoud en een eventueel meegestuurde bijlage met een maximale omvang van 3 MB;
- Het is voor gebruikers in ieder geval verboden middels het netwerk van Kindante de e-mailfaciliteit te gebruiken om:
  - ✓ Berichten anoniem of onder een fictieve naam te versturen;
  - ✓ Dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende berichten te versturen. Indien een gebruiker ongevraagd informatie van deze aard krijgt aangeboden, dient dit te worden gemeld aan de netwerkbeheerder, ICT-er op school of aan de directie van de school;
  - ✓ Kettingmailberichten te versturen;
  - ✓ Niet-zakelijke privé-berichten, publicaties/rondschrijven, nieuwsbrieven, reclame, power points e.d. (evt. van buiten de organisatie) te versturen;
  - ✓ Iemand elektronisch lastig te vallen (de ontvanger wenst van de verzender geen mail te ontvangen);
  - ✓ Op andere wijze te handelen in strijd met het doel van deze gedragscode.
- De gebruiker is verplicht zijn e-mailbox regelmatig op te schonen, door niet relevante e-mails met evt. bijlagen te verwijderen uit “postvak-in”, “verzonden items” en “verwijderde items”, teneinde de schijf/opslagcapaciteit niet te overbelasten. Met de intrede van digitale fotografie en de scanfaciliteit van onze multifunctionals neemt het aantal bestanden, ook in mailboxen, soms extreem toe. Het is de verantwoordelijkheid van iedere gebruiker van het Kindantenetwerk, om zo effectief mogelijk om te gaan met de beschikbare schijfruimte.

6. Het gebruik van vaste telefoon

- Medewerkers van Kindante mogen telefoons van Kindante gebruiken in het kader van functie-uitoefening;
- Medewerkers mogen incidenteel en kortstondig de telefoon gebruiken voor het voeren van privégesprekken als daar uit noodzaak aanleiding toe is, mits dit geen storende onderbreking vormt van de werkzaamheden;
- Het is in ieder geval voor gebruikers verboden telefoons van Kindante te gebruiken om:
  - ✓ Service- en amusementsnummers te bellen die beginnen met 0906 en 0909, tenzij dit gebeurt vanuit een schoolse aangelegenheid;
  - ✓ Internationale nummers te bellen voor privédoeleinden.

7. Gebruik van zakelijk ter beschikking gestelde mobiele telefoon (GSM) c.q. abonnement

- De zakelijk ter beschikking gestelde mobiele telefoon c.q. het abonnement wordt ingezet, of beschikbaar gesteld, om de mobiele bereikbaarheid van een medewerker te realiseren en dient overwegend voor inkomende telefoongesprekken en berichten;
- Iedereen die een zakelijke mobiele telefoon c.q. het abonnement gebruikt, dient terughoudend om te gaan met het voeren van uitgaande telefoongesprekken en berichten via de mobiele telefoon, tenzij dat uit hoofde van de functie noodzakelijk is;
- Bij uitgaande gesprekken en berichten dient dan ook het urgente zakelijke karakter voorop te staan en geniet het gebruik van een vaste (VoIP) telefoon altijd de voorkeur;
- Het is een medewerker toegestaan om een ter beschikking gestelde mobiele telefoon c.q. het abonnement te gebruiken om te telefoneren of te smssen, te pingen, WhatsApp te gebruiken, te fotograferen, te filmen, geluidsfragmenten op te nemen, of te surfen op internet, als daar werk gerelateerd behoefte aan is;
- De kosten van het gebruik van een mobiele telefoon van Kindante in het buitenland worden bij de gebruiker in rekening gebracht, tenzij er sprake is van een aantoonbare dienstreis en de kosten voortkomen uit zakelijke gesprekken.

8. Gebruik van mobiele telefoons door leerlingen of ouders

- A. Een mobiele telefoon van een leerling mag onder schooltijd niet gebruikt worden, tenzij dit een onderwijskundig doel dient en geautoriseerd is door de directie van school;
- B. Het niet gebruiken van een mobiele telefoon impliceert dus ook het verbod op opnemen van geluidsfragmenten, het nemen van foto's of het maken van video-opnames binnen school (ook voor ouders!), tenzij daarvoor toestemming is gegeven door de directie;
- C. Zijn er al met toestemming bestanden zoals genoemd in 8B gemaakt, dan is het publiceren van deze bestanden middels internet of e-mail ten strengste verboden, tenzij daar door alle personen, voorkomend op die bestanden, toestemming voor is verleend.

9. Monitoring VoIP – telefoonverkeer

- A. Monitoring van telefoongebruik vindt slechts plaats in het kader van de doelstelling van de gedragscode, zoals in de inleiding verwoord;
- B. Het genereren van gegevens uit de VoIP - centrale vindt in beginsel plaats op het niveau van de Kindanteorganisatie en wordt een-op-een gecommuniceerd op schoolniveau; praktisch gezien, worden de gegenereerde gegevens automatisch, per mail, Pdf-formaat doorgezet naar de betreffende directie van een VoIP school met een maandelijkse frequentie;
- C. De gegenereerde gegevens van VoIP verschaffen inzicht in verkeersgegevens, nooit op inhoud;
- D. Met verkeersgegevens wordt bedoeld: per toestelnummer kan inzichtelijk worden gemaakt: het aantal uitgaande gesprekken en totale gespreksduur per toestel per maand;
- E. Ontvangen gesprekken op een toestelnummer zijn niet te monitoren;
- F. De directies, waarvan de scholen zijn aangesloten op het (VoIP) telefoonnetwerk, ontvangen maandelijks de gegenereerde gegevens zoals genoemd onder D).Het betreft hier een

overzicht van het aantal gevoerde gesprekken per toestel in de schoolorganisatie en de totale gespreksduur; pas bij verdenking van zwaar misbruik, b.v. zeer hoge belkosten of extreem veel telefoonverkeer, kan er op verzoek een overzicht worden gegenereerd waarop niet alleen het aantal gesprekken per toestel wordt getoond, maar ook de nummers waar naartoe werd gebeld.

10. Monitoring e-mailverkeer

- Monitoring van e-mailverkeer vindt slechts plaats in het kader van de doelstelling van de gedragscode, zoals in de inleiding verwoord;
- De netwerkbeheerder/ICT-er op school kan de postbusgroottes van gebruikers in gebruikersstatistieken genereren, om tijdig te kunnen sturen op de capaciteit van schijfruimte;
- Bij de monitoring van e-mail, gaat het over aantallen mails in postvak-in, verzonden items en verwijderde items, of de totale bestandsgrootte van genoemde boxen, nooit over de inhoud;
- Indien de postbus van een gebruiker de maximale grootte overschrijdt, zal de ICT-er op school, in overleg met de gebruiker trachten de postbus op te schonen, opdat de inhoud van de postbus kan worden teruggebracht naar de toegestane omvang;
- De postbusgrootte kan afhankelijk van de functies van medewerker worden aangepast;
- E-mails met attachments, die voor meerdere personen in een organisatie tegelijk worden verstuurd geldt: het attachment, een bestand, wordt in het netwerk maar 1 keer centraal opgeslagen, om overvolle dataschijven en mappen van gebruikers te voorkomen; het geniet te allen tijde de voorkeur, om bestanden van deze aard te delen op de dataschijf , dan wel op Intranet-omgeving (Boekenkast Afas).

11. Monitoring van internetverkeer

- Monitoring van internetverkeer vindt slechts plaats in het kader van de doelstelling van de gedragscode, door Unilogic Networks, zoals in de inleiding verwoord;
- Internetverkeer wordt uit oogpunt van overdrachtssnelheden continu gemonitord door de netwerkbeheerder Unilogic Networks, in het kader van performance-checks;
- Misbruik van internet kan getraceerd worden als een werkstation in het gehele Kindantenetwerk zorg draagt voor een red alert, dat veroorzaakt wordt door enorm datatransport tussen het netwerkstation en het World Wide Web. Dergelijk misbruik wordt in eerste instantie opgemerkt door Unilogic Networks en gecommuniceerd met de senior adviseur onderwijs/ICT van de stichting, die dit oppakt met de leidinggevende van de desbetreffende Kindantelocatie;
- Bij de monitoring van misbruik van internet, kan worden nagegaan welke gebruiker wanneer op welk netwerkstation van Kindante, welke website bezoekt of heeft bezocht.

12. Mobiele telefonie, e-mailverkeer en internetgedrag, werk-gerelateerd in de privé situatie

Het is vandaag de dag heel gewoon dat werknemers “telewerken”. Hiermee wordt bedoeld dat vanuit de privé-situatie ingelogd kan worden op het netwerk t.b.v. mail en/of het bewerken van bestanden. Bovendien worden steeds meer webapplicaties gebruikt (b.v. Esis, website van school, Intranet). Ook hier gelden de gedragsregels, zoals in deze gedragscode genoemd m.b.t. inhoud, het algemeen gebruik en omgang met inloggegevens zoals gebruikersnaam en wachtwoorden.
Met klem worden alle gebruikers van het netwerk van Kindante erop geattendeerd, om juist in de thuissituatie of op een andere werkplek buiten school of kantoor zeer voorzichtig om te gaan met inloggegevens en wachtwoorden en nooit de p.c. of laptop onbeheerd achter te laten zonder uit te

loggen. Denk hierbij aan uw eigen privacygevoelige informatie, die van Kindante en/of die van medewerkers, kinderen en ouders. Ook hier geldt het advies om wachtwoorden iedere drie maanden te veranderen.

13. Richtlijnen voor het gebruik van Social Media

Social media zijn niet meer weg te denken uit de manier waarop we vandaag de dag communiceren. Social media zijn zeer geschikt om in te zetten voor communicatie met de verschillende doelgroepen waar we mee werken. Van belang is te beseffen dat je met berichten op social media (onbewust) de goede naam van een school of Kindante en betrokkenen ook kunt schaden. Om deze reden verwacht Kindante dat alle medewerkers bewust met social media omgaan. In dit document staan de belangrijkste richtlijnen voor het gebruik van social media genoemd.

- De school zorgt ook digitaal voor een veilig klimaat en communiceert met medewerkers, leerlingen en ouders hoe zij dit doet.
- Stem vooraf af of de pagina openbaar wordt of enkel bestemd is voor een besloten groep.
- Bedenk dat bij een openbare pagina, geplaatste berichten (en foto's) door alle volgers gedeeld kunnen worden en dus openbaar worden en zichtbaar voor iedereen.
- Check voor het plaatsen van foto's en/of namen van leerlingen en medewerkers of zij hier toestemming voor hebben gegeven.
- Plaats bij de foto's geen namen. Niemand wordt dan in verlegenheid gebracht door de foto's.
- De school deelt kennis en andere waardevolle informatie, zoals nieuwe ontwikkelingen binnen school of Kindante.
- Let op het taalgebruik: vermijd taalfouten, onduidelijke zinnen of woorden. o Realiseer dat internetberichten blijvend zijn.
- Indien negatieve berichten of reacties op de social media-pagina van de school worden geschreven: geef er niet impulsief een reactie op. Ga er met de betrokkenen over in een persoonlijk gesprek. o De school behoudt het recht om ongepaste reacties (bijvoorbeeld ongepast taalgebruik) te verwijderen.
- Negatieve reacties worden niet uit de weg gegaan, als ze maar opbouwend bedoeld zijn.
- Deel geen vertrouwelijke informatie over de school of over Kindante.
- Schrijf nooit een negatief bericht of reactie over een andere school, organisatie of over medewerkers/leerlingen/ouders/partners.
- Schrijf geen negatieve berichten/oordelen over de school, Kindante of bijvoorbeeld wetsvoorstellen.
- Zet geen persoonlijke berichten (bijvoorbeeld over je familie of vrienden) op de social mediapagina van de school.
- Reageer niet vanuit de schoolpagina op berichten van vrienden. Houd werk en privé gescheiden! o Maak geen gebruik van de mogelijkheid 'pagina promoten'; dit kost geld!

Social media hebben soms als gevolg dat er een grijs gebied ontstaat tussen je persoonlijke leven en werk. Uitgangspunt is dat professionals zelf weten hoe zij hiermee verstandig omgaan.
Hoofdregel: het gedrag van medewerkers op social media wijkt niet af van wat in de klas of op school gebruikelijk is. Kindante respecteert de vrijheid van meningsuiting van haar medewerkers, maar herinnert je eraan dat je als medewerker een voorbeeldfunctie hebt en altijd ambassadeur van Kindante bent. Je mag werk gerelateerde onderwerpen publiceren mits het geen vertrouwelijke informatie over Kindante betreft. De publicatie mag Kindante niet schaden. Bij twijfel niet publiceren, of ga in overleg met je leidinggevende of de communicatieadviseur.

Laat als ambassadeur van Kindante en van de school vooral de goede, positieve kanten van je werk zien via social media.
Indien je negatieve of positieve berichten over een school van Kindante of Kindante signaleert, stuur deze dan naar de communicatieadviseur Maud Golsteyn (m.golsteyn@kindante.nl) en je leidinggevende. Vermijd de verleiding om impulsief te reageren (bijvoorbeeld omdat je emotioneel betrokken bent). Stem bij twijfel altijd af met de communicatieadviseur en je leidinggevende.

Je bent op de hoogte dat publicaties op social media altijd vindbaar zijn en vaak vindbaar blijven.
Bij onderwijsinhoudelijke onderwerpen maak je duidelijk dat je op persoonlijke titel publiceert.

Plaats, deel of like nooit vertrouwelijke informatie over de school of over Kindante op social media.
Plaats, deel of like geen berichten die tegenstrijdig zijn met beleid van de school of van Kindante, of berichten die schadelijk kunnen zijn voor de school of Kindante.

Ben voorzichtig in de digitale omgang met leerlingen en ouders op social media.
Plaats geen foto's/ informatie van/over leerlingen op je eigen social media.
Ga niet in discussie met een leerling of ouder op social media. In het geval dat een discussie dreigt te ontsporen, neem dan direct contact op met de leidinggevende om de te volgen strategie te bepalen.

Als je LinkedIn-, Twitter-, Instagram- of Facebookpagina openbaar is, kan je toekomstig werkgever deze bekijken. Sterker nog, volgens het College Bescherming Persoonsgegevens (CBP) hebben werkgevers daar alle recht toe aangezien de informatie via social media en Google openbaar is. Gebruik maken van deze informatie in het gesprek zonder dat te vermelden is niet netjes, maar mogelijk.

Houd rekening met het wettelijk vastgelegde auteurs-, beeld- en citaatrecht. Het is verboden om zonder toestemming van de maker andermans werk te publiceren. Schending van deze wet levert je een boete op van honderden euro's.

Kindante mag een medewerker aanspreken als zijn of haar uitingen op social media niet geoorloofd of gepast zijn. Bij grove schendingen van de code kan tevens een gesteld disfunctioneren of ontslag onderbouwd worden.

Bijlage 9: 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 reunies.

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;

bijlage 10: voorbeeldbrief informatie aan ouders over IBP

Logo school

Beste Ouder(s), verzorgers,

Ongetwijfeld heeft u de laatste tijd in alle media vernomen, dat de veiligheid van data een heel actueel onderwerp is. Helaas niet altijd vanuit een succesvolle gebeurtenis, maar eerder naar aanleiding van lekken van informatie of ongevraagd delen van privacygevoelige informatie aan derden. Middels deze brief willen wij u informeren, over hoe ons bestuur en onze school omgaat met privacygevoelige informatie.

Vanaf vorig schooljaar zijn we bezig met het implementeren van Informatiebeveiliging en Privacy (IBP) volgens de richtlijnen van de Algemene Verordening Privacy (AVG). Ons bestuur heeft voor alle medewerkers en kinderen volgens landelijk beleid richtlijnen, procedures en protocollen opgesteld, zodat Uw gegevens en de gegevens van Uw kind(eren) goed beveiligd en volgens regels worden verwerkt.

Het verzamelen van privacygevoelige gegevens gebeurt ten allen tijde alleen vanuit de grondslag, dat de school dient te administreren. De gegevens zijn opgeslagen in administratiesoftware en/of in het computernetwerk en zijn alleen voor de ogen beschikbaar gemaakt van collega's die deze gegevens nodig hebben voor hun dagelijks werk. Uiteraard zijn deze omgevingen beveiligd middels wachtwoorden en beveiligde verbindingen.

Daarnaast wisselen we gegevens uit met de overheid (verplicht vanwege financiering), met partners alleen indien strikt noodzakelijk (zorgverlening, logopedie, huisarts) en geanonimiseerd met uitgevers van educatieve software. Hierbij wordt in acht genomen, dat alleen die gegevens worden uitgewisseld die relevant zijn, vanuit beveiligde omgevingen en liggen er getekende verwerkersovereenkomsten aan ten grondslag.
Ook is er binnen ons bestuur een meldpunt datalekken (b.v. iemands iPad is gestolen, of laptop uit de auto ontvreemd) om samen een oplossing te zoeken en eventuele betrokkenen informeert, mocht er privacygevoelige informatie zijn gelekt.

Daarnaast zijn er tal van afspraken en gedragsregels, die vanuit het bewustzijn van privacy belangrijk zijn. We noemen er een paar:

- We gebruiken foto's van uw kind(eren) alleen als u daarvoor toestemming heeft gegeven
- Niemand kan zomaar foto's gaan maken op school en die delen met anderen
- Na werktijd ligt er geen privacygevoelige informatie op bureaus
- Nergens hangen lijsten met namen, adressen of telefoonnummers
- Locken we computerschermen bij het verlaten van de werkplek
- Hebben we geen papieren lijstjes met wachtwoorden
- Dat wat we op papier bewaren (evt. dossiers) ligt veilig achter slot en grendel
- We gebruiken geen USB-sticks

We hopen U zo voldoende geïnformeerd te hebben en u kunt het vastgestelde beleid rondom bescherming van privacy altijd op school of via onze website inzien. Omgaan met privacygevoelige gegevens is mensenwerk en vereist continue aandacht. Wij respecteren uw feedback.

Vriendelijke groet,

Directie en Team XXXX

Protocol ESIS rollen en rechten Kindante

Versiebeheer

VERSIE	Auteur	Status	Datum
Versie 1.0	Ed Toussaint Claudia de Rooij	definitief	16 april 2018

Dit protocol is gemaakt om de geldende AVG wetgeving toe te passen binnen de Kindante ESIS administratie en zal als addendum worden toegevoegd aan het vigerende beleid. In ESIS worden zeer privacygevoelige gegevens genoteerd: adresgegevens en BSNrs van leerlingen, toetsresultaten en dossiergegevens zoals diagnoses en verslagen van gesprekken en gegevens van de ouders. Daarnaast staan er ook adresgegevens in van de medewerkers.
Het doel van dit document is te beschrijven wie welke rechten standaard mag krijgen binnen ESIS en wie deze rechten mag aanvragen. Uitzonderingen op deze regels moeten volgens onze stichting kunnen worden gemaakt, met opgaaf van beargumenteerde redenen.

Wie deelt rechten uit?

Het aanmaken van inloggegevens en het toekennen van rollen in ESIS wordt voor de gehele stichting alleen gedaan door de applicatiebeheerder, domein ICT van het BURO.

Wie mag gebruikers en rollen aanvragen?

Het aanvragen van een nieuwe gebruiker of aanvullende rollen mag op een school alleen worden gedaan door de directeur, de managementassistent of de ICT-er. Wordt het verzoek door iemand anders gedaan, dan zal de applicatiebeheerder de aanvraag verifiëren bij één van de genoemde personen van de betreffende school.

Standaardrechten

Op een school worden deze standaardrechten uitgedeeld:

Functie	**Rol in ESIS**
Directeur	Directie
Interne begeleider	Interne begeleider
ICT-er	Applicatie beheerder
Leerkracht	Groepsleerkracht
Managementassistent	Administrateur
Conciërge	Conciërge

Bij andere functies wordt kritisch bekeken welke rechten strikt noodzakelijk zijn.
Toelichting meest gebruikte rollen:

Rol	**Rechten**
Directie	Leerlingadministratie: alleen lezen voor alle groepen Leerlingdossier: volledige toegang voor alle groepen Medewerkermodule: volledige toegang
Interne begeleider	Leerlingadministratie: alleen lezen voor alle groepen Leerlingdossier: volledige toegang voor alle groepen Medewerkermodule: geen toegang
Applicatie beheerder	Leerlingadministratie: volledige toegang voor alle groepen Leerlingdossier: volledige toegang voor alle groepen Medewerkermodule: volledige toegang
Groepsleerkracht	Leerlingadministratie: alleen lezen voor toegewezen groepen Leerlingdossier: volledige toegang voor toegewezen groepen Medewerkermodule: geen toegang
Administrateur	Leerlingadministratie: volledige toegang voor alle groepen Leerlingdossier: volledige toegang voor alle groepen Medewerkermodule: volledige toegang
Conciërge	Leerlingadministratie: alleen lezen naw gegevens leerlingen+ouders Leerlingdossier: geen toegang Medewerkermodule: geen toegang

Toelichting:
Voor de managementassistenten (Rol: administrateur) liggen de hoofdwerkzaamheden bij het beheren van de leerlingadministratie. Het komt echter steeds vaker voor dat deze persoon gevraagd wordt om extra werkzaamheden te doen in ESIS waarvoor toegang nodig is tot het leerlingdossier. Alle directies zijn geïnformeerd op 3 april 2018 en akkoord gegaan met het feit dat alle managementassistenten ook toegang hebben tot de leerlingdossiers.
Voor de ICT-ers op school (Rol: applicatie beheerder) liggen de hoofdwerkzaamheden bij het ondersteunen van hun collega's. Zij hoeven in feite niks te kunnen wijzigen in de leerlingadministratie en het leerlingdossier, maar om hun collega's goed van dienst te kunnen zijn is het toch noodzakelijk dat zijn deze toegang hebben. Alle directies zijn geïnformeerd op 3 april 2018 en akkoord gegaan met het feit dat alle ICT-ers toegang hebben tot de leerlingadministratie en de leerlingdossiers.

Standaardprocedure

De procedure om een nieuwe medewerker toegang te geven tot ESIS:

1. De nieuwe medewerker moet eerst een Windows account hebben met emailadres, dit wordt door de ICT-er aangemaakt op school of aangevraagd bij Unilogic (dit mag de directeur uiteraard ook doen). Dit emailadres is nodig omdat het in ESIS moet worden geregistreerd om het wachtwoord naartoe te sturen.
2. Iemand op school (meestal de managementassistent) voert de persoon in als Medewerker in ESIS en koppelt hem/haar aan de juiste groep(en) wanneer van toepassing.
3. Deze persoon (meestal de managementassistent) geeft dan aan de applicatiebeheerder op het BURO door dat er een nieuwe medewerker is ingevoerd met het verzoek een Gebruiker aan te maken voor de medewerker. Daarbij moet worden vermeld welke functie de persoon heeft zodat de juiste rol kan worden gegeven.
4. De applicatiebeheerder maakt de Gebruiker aan, daarna stuurt ESIS een automatische email naar de medewerker in kwestie met inloggegevens. Als een medewerker wisselt van school, dan wordt het account door de applicatiebeheerder verhuist en volgt er geen email. De medewerker kan dan met zijn/haar bestaande wachtwoord inloggen of via de inlogsite een nieuw wachtwoord opvragen.
5. De applicatiebeheerder koppelt aan de aanvrager terug dat de Gebruiker is aangemaakt of verhuist.

Uitzonderingen

Wij zijn als stichting van mening dat uitzonderingen op bovenstaande moeten kunnen worden gemaakt als het takenpakket van een medewerker (tijdelijk) wordt uitgebreid en hij/zij toegang moet hebben tot bepaalde gegevens hiervoor. Ten eerste zijn er veel directeuren die extra rollen hebben. De directeur heeft de eerste verantwoordelijkheid over de gegevens van de leerlingen op zijn/haar school en moet dan ook toegang kunnen krijgen tot alle gegevens. Deze eventuele extra rechten gaan wij dan ook niet documenteren.
Daarnaast komt het voor dat bv een leerkracht een extra taak krijgt binnen de school waardoor hij/zij meerdere groepen moet kunnen zien. In deze gevallen kijken we kritisch naar welke rechten de medewerker dan zou moeten krijgen en vragen wij om argumentatie en de periode waarin de persoon meer rechten moet hebben. Het is de gezamenlijke verantwoordelijkheid van de school en de applicatiebeheerder van het BURO om in de gaten te houden wanner de rechten weer moeten worden afgenomen.

Verwijderen van Gebruikers

Het is de verantwoordelijkheid van de school om bij de applicatiebeheerder van het BURO door te geven wanneer medewerkers de school verlaten. Dit is noodzakelijk want ook al verwijdert de school een leerkracht van de groep, de medewerker kan dan nog steeds inloggen en overzichten uitdraaien waarin privacygevoelige informatie kan staan.

Controle

Wanneer iemand tijdelijke uitbreiding heeft gehad van rechten dan zal de applicatiebeheerder na de aangegeven periode contact opnemen met de school om na te gaan of de extra rechten verwijderd kunnen worden. Ook zal de applicatiebeheerder steekproefsgewijs nog eens extra scholen controleren op alle gebruikers, zodat mensen die er niet meer werken ook uit het systeem worden verwijderd.

Vervangers

Bij een langdurige vervanging is het altijd aan te bevelen om de persoon een eigen inlog te geven in ESIS. Ga aub geen accounts met wachtwoorden uitlenen.
Voor een korte vervanging moet je de vraag stellen of deze persoon voor de korte aanwezigheid toegang moet hebben tot ESIS. De meest gehoorde opmerking mbt vervanging is dat de persoon in Basispoort moet kunnen werken. Dat is te ondervangen door alleen in de Medewerker-module een ‘vervanger’ aan te maken en die aan alle groepen te koppelen (dit kan worden gedaan door de managementassistent). Er moet wel een bestaand emailadres aan gekoppeld zijn zodat de vervanger ook in Basispoort kan inloggen. Het is dan niet nodig om ook daadwerkelijk een Gebruiker (inlog) is ESIS te maken voor de vervanger. De vervanger kan dus op deze manier wél in Basispoort werken, maar níet in ESIS.
Het is niet de bedoeling om een vervangers-account (Gebruiker) in ESIS te maken die toegang heeft tot alle groepen. De vervanger zou dan alles van alle leerlingen kunnen zien, dat is uiteraard absoluut onwenselijk! Zou je toch graag een ‘vervanger’-account willen gebruiken in ESIS dan moet je deze alleen koppelen aan de groep waarin de vervanger werkt (en dus weer aanpassen bij een volgende vervanging) en moet na vertrek van de vervanger direct het wachtwoord worden veranderd.

Rollen en rechten op het BURO

Op het bestuursbureau (BURO) van Kindante hebben ook enkele medewerkers toegang tot ESIS:

- De applicatiebeheerder heeft een Supervisor-rol op alle scholen en op bestuursniveau. Dit is nodig omdat de applicatiebeheerder alle inlogaccounts van ESIS beheert en fungeert als vraagbaak/ 1^{e} lijns helpdesk voor de scholen. Het is daarom van belang dat de applicatiebeheerder alles kan zien zodat problemen en vragen snel kunnen worden opgepakt en opgelost.
- Afdeling Onderwijs heeft ook 2 medewerkers die dezelfde rechten hebben als de applicatiebeheerder. In hun functie is het van belang dat zij op ieder tijdstip een doorsnede kunnen maken van bv tussenopbrengsten. Zij begeleiden scholen regelmatig naar een hoger niveau van functioneren en ESIS speelt daarbij een belangrijke rol.
- Afdeling Financiën heeft op alle school de rol Financiën. Deze rol heeft alleen maar rechten om Telformulieren te produceren. Daarop staan alleen maar aantallen leerlingen, zij hebben geen toegang tot privacy-gevoelige informatie.