HANDBOEK-BELEIDSPLAN

INFORMATIEBEVELIGING EN PRIVACY

Instemming GMR	21-03-2019
Vastgesteld CVB	21-03-2019

Dit handboek treedt in werking op 21 maart 2019

Inhoudsopgave

Inleiding

Informatie en ICT zijn noodzakelijk in de uitvoering van het onderwijs. Doordat we met persoonsgegevens van medewerkers, leerlingen en anderen werken, is privacywetgeving daarop van toepassing. Deze wetgeving bepaalt niet alleen onder welke voorwaarden persoonsgegevens gebruikt mogen worden, maar geeft ook aan dat er passende technische en organisatorische maatregelen op het gebied van informatiebeveiliging en privacy (afgekort: IBP) genomen moeten worden om persoonsgegevens te beschermen. Hiervoor is er binnen De Vivente groep een IBP-handboek opgesteld. In dit handboek wordt het IBP-beleid van De Vivente-groep verwoordt. Dit plan is op te vragen bij het stafkantoor.

Dit IBP-handboek is opgesteld in samenwerking met Privacy op School, Het Greijdanus, de Oosthoek en Florion.

In het IBP-handboek staan richtlijnen, procedures, afspraken en praktische handreikingen die nodig zijn om informatiebeveiliging en privacy goed te regelen. Deze maatregelen nemen we niet alleen omdat de wet dit voorschrijft, maar ook op basis van de normen en waarden die wij vanuit onze visie op onderwijs met elkaar delen en uitdragen:

De Vivente-groep positioneert zich als de aanbieder van toegankelijk Christelijk onderwijs Het belang van hoogwaardig onderwijs aan kinderen staat voorop. Onderwijs waarin talenten worden ontplooid met als doel kinderen voor te bereiden op een wereld waarin kennis, veerkracht en competenties als samenwerken en het verwerken van informatie de basis zijn.

Het handboek is onderverdeeld in twee delen voor afzonderlijke doelgroepen:

Deel A - Alle medewerkers

Dit deel bevat de algemene informatie die voor alle medewerkers van De Vivente-groep van belang is. Van alle medewerkers wordt verwacht dat zij op de hoogte zijn van de afspraken die hierin vermeld staan en hier ook naar handelen. In dit deel wordt o.a. antwoord gegeven op de volgende vragen:

- Welke afspraken gelden er voor mij als het gaat om de verwerking van leerlinggegevens?
- Waar moet ik mij aan houden bij het gebruik van sociale media?
- Welke gegevens bewaart de school van mij en anderen en waarom?
- Waar moet ik op letten bij het gebruik van beeldmateriaal en online diensten?
- Waar moet ik op letten bij het uitwisselen van gegevens met andere partijen?
- Als ik gegevens kwijt ben of ik heb een vermoeden van misbruik, bij wie moet ik dan zijn?
- Waar moet ik persoonsgegevens of persoonlijke informatie opslaan?

Deel B – Schoolleiders en leidinggevenden

In dit deel is informatie terug te vinden die vooral van belang is voor de schoolleider: hoe zorg ik ervoor dat het IBP-beleid op mijn school goed geregeld is? In dit deel wordt o.a. antwoord gegeven op de volgende vragen:

- Wat moet ik met ouders regelen rondom privacy?
- Welke afspraken moet ik maken met mijn medewerkers in het kader van privacy?
- Wat moet ik afspreken met medewerkers in het kader van geheimhouding?
- Wat moet ik weten over datalekken?
- Wat moet ik weten over cameratoezicht?
- Wat moet ik weten als het gaat om het verlenen van toegang tot persoonsgegevens?
- Hoe lang moet ik persoonsgegevens bewaren?
- Welke afspraken maak ik over devices die in bruikleen worden gegeven?
- Wat moet ik weten over externe partijen die namens de school persoonsgegevens verwerken?
- Welke rollen en verantwoordelijkheden t.a.v. IBP zijn er binnen de schoolorganisatie belegd?
- Welke technische maatregelen moet ik geregeld hebben binnen de school?
- Hoe kan ik aantonen dat ik IBP op orde heb?

DEEL A INFORMATIE VOOR ALLE MEDEWERKERS

Inhoudsopgave

Gedragsregels Privacy

Voor een veilig schoolklimaat is het belangrijk dat de afspraken rondom informatiebeveiliging en privacy door alle werknemers worden nageleefd en uitgedragen. Daarom is er een gedragscode opgesteld waaraan alle medewerkers zich dienen te houden.

De afspraken zijn verdeeld in drie onderdelen:

A. Waar en hoe bewaar ik leerlinggegevens?
B. Hoe houd ik indringers op afstand?
C. Regels rondom het delen, mailen, internetgebruik en sociale media

Hieronder volgen per onderdeel de afspraken.

A. Leerlinggegevens

1. **Verwerk leerling gegevens zoveel mogelijk digitaal.**
   Leerlinggegevens worden zoveel mogelijk digitaal opgeslagen, geraadpleegd en bewerkt in ParnasSys. Dit geldt ook voor gegevens die via ouders/verzorgers en/of externen worden ontvangen. Bewaar geen gegevens op een USB-stick. Gedownloade bestanden dienen verwijderd te worden van de computer. Als je bestanden opslaat in downloads worden deze automatisch na 1 dag verwijderd.
   Gegevens die op papier aangeleverd worden, worden gescand en aan ParnasSys toegevoegd. Vergeet niet om de scan van je eigen computer te verwijderen en de in gescande papieren versies te vernietigen.

2. **Formuleer gegevens die je vastlegt over een persoon zorgvuldig en professioneel.** Ouders hebben het recht om het dossier in te zien. Zorg ervoor dat de gegevens op een zakelijk schrijfwijze, zonder emotie zijn geformuleerd.

3. **Gebruik voor de verwerking van leerlinggegevens bij voorkeur een computer van school.**
   Moet je leerlinggegevens downloaden en bewerken op een computer? Doe dit alleen op een beveiligde computer (die voorzien is van encryptie of versleuteling), bij voorkeur een computer van school. Mocht je thuis werken verwijder de bestanden dan na gebruik van jouw computer. Zorg ervoor dat anderen (bijv. familieleden) niet bij jouw werkbestanden kunnen komen.

4. **Ga na welke afspraken er binnen de school gemaakt zijn voordat je gegevens uitwisselt met derden.**
   Wanneer je gegevens uit wil wisselen met externen, zoals bijvoorbeeld de logopedist, een arts, jeugdzorg of een schoolbegeleidingsdienst dan is het nodig om toestemming te vragen van ouders. Zorg dat je de toestemming registreert en houdt daarbij ook rekening met de verdeling van het ouderlijk gezag. Voor de uitwisseling van gegevens met het samenwerkingsverband of

een andere school gelden aparte afspraken. Hiervoor kun je terecht bij je IB-er. Hij/zij is op de hoogte van wat is afgesproken.

5. **Vraag toestemming aan derden (ouders, hulpverleners etc.) wanneer je voornemens bent de door hen aangeleverde informatie (zowel geschreven als mondeling) op te slaan in het leerlingdossier.**
   Dit betreft andere informatie dan de onderwijskundige informatie die benodigd is voor het verzorgen van onderwijs.

B. Hoe houd ik indringers op afstand?

1. **Zorg er bij vertrouwelijke (telefonische) gesprekken voor dat er niet kan worden meegeluisterd.**
   Trek je je even terug als een gesprek een vertrouwelijk karakter heeft of krijgt.

2. **Bewaar laptops of tablets altijd op een veilige plek, zeker tijdens vakantieperiodes.**
   Het is een open deur, maar toch gebeurt het heel erg makkelijk. Maak elkaar er dus op attent als je een laptop of tablet onbeheerd ziet liggen. Als je computer gestolen wordt, heeft dat gevolgen voor de school en de leerling.

3. **Controleer e-mail.**
   Klik alleen op linkjes en open alleen bijlagen in e-mails van betrouwbare afzenders en pas op met het downloaden van bestanden.
   Virussen kunnen makkelijk worden binnengehaald via (phishing)mails. In het criminele circuit is dit een veelgebruikte methode om aan jouw gegevens te komen. Ook kunnen de gegevens op je computer versleuteld worden (ransomware).

4. **Meld je altijd af - mits de situatie dit toelaat - als je de computer onbeheerd achterlaat. En zorg ervoor dat er op je werkplek geen gevoelige informatie zichtbaar of voor het grijpen ligt, ook bij de printer.**
   Met de combinatie van de Windows- en L-toets kun je je makkelijk afmelden. Maak er een gewoonte van om papieren op je bureau om te draaien. Zo voorkom je dat anderen informatie zien die niet voor hen is bedoeld.

5. **Zet je digibord op freeze als je wachtwoorden intoetst of persoonsgegevens in je scherm ziet staan. En zorg dat niemand meekijkt als jij je wachtwoord intoetst.**
   Het digibord kan je op freeze zetten met behulp van de afstandsbediening. Voordat je het weet zien leerlingen gevoelige gegevens of kunnen ze aan de hand van je afgekeken gebruikersnaam en wachtwoord proberen in te loggen.
   Zet ook de notificatie-functie van je e-mail uit, zodat er tijdens je les geen meldingen op het bord binnen komen die leerlingen kunnen zien, maar niet voor hun ogen bestemd zijn.

6. **Laat je wachtwoorden van het leerlingadministratiesysteem of andere systemen met persoonsgegevens niet onthouden door je internetbrowser. En schrijf je logingegevens nooit op.** Zonder dat je er erg in hebt, klik je de optie 'wachtwoord onthouden' in je browser aan. Heel makkelijk als je vaak moet inloggen, maar iemand anders kan dan dus ook inloggen. Een sterk wachtwoord kan je maken door een wachtwoordzin te gebruiken. (BV Jan loopt binnen bij Vivente!) Wachtwoordzinnen zijn heel moeilijk te kraken.

7. **Houd je logingegevens altijd voor jezelf, ook al vragen anderen aan je om ze te delen.** Je login is in feite een sleutel om toegang te krijgen tot de informatie die voor jou toegankelijk moet zijn. Daarnaast herkent het systeem jou door je login, zodat het kan bijhouden wie welke gegevens heeft toegevoegd of gewijzigd.

C: Regels rondom het delen, mailen, internetgebruik en sociale media

1. **Maak gebruik van een link naar ParnasSys of Office 365 om leerlinggegevens uit te wisselen met collega's.**
   Verstuur leerlinggegevens liever niet per mail, maar verstuur een link met de vindplaats van de benodigde gegevens.

2. **Vraag ouders om toestemming om een (privé)account aan te maken voor online diensten.** Leerlingen moeten toestemming hebben van hun ouders/verzorgers om een (privé)account aan te maken voor online diensten zoals Pinterest, Canva, Google etc.

3. **Deel over individuele leerlingen nooit informatie via social media.**
   Doe dit vooral in persoon of desnoods via de telefoon. Wat je communiceert via social media kan makkelijk anders worden geïnterpreteerd door de lezer als je hier niet alert op bent.

4. **Gebruik de accounts die door de school worden beheerd als je met ouders of leerlingen wil communiceren via e-mail of social media.**
   Formuleer je boodschap ook hier professioneel en zorgvuldig, in correcte taal.

5. **Zet e-mailadressen altijd in de BCC-regel als je naar (grote) groepen mensen een bericht verstuurt.**
   Zo blijven de e-mailadressen van de groepsleden afgeschermd.

6. **Stuur nooit een e-mailbericht door naar derden zonder de degene van wie je het bericht ontvangen hebt hierover te informeren.**

7. **Wanneer je een bericht stuurt met belangrijke en/of gevoelige informatie naar (een groep) ouders/verzorgers laat dit dan nalezen door een collega.**

   Een foutje is snel gemaakt en bovendien kan een ander kan je boodschap anders interpreteren dan jij hem bedoeld hebt. Het is dan fijn als er iemand met je meeleest voordat je hem verstuurt.

8. **Zakelijk gebruik e-mail en internet**

   Het internet en e-mailsysteem wordt voor zakelijk gebruik beschikbaar gesteld. Gebruik is derhalve verbonden aan taken die voortvloeien uit de functie. Beperkt persoonlijk gebruik van het internet en e-mailsysteem is evenwel toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden en dit geen verboden gebruik oplevert.

9. **Tegengaan van seksuele intimidatie**

   Via e-mail kan eenvoudig seksuele intimidatie worden gepleegd. Zowel de inhoud van het bericht als de bijlagen kunnen seksueel intimiderend zijn. De Vivente-groep kan inkomende berichten onderwerpen aan een geautomatiseerde controle.

Protocol social media

Niet meer weg te denken uit het dagelijks leven is het gebruik van sociale media. Sociale media is een verzamelnaam voor alle internet-toepassingen waarmee het mogelijk is om informatie met elkaar te delen op een gebruiksvriendelijke en 'vaak' leuke wijze. Het bevat niet alleen informatie in de vorm van tekst, maar ook beeld en geluid worden gedeeld. Bekende voorbeelden van sociale media zijn Facebook, YouTube, LinkedIn, WhatsApp, Snapchat en Twitter.

Net als bij de opkomst van e-mail en internet ontstaan er ook nu vragen bij het gebruik van sociale media in organisaties. Privé-gerelateerde en werkgerelateerde zaken zijn niet zo gemakkelijk te scheiden. Om verschillende denkbeelden over het gebruik van sociale media niet te laten leiden tot misverstanden zijn deze richtlijnen ontwikkeld.

Sociale media biedt de mogelijkheid te laten zien dat je trots bent op elkaar en op de school. En tegelijkertijd kunnen ze een bijdrage leveren aan een positief beeld van de school. Aan de andere kant kunnen berichten op sociale media (soms onbewust) leerlingen, personeelsleden en de goede naam van de school schaden. Daarom vragen de scholen van De Vivente-groep alle leerlingen, ouders en personeelsleden om verantwoord met sociale media om te gaan:

- Op sociale media ga je op een sociale manier met elkaar om, dus met respect.
- Op sociale media praat je wel MET elkaar en niet OVER een ander, net als in andere gesprekssituaties.
- Op sociale media praat je alleen namens jezelf; niet namens of onder de naam van anderen. (De medewerkers die sociale media gebruiken namens de school, hebben hiervoor toestemming gekregen).
- Je zet alleen berichten op sociale media als die de ander of de school niet schaden.
- Sociale media gebruik je als leerling in de les alleen als je daarvoor toestemming hebt gekregen en dus als het nuttig is voor de les die je volgt.
- Wil je via sociale media foto's, filmpjes en/of geluidsfragmenten delen waar anderen ook op staan, dan mag dat alleen als die anderen daartegen geen bezwaar hebben.
- Heb je iets in vertrouwen gehoord over een ander of iets dat een ander kan schaden, dan deel je dat niet met anderen via sociale media.
- Heb je een klacht of kritiek op de school of iemand die betrokken is bij school, dan maken we de vraag of klacht niet via sociale media bekend, maar leggen we het (persoonlijk) neer bij de aangewezen persoon in kwestie.
- We accepteren niet dat sociale media gebruikt wordt om anderen te pesten, te kwetsen, te stalken, te bedreigen, zwart te maken of op een andere manier te beschadigen.
- Als je je niet aan deze normale fatsoensnormen houdt, worden er op school maatregelen genomen.
- Als je met jouw gebruik van sociale media strafrechtelijk de fout ingaat, kunnen de school en/of andere beschadigde personen hiervan aangifte doen bij de politie.

Meldingen over berichten die in strijd zijn met de afspraken hierboven, kunnen verstuurd worden naar het emailadres van de desbetreffende school. De school onderneemt in alle gevallen actie op gedane meldingen.

Internetgebruik door leerlingen

Om alle leerlingen zo veilig mogelijk om te laten gaan met het internet hebben we een aantal afspraken hierover op papier gezet die met de leerlingen worden besproken die gebruik maken van het internet en mogelijk sociale media.

1. Ik mag alleen gaan surfen op het internet of sociale media gebruiken als ik toestemming van mijn juf of meester heb.
2. Ik zoek alleen naar informatie die ik nodig heb voor een spreekbeurt, werkstuk of een project.
3. Bij het gebruik van een zoekmachine gebruik ik normale zoektermen.
4. Pop-ups en andere reclame klik ik weg.
5. Ik geef nooit persoonlijke gegevens als mijn naam, adres, telefoonnummer of emailadres door. Ook gegevens (of foto's) van anderen mag ik niet doorgeven.
6. Ik ga meteen naar mijn juf of meester als ik op internet vervelende informatie tegenkom.
7. Ik zal nooit iemand die ik op internet ben tegengekomen, toestemming geven mij in het echt te ontmoeten.
8. Ik zal 'internet personen' geen foto's toesturen zonder toestemming van juf of meester.
9. Ik ga niet reageren op vervelende e-mailberichten of andere meldingen. Het is immers niet mijn schuld dat sommige mensen zich niet weten te gedragen. Ik waarschuw gelijk de juf of meester.
10. Chatten, foto's plaatsen en downloaden van bestanden is niet toegestaan. Bij twijfel overleg ik met mijn juf of meester.
11. Printen doe ik alleen met toestemming van de juf of meester.

- Social media en internet zijn een bron van informatie; gebruik het als het je helpt bij het leren.
- We gedragen ons op sociale media en op het internet netjes.
- We zijn respectvol naar de ander.
- We denken na voordat we informatie delen.
- Maak je foto's of opnames om die te publiceren? Vraag toestemming aan de ander

Privacyreglement

Het privacyreglement maakt duidelijk (transparant) aan de personen van wie gegevens worden verzameld (ook wel betrokkenen genoemd) waarvoor de verzamelde gegevens nodig zijn en welke gegevens dit zijn (doel en doelbinding uit de vuistregels).

Ook is hierin te lezen wie binnen de school toegang heeft tot deze gegevens, hoe de gegevens zijn beveiligd en met wie ze uitgewisseld mogen worden.

Het reglement is in te zien via de website www.vivente.nu Het reglement is ook als bijlage A toegevoegd bij dit handboek.

Ouders worden via het inschrijfformulier en via de website van de scholen gewezen op het privacyreglement.

Toestemming

Beeldmateriaal

Ouders, moeten altijd toestemming geven voor het gebruik van hun beeldmateriaal of die van hun kinderen. Die toestemming moet specifiek zijn. Dat betekent dat het voor ouders en medewerkers duidelijk moet zijn voor welk gebruik van het beeldmateriaal ze toestemming geven. Bijvoorbeeld voor het gebruik op de website, in een nieuwsbrief of de schoolgids. Ouders moeten ook de mogelijkheid hebben deze toestemming weer in te trekken.

De school moet een veilige omgeving zijn voor alle kinderen (en hun ouders) en zij moeten niet het risico lopen ongewenst gefotografeerd te worden.
Daarom wordt, voorafgaand aan activiteiten, aan ouders gevraagd om terughoudend te zijn met het maken van foto's en video's en is het niet toegestaan om foto- of video-opnames die gemaakt zijn op school te delen via sociale media of te gebruiken voor commerciële doeleinden.

Wanneer er activiteiten georganiseerd worden, zijn er vaak ouders die foto's of video's maken (bijvoorbeeld bij feestelijke gelegenheden) We maken hierbij onderscheid tussen twee situaties:

- Ouders in algemene zin op het terrein van De Vivente-groep, bijvoorbeeld op het schoolplein. Als je ouders hier foto's of video's ziet maken, spreek ze hier dan op aan en wijs ze op de privacy van (andere) leerlingen. Echter is dit niet helemaal tegen te gaan en is er een grote mate van eigen verantwoordelijkheid van de ouders.
- Ouders die meegaan op schoolactiviteiten. Dit vereist duidelijke afspraken over het maken van beeldmateriaal. Zorg dat ouders alleen foto's en video's maken van kinderen wiens ouders hiervoor specifiek toestemming hebben gegeven.

Het maken van foto's of video-opnamen van een leerling door (een medewerker van) De Vivente groep geschiedt altijd op basis van toestemming van ouders/voogden. Bij de inschrijving van een leerling wordt hier toestemming voor gevraagd. Elk jaar worden de ouders gewezen op het feit dat zij hun toestemming ook weer mogen intrekken.

Het is op de Vivente-groep scholen gebruikelijk dat er tijdens de lessen video-opnamen worden gemaakt. Deze opnamen zijn bestemd om het lesgeven van de groepsleerkracht te verbeteren deze opnames worden alleen binnen De Vivente-groep scholen gebruikt.

Stagiares moeten voor hun opleiding soms ook video opnamesmaken. Staan op deze video opnames leerlingen herkenbaar in beeld dan moet hiervoor aan de betreffende ouders toestemming worden gevraagd.

Af en toe worden er foto's video-opnamen gemaakt die gebruikt kunnen worden als voorlichtingsmateriaal. Als een kind hierop te zien is, kunnen deze opnamen alleen met toestemming van de ouder(s)/voogd(en) als zodanig worden gebruikt.

Online diensten

Voor het gebruik van online diensten door leerlingen binnen of buiten de school moeten ouders ook toestemming verlenen. Dit betekent dat wanneer leerlingen in de klas gebruik willen maken van een eigen privéaccount voor bijvoorbeeld Whatsapp of Pinterest, ouders hier vooraf toestemming voor moeten geven. Dit betreft alleen online diensten die ook buiten de school om in het maatschappelijk verkeer gebruikt kunnen worden, dus niet voor e-mail, digitale leeromgevingen of leermiddelen waarvoor door de school zelf een account wordt verstrekt.

Eisen mobiele devices

De mobiele devices in eigendom van de medewerker en kan gebruikt worden voor schoolwerkzaamheden indien ze voorzien zijn van de volgende beveiligingseisen, zodat persoonsgegevens goed beschermd zijn.

- Het device is voorzien van een wachtwoord of code
- Het device is voorzien van anti-virussoftware (laptop) en de laatste updates(mobiele telefoon).
- E-mail en andere apps of online toepassingen van De Vivente groep moeten afgeschermd worden met een apart wachtwoord
- E-mail en andere apps of online toepassingen mogen niet toegankelijk zijn voor andere gebruikers
- Wachtwoorden mogen niet onthouden worden in de browser
- Er worden geen bestanden lokaal opgeslagen, maar alleen op de daarvoor aangewezen bewaarplaatsen van De Vivente groep
- Er worden geen leerlinggegevens op devices verwerkt die gebruikt worden in openbare netwerken

Uitwisseling persoonsgegevens

Wanneer je gegevens uit wil wisselen met externen, zoals bijvoorbeeld de logopedist, schoolarts, jeugdzorg of een schoolbegeleidingsdienst dan is het nodig om toestemming te vragen van ouders. Zorg dat je de toestemming registreert in ParnasSys en houd daarbij ook rekening met de verdeling van het ouderlijk gezag. Voor de uitwisseling van leerlinggegevens met het samenwerkingsverband of een andere school gelden aparte afspraken. Kijk hieronder in de tabel met welke partijen je gegevens mag uitwisselen en op welke manier.

Leerlingen

Verstrekking aan	Doel	Uitwisseling toegestaan	Wijze waarop	Toestemming nodig?
Dienst Uitvoering Onderwijs	Bekostiging*	Ja	Koppeling ParnasSys	Nee
Educatieve uitgeverijen en Basispoort	Gebruik digitale leermiddelen	Ja	Koppeling ParnasSys	Nee (wel verwerkersovereenkomst)
Educatieve Apps	Onderwijs	Ja	Handmatige invoer	Ja, als ze ook na de schoolloopbaan gebruikt kunnen blijven worden door de leerlingen.
Basisscholen of scholen voor voortgezet onderwijs	Overdracht leerlingdossier (na aanmelding)*	Ja	Koppeling OSO	Nee (wel inzage)
Externe Onderwijsspecialisten	Zorgbegeleiding van een leerling	Ja	Verstrekken account	Ja
Stagiaires	Opleiden	Ja	Verstrekken account	Nee
Samenwerkingsverband	Toelaatbaarheidsverklaring afgeven*	Ja, zie ook: https://passendonderwijsenprivacy.nl	n.t.b.	Nee
TSO	Tussenschoolse opvang	Ja	n.t.b.	Ja
Oudervereniging/ouderraad	Innen ouderbijdrage	Ja	n.t.b.	Ja
GGD/JGZ	Bezoek schoolarts	Nee	n.v.t.	n.v.t.

Inspectie van het onderwijs	Toezicht*	Ja	Via Internet School Dossier (ISD)	Nee
Leerplicht Gemeente	Controle verzuim	Ja	Verzuimloket	Nee

* Wettelijk verplicht

Datalekken

Zijn er leerlinggegevens verloren gegaan? Is je laptop gestolen? Heb je last van een virus waardoor je niet meer bij je bestanden kunt? Of vertrouw je iets niet? Dan ben je verplicht dit zo snel mogelijk te melden via de schoolleider in verband met de meldplicht datalekken.

We spreken van een datalek wanneer er mogelijk persoonsgegevens (van leerlingen, hun ouders of medewerkers) in handen kunnen vallen van derden die geen toegang tot die gegevens mogen hebben of wanneer er persoonsgegevens onbedoeld verloren zijn gegaan.

Voorbeelden van datalekken zijn:

- een e-mail die aan een verkeerd persoon geadresseerd is
- een kwijtgeraakte USB-stick met persoonsgegevens
- inloggegevens die openbaar zijn geworden
- een gestolen iPad
- een gehackte computer

Het bevoegd gezag van de school is verantwoordelijk voor de bescherming van persoonsgegevens van leerlingen en personeel en moet bepalen of er een melding gedaan moet worden bij de Autoriteit Persoonsgegevens. Wanneer er een datalek ten onrechte niet wordt gemeld, kan een hoge boete opgelegd worden.

Ben je dus (een device met) persoonsgegevens kwijtgeraakt of heb je onrechtmatigheden geconstateerd met betrekking tot de toegang tot persoonsgegevens? Meld dit dan direct bij je leidinggevende en/of via avg@vivente.nu

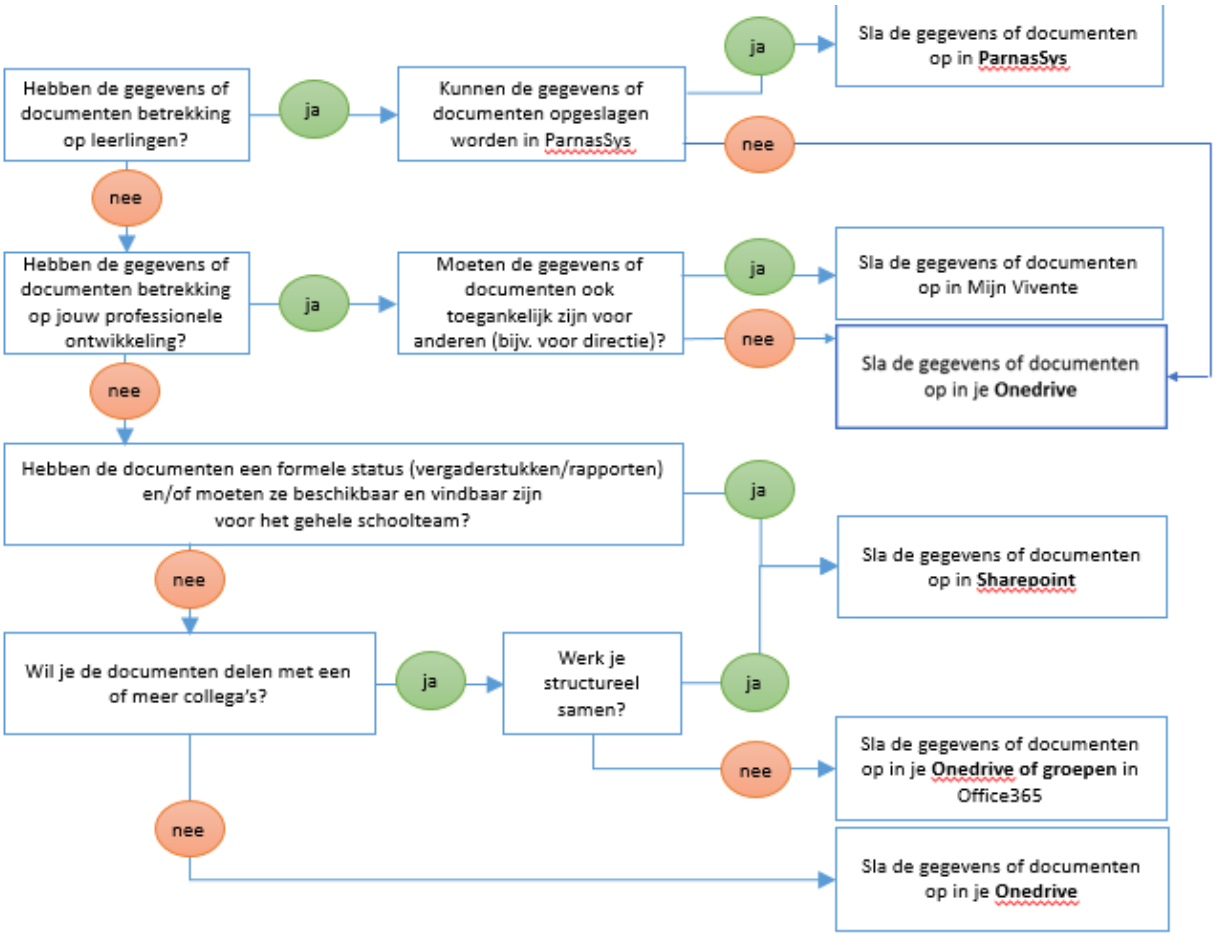
Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens door de Functionaris Gegevensbescherming.

In bijlage E is de volledige procedure melden datalekken opgenomen.

Document- en datamanagement

Om ervoor te zorgen dat we binnen de school onze documenten en gegevens (data) overzichtelijk en veilig opgeslagen hebben, zijn er afspraken over wat we waar bewaren. Op deze manier zijn documenten eenvoudiger terug te vinden, maar kunnen ze ook beter afgeschermd en geback-upt worden.

In het schema hieronder kun je nagaan op welke plek je gegevens en documenten op moet slaan.



DEEL B INFORMATIE VOOR SCHOOLLEIDERS EN LEIDINGGEVEDEN

Inhoudsopgave

Privacyreglement

Ouders hebben het recht om te weten welke gegevens er van hen en van hun kinderen worden verzameld door de school en voor welke doeleinden deze gegevens verzameld worden. Met het privacyreglement voldoet het bestuur van de Vivente-groep aan zijn wettelijke informatieplicht, mits deze ook actief wordt aangeboden aan de ouders[1]. Daarom is het voor scholen belangrijk om het privacyreglement met ouders te communiceren.

In bijlage B en bijlage C is een tekst opgenomen die door alle scholen van De Vivente groep gebruikt wordt om ouders via de website en de schoolgids te wijzen op het privacyreglement van de school. Het kan in sommige gevallen nodig zijn om deze tekst uit te breiden indien er op school aanvullende bijzondere persoonsgegevens verwerkt worden. Ouders kunnen het reglement ook opvragen bij de directie van de school.

Indien er sprake is van een situatie van echtscheiding, hanteert De Vivente- groep het protocol 'gescheiden ouders', waarin de onderdelen uit de wetgeving zijn weergegeven.

Toestemming

Voor het gebruik van foto- en filmopnames van leerlingen en medewerkers is schriftelijke toestemming vereist. Het handigste is om de toestemming voor het gebruik van foto-en filmopnames direct bij de inschrijving van een leerling of indiensttreding van een werknemer te regelen.
Om dit voor leerlingen te regelen is binnen De Vivente groep een voorbeeld van een toestemmingsformulier beschikbaar gesteld. De tekst is te vinden in bijlage D. Hierop geven ouders aan of zij toestemming geven voor het gebruik van beeldmateriaal en voor welke doeleinden.
Als schoolleider is het belangrijk om ouders jaarlijks te herinneren (bijvoorbeeld via de nieuwsbrief en in de schoolgids) dat deze toestemming herroepen of alsnog verleend kan worden. Dit betekent ook dat wanneer toestemming wordt ingetrokken, het materiaal van het betreffende medium moet worden verwijderd.

Wanneer je (of een medewerker) gegevens uit wil wisselen met externen, zoals bijvoorbeeld de logopedist, een schoolarts, jeugdzorg of een schoolbegeleidingsdienst dan is het nodig om toestemming te vragen van ouders. Zorg dat de toestemming geregistreerd wordt in ParnasSys en houd daarbij ook rekening met de verdeling van het ouderlijk gezag.

[1] Ouders kan desgewenst ook gelezen worden als verzorgers.

Protocol melden datalekken

Op 1 januari 2016 is de Wet meldplicht datalekken ingevoerd. Door deze meldplicht zijn ook scholen verplicht melding te maken van ernstige datalekken bij de Autoriteit Persoonsgegevens. Het nalaten van deze melding kan leiden tot een hoge financiële boete.

De meldplicht is alleen van toepassing wanneer persoonsgegevens worden verwerkt. Bijvoorbeeld in de leerlingadministratie of digitale leermiddelen. Als de school gebruik maakt van leveranciers, zoals uitgevers of distributeurs, die persoonsgegevens ontvangen van de school, dan moet de school met deze bewerkers aanvullende afspraken maken in de verwerkersovereenkomsten over het melden van datalekken.

Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, óf waarbij het niet valt uit te sluiten dat persoonsgegevens verloren zijn gegaan. Er is persoonlijke informatie 'gelekt'. Een klassiek voorbeeld van een datalek is een hack waarbij een database met persoonsgegevens is gestolen. Maar het verliezen van een usb-stick met daarop de adresgegevens van klas 3b, is ook een datalek.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het schoolbestuur. Een leverancier is een bewerker voor de school. Binnen de Vivente-groep is afgesproken dat de Functionaris gegevensbescherming van de Vivente-groep verantwoordelijk is voor de melding.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens. Het is dus belangrijk dat u zo spoedig mogelijk (4 uur) contact opneemt met de FG.

De volledige procedure datalekken is te vinden in bijlage E.

Toegangsbeleid

Niet alle medewerkers hebben toegang nodig tot (alle) leerlinggegevens. Per rol is vastgesteld welke gegevens kunnen worden ingezien en gewijzigd, waarbij is gekeken wat die rol nodig heeft aan gegevens om zijn of haar werkzaamheden uit te kunnen voeren. Gegevens die daarbij niet noodzakelijk zijn, kan die rol dan ook niet inzien of wijzigen.

Uitgangspunten

- Gegevens van leerlingen en medewerkers worden opgeslagen in de daarvoor aangewezen bewaarplaatsen (zie onderdeel Document- en datamanagement).
- De afspraken met betrekking tot toegang tot en het verwerken van persoonsgegevens door de verschillende rollen binnen De Vivente-groep staan hieronder beschreven in een zogenaamde autorisatiematrix.
- Alle accounts die worden verstrekt dienen te voldoen aan deze autorisatiematrix.
- De directeur van de school is verantwoordelijk voor het verstrekken van de juiste toegang (lees: accounts met de juiste rollen en rechten in ParnasSys/Afas/Mijn Vivente/Basispoort). De directeur ziet er ook op toe dat de accounts worden ingetrokken na het beëindigen van een arbeids- of samenwerkingscontract of het wijzigen van functies. Daarnaast worden de accounts van systemen met persoonsgegevens periodiek gecontroleerd.
- Naast het toepassen van de autorisatiematrix worden de volgende beveiligingsmaatregelen toegepast op systemen waarin persoonsgegevens worden gebruikt:
- Inloggegevens worden via het e-mailadres van De Vivente groep verstrekt aan de medewerker en nooit gedeeld met anderen.
- Inloggegevens worden periodiek (minstens 1x per jaar) vernieuwd.
- Er wordt technisch afgedwongen (waar mogelijk) om sterke wachtwoorden te gebruiken.

Bewaartermijnen

Vanuit de privacywetgeving zijn er geen concrete bewaartermijnen voor persoonsgegevens vastgesteld. Wel dient de organisatie hiervoor richtlijnen te hebben. Hierbij is het van belang om na te gaan hoe lang de gegevens nodig zijn voor het doel waarvoor deze zijn verzameld. In andere wetten zijn in sommige gevallen wel bewaartermijnen opgenomen waaraan organisaties zich moeten houden.

De Vivente groep hanteert mede op basis hiervan de bewaartermijnen voor persoonsgegevens zoals hieronder aangegeven.

Wanneer de bewaartermijn verstreken is moeten de betreffende gegevens vernietigd worden.

Gegevens	**Maximale wettelijke bewaartermijn**
Gegevens over verzuim en afwezigheid.	Maximaal 5 jaar nadat een leerling is uitgeschreven.
Gegevens in- en uitschrijving (noodzakelijk voor berekening van bekostiging)	Maximaal 5 jaar nadat een leerling is uitgeschreven.
Gegevens die nodig zijn om te berekenen hoeveel bekostiging de school krijgt.	Minimaal 7 jaar na afloop van het schooljaar waarop de bekostiging betrekking heeft.
Gegevens in het leerlingdossier.	Maximaal 2 jaar nadat een leerling is uitgeschreven en 3 jaar als er sprake is van een verwijzing naar het speciaal onderwijs.
Gegevens met betrekking tot bezwaar-, klachten- of gerechtelijke procedure.	Maximaal 5 jaar nadat leerling is uitgeschreven.
Camerabeelden t.b.v. toezicht.	Maximaal 4 weken, tenzij er een incident is vastgelegd.

Gegevens in personeelsdossier met betrekking tot fiscale bewaarplicht.	Maximaal 5 jaar na uitdiensttreding
Overige gegevens in het personeelsdossier.	Maximaal 2 jaar na uitdiensttreding
Gegevens over het gebruik van ICT-middelen en het schoolnetwerk door personeel en leerlingen.	Maximaal 6 maanden na uitdienstreding
Sollicitatiebrief, formulier, correspondentie omtrent de sollicitatie, getuigschriften, verklaring omtrent gedrag, psychologisch onderzoek.	Maximaal 4 weken zonder toestemming, maximaal 1 jaar met toestemming van de sollicitant, maximaal 2 jaar na uitdiensttreding van benoemde collega.

Afspraken over mobiele devices in bruikleen

De school leent afhankelijk van de functie of aard van de werkzaamheden mobiele devices uit aan haar medewerkers. Dit kan gaan om een smartphone, tablet of een laptop. De devices zijn voorzien van beveiliging, zodat gegevens goed beschermd zijn. De devices zijn naast anti-virus o.a. voorzien van back-up functionaliteit, encryptie en worden na inname weer opgeschoond.

Aanvullend hierop wil de school nog een aantal afspraken schriftelijk vastleggen over het gebruik van het device wanneer deze in bruikleen wordt gegeven aan een medewerker. Deze afspraken zijn vastgelegd in bijlage F van dit handboek.

Verwerkersovereenkomsten

In de privacywetgeving is bepaald dat het schoolbestuur als Gegevensverantwoordelijke afspraken moet maken met alle leveranciers van de school die leerlinggegevens verwerken in zogenaamde Verwerkersovereenkomsten. Het gaat hierbij bijvoorbeeld om uitgevers van digitaal lesmateriaal, leveranciers van toetsen, onderwijsadviesdiensten, etc.

Een uitzondering hierop vormt de uitwisseling van gegevens met de overheid (DUO) in het kader van bekostiging of toezicht of het Samenwerkingsverband in het kader van passend onderwijs.

De verwerkersovereenkomsten worden waar mogelijk bovenschools afgesloten. Hiervoor is in 2018 een inventarisatie gedaan van de lopende contracten van de scholen binnen De Vivente groep.

Wanneer een school een contract afsluit met een nieuwe leverancier zal er een nieuwe verwerkersovereenkomst gesloten moeten worden. Deze contracten worden boven schools afgesloten.

Wanneer het gaat om een leverancier die alleen een contract heeft met een individuele school, is de school zelf verantwoordelijk voor het afsluiten van de verwerkers-overeenkomst. Wanneer het een contract met meerdere scholen betreft, dan wordt dit bovenschools geregeld. De school dient in alle gevallen afstemming te zoeken met de Functionaris Gegevensbescherming (l.r.zegers@goon.nl)

Voor het afsluiten van verwerkersovereenkomsten wordt gebruik gemaakt van de meest actuele model verwerkersovereenkomst, die te vinden is via: https://www.privacyconvenant.nl
De Vivente-groep gaat niet akkoord met het beperken van de aansprakelijkheid door een leverancier.

Via het stafkantoor is een overzicht op te vragen van de leveranciers waar het bestuur op dit moment een verwerkersovereenkomst mee heeft. Ook voor vragen over het afsluiten van verwerkersovereenkomsten of het doorgeven hiervan, kan men terecht bij de Functionaris Gegevensbescherming.

Vragen of klachten over privacy

Het is belangrijk om klachten of vragen over privacy serieus te nemen. Om deze goed te beantwoorden is het nodig om kennis en expertise te hebben op het gebied van privacy.

Vandaar dat we binnen de Vivente-groep hier een centraal punt voor in hebben gericht.

Wettelijk hebben de personen (betrokkenen) van wie De Vivente groep persoonsgegevens verzamelen bepaalde rechten. Deze rechten zijn:

- **Inzage en overdracht** – een kopie van alle gegevens die over die persoon zijn verzameld.
- **Rectificatie** – als blijkt dat de gegevens die zijn verzameld onjuist of onvolledig zijn, dan heeft die persoon het recht om deze gegevens te laten aanvullen of corrigeren.
- **Wissen** – het is verplicht om gegevens te wissen als de persoon die om inzage heeft gevraagd dit vraagt. Dit is niet altijd het geval, soms heeft de school bijvoorbeeld een wettelijke plicht om bepaalde informatie te verwerken en kan zij dit niet zomaar verwijderen. Dit zal per geval moeten worden bekeken.

Als een medewerker inzage wil in de gegevens die over de medewerker zijn verzameld of je krijgt de vraag van een leerling of een ouder, dan kan dat op de volgende manier.

- Als **medewerker** kan je jouw vraag om inzage stellen aan: pz@vivente.nu
- Een leerling of ouder die jou deze vraagt stelt, kan je doorverwijzen naar: de schoolleider
- Er geldt een reactietermijn van 1 maand (met gegronde redenen kan je deze reactietermijn verlengen met nog 2 maanden)

Rollen en verantwoordelijkheden

Binnen het vaststellen en uitvoeren van het IBP-beleid zijn verschillende rollen en verantwoordelijkheden vastgesteld binnen De Vivente groep.

Dit handboek is bedoeld om praktische uitvoering te geven aan het IBP-beleid van de Vivente-groep, met name ten aanzien van de organisatorische maatregelen. Voor de technische maatregelen voor informatiebeveiliging en privacy dienen afzonderlijke plannen opgesteld te worden.

Onderwerp	Verantwoordelijk voor	Rol/functie
Privacyreglement	Vaststellen	Bestuurder en GMR
	Communicatie met ouders/medewerkers	Directeur
Gebruik beeldmateriaal en online diensten	Toestemming vragen aan ouders en registreren	Directeur
Uitwisseling persoonsgegevens	Bepalen met welke partijen persoonsgegevens uitgewisseld mogen worden en op welke wijze.	Directeur
	Toestemming vragen aan ouders en registreren	Directeur
IBP-handboek	Vaststellen	Bestuurder en GMR
	Bewustwording en toezien op toepassing gedragscode	Directeur
	Toepassen afgesproken regels in het IBP-handboek	Medewerkers
	Opstellen en toepassen protocol voor leerlingen	Directeur
Document- en datamanagement	Toepassen van technische beveiligingsmaatregelen (backup, encryptie, etc.)	Bovenschoolse ICT-er/externe onderwijsleveranciers
	Vaststellen bewaarplaatsen	Directeur
	Vaststellen bewaartermijnen	Bestuurder
	Vernietiging persoonsgegevens conform bewaartermijnen	Directeur
Toegangsbeleid	Verstrekken en intrekken accounts conform autorisatiematrixen	Directeur en bestuurder (voor staf)
	Toepassen technische beveiligingsmaatregelen (o.a.	Bovenschoolse ICT-er

	automatisch vernieuwen en sterkte wachtwoord)	
Verwerkersovereenkomsten	Doorgeven nieuwe verwerkers (leveranciers) aan Functionaris Gegevensbescherming	Directeur
	Afsluiten verwerkersovereenkomsten voor meerdere scholen	Bestuurder
	Afsluiten verwerkersovereenkomsten voor individuele scholen	Bestuurder
Datalekken	Protocol vaststellen	Bestuurder en GMR
	Datalekken doorgeven aan Meldpunt	Medewerkers (Ontdekkers)
	Verzamelen meldingen en benodigde informatie	Directeur (Meldpunt) i.o.m. FG
	Melden en registreren	FG
	Afweging maken tot melding Autoriteit Persoonsgegevens	FG i.o.m. Bestuurder
	Melding maken bij Autoriteit Persoonsgegevens	FG
Devices in bruikleen	Afsluiten gebruikersovereenkomst voor devices die in bruikleen worden gegeven.	Bestuurder
Handboek Privacy	Controle en toezicht op toepassing handboek	Bestuurder

Checklist beveiliging ICT

Fysieke beveiliging en continuïteit van ICT

- ☐ Persoonsgegevens worden uitsluitend verwerkt in een gesloten, fysiek beveiligde omgeving met bescherming tegen bedreigingen van buitenaf.
- ☐ Persoonsgegevens worden uitsluitend verwerkt op apparatuur waarbij maatregelen zijn genomen om de apparatuur fysiek te beveiligen en de continuïteit van de dienstverlening te verzekeren.
- ☐ Er worden periodiek back-ups gemaakt ten behoeve van de continuïteit van de dienstverlening. Deze back-ups worden vertrouwelijk behandeld, bewaard in een gesloten omgeving en na het verstrijken van de bewaartermijn vernietigd.
- ☐ De locaties waar gegevens worden verwerkt worden periodiek getest, onderhouden en periodiek beoordeeld op veiligheidsrisico's.

De netwerk-, server- en applicatiebeveiliging

- ☐ De netwerkomgeving waarbinnen gegevens worden verwerkt is strikt beveiligd. Daarbij worden verkeersstromen gescheiden en zijn maatregelen geïmplementeerd tegen misbruik en aanvallen.
- ☐ De omgeving waarbinnen persoonsgegevens worden verwerkt wordt gemonitord.
- ☐ Op systemen worden periodiek de laatste (beveiligings)patches en updates geïnstalleerd.
- ☐ Penetratietests en vulnerability assessments worden periodiek uitgevoerd.
- ☐ Niet (meer) gebruikte informatie wordt verwijderd.
- ☐ Op wachtwoorden worden cryptografische maatregelen toegepast om deze gegevens veilig op te slaan.
- ☐ Er wordt voor inlogprocessen gebruik gemaakt van versleutelde verbindingen. De uitwisseling van persoonsgegevens aan derden in opdracht van De Vivente groep vindt versleuteld plaats.

Netwerkcomponenten

- ☐ De netwerkcomponenten binnen de scholen van De Vivente groep hebben enkel tot doel dat er gebruik kan worden gemaakt van de digitale omgeving, internet, copiers en printers en WIFI. Alle wifi-punten worden automatisch geüpdatet.
- ☐ Alle netwerkpunten (switches en routers) worden geüpdatet indien nodig. Alle netwerkcomponenten die password protected ingesteld kunnen worden zijn beveiligd.

Controle en toezicht

Jaarlijks wordt onderstaande (niet uitputtende) controlelijst ingevuld door alle scholen om na te gaan of het handboek is geïmplementeerd. De resultaten worden gerapporteerd aan de bestuurder.

#	Maatregelen met betrekking tot privacy en informatiebeveiliging	Ja*/ Nee	Waaruit blijkt dit?
1	Het privacyreglement wordt door de school jaarlijks onder de aandacht gebracht van ouders en medewerkers.		
2	Voor de publicatie van foto- en filmbeelden en online diensten is door de school vooraf toestemming vastgelegd.		
3	Met alle leveranciers die namens de school persoonsgegevens verwerken is een verwerkersovereenkomst afgesloten.		
4	Voor de uitwisseling van persoonsgegevens met derden, niet zijnde verwerkers, is toestemming vastgelegd.		
5	Het protocol datalekken is bij de medewerkers bekend. Men weet wat er van hen verwacht wordt.		
6	Toegang tot software en systemen met persoonsgegevens op school worden verleend conform de vastgestelde toegangsmatrixen.		
7	De afspraken over de bewaarplaatsen van gegevens en informatie (Document- en datamanagement) worden nageleefd.		
8	Er wordt middels het IBP-handboek en het voorlichtingsmateriaal structureel en regelmatig aandacht besteed aan de zorgvuldige verwerking van persoonsgegevens. Dit betekent dat de medewerkers op de hoogte zijn van onze IBP-afspraken.		
9	Bij uitdiensttreding worden alle accounts ingetrokken en apparatuur ingenomen.		
10	Voor alle door de school uitgegeven apparatuur aan medewerkers zijn gebruikersovereenkomsten afgesloten.		
11	Fysieke ruimtes op school met persoonsgegevens van gevoelige aard (op papier of op de server) zijn beveiligd tegen onbevoegde toegang.		
12	Er wordt voldaan aan de checklist beveiliging ICT.		

BIJLAGEN

A. Privacyreglement Vivente-groep

Dit protocol beschrijft hoe binnen ons bestuur wordt omgegaan met de verwerkingen van persoonsgegevens en de beveiliging van de informatie.
Dit protocol is onderdeel van het IBP-handboek voor medewerkers. Hierin staan naast dit protocol praktische afspraken over onder andere gegevensopslag, omgang met sociale media en internet en toestemming voor beeldmateriaal van leerlingen.

Met dit document wordt voldaan aan de wettelijke informatieplicht conform **Algemene Verordening Gegevensbescherming** (AVG) die in 2018 is ingegaan.

Het is bedoeld als centrale informatiebron voor alle betrokkenen (leerlingen, hun ouders/verzorgers, personeelsleden, etc.) en beschrijft per categorie het type verwerkingen, waarom die worden uitgevoerd, welke persoonsgegevens worden verwerkt en aan wie die gegevens worden verstrekt.

Dit document wordt jaarlijks herzien.

1. Privacy van leerlingen en hun ouders

De Vivente-groep positioneert zich als de aanbieder van toegankelijk christelijk onderwijs Het belang van hoogwaardig onderwijs aan kinderen staat voorop. Onderwijs waarin talenten worden ontplooid met als doel kinderen voor te bereiden op een wereld waarin kennis, veerkracht en competenties als samenwerken en het verwerken van informatie de basis zijn.

Om deze doelstelling waar te maken is het van belang goed te weten wie deze leerling is, wat zijn of haar talenten en uitdagingen zijn en hoe het onderwijs voor deze leerling het beste kan worden verzorgd. Om hier een beeld van te krijgen worden persoonsgegevens van die leerling op school verzameld en bewaard. In dit hoofdstuk is te lezen om welke verzamelingen dit gaat, waarom die gegevens worden gebruikt, wie ze gebruikt en aan wie ze worden verstrekt.

1.1 Om welke gegevens gaat het?

Voor de begeleiding van de leerling tijdens zijn of haar schoolloopbaan worden gegevens verzameld om de leerling optimaal te laten functioneren, zowel wat betreft prestaties als welbevinden. Deze gegevens worden vastgelegd in een leerlingdossier.

Persoonsgegevens
De gegevens die worden verzameld en opgeslagen zijn:

- Naam, voornamen, geslacht, geboortedatum, geboorteland, nationaliteit, adresgegevens en soortgelijke voor communicatie benodigde gegevens van de leerling

- Administratienummer (o.a. BSN)
- Gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling
- Gegevens over de aard en het verloop van het onderwijs, alsmede de behaalde resultaten en gegevens over verlof en verzuim
- Gegevens over de organisatie van het onderwijs, zoals welke klas, vakken en dergelijke
- Zorggegevens die nodig zijn voor de organisatie van het onderwijs (recht op meer tijd, klasorganisatie, etc)
- Gegevens van psychosociale aard, zoals testrapporten, persoonlijkheidsonderzoeken, intelligentieonderzoeken en orthopedagogische onderzoeken
- Ontwikkelingsperspectiefplannen van de leerling
- Gespreksverslagen
- Verslaglegging van het multidisciplinair overleg (MDO)
- Gegevens nodig voor het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten
- Loggegevens over gebruik van de systemen

Deze gegevens worden zoveel mogelijk digitaal opgeslagen. Is dit technisch niet mogelijk dan worden de gegevens op papier bewaard.

1.2 Wat is het doel van de verzameling van deze gegevens?

Deze gegevens worden verzameld om:

- Overzicht te hebben van de leerlingen die onderwijs volgen
- Overzicht te hebben van de aard, organisatie en verloop van dat onderwijs per leerling en de behaalde studieresultaten
- Te communiceren met leerlingen en/of hun ouders/ verzorgers
- Persoonlijke (waaronder medische) omstandigheden van een leerling en de gevolgen daarvan voor het volgen van onderwijs bij te houden
- Financieel beheer uit te kunnen voeren
- Aan de wettelijke eisen rond monitoring en verantwoording naar toezichthoudende instanties en zorginstellingen te kunnen voldoen
- Toegang tot de systemen te krijgen dit in relatie tot het onderwijssysteem.
- De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het bewaken van de consistentie en betrouwbaarheid van de opgeslagen gegevens te verzorgen
- De continuïteit en goede werking van de systemen te waarborgen

1.3 Wie hebben toegang tot de leerlinggegevens en hoe worden deze beveiligd?

Binnen de school hebben de volgende type medewerkers toegang tot (een deel van) de gegevens:

- Leden van het CvB, de directie en het MT
- Onderwijzend personeel
- Onderwijsondersteunend personeel met lesgevende en/of behandeltaken.
- OOP zonder lesgevende en/of behandeltaken.

Niet alle rollen hebben tot alle gegevens toegang. Per rol is vastgesteld welke gegevens kunnen worden ingezien en gewijzigd. De aard van zijn of haar werkzaamheden is bepalend voor de toegang tot de gegevens. Gegevens die daarbij niet noodzakelijk zijn, kan die rol ook niet inzien of wijzigen.

Gegevens met betrekking tot administratie, inschrijving, onderwijsbegeleiding en zorg worden in ParnasSys opgeslagen. Voor ParnasSys is een toegangsbeleid opgesteld waarin is vastgelegd welke functies tot welke gegevens toegang mogen hebben. Dit beleid wordt jaarlijks gecontroleerd.
Daarnaast wordt van elke leerling een digitaal dossier bij gehouden. Indien er van een leerling een papieren dossier wordt bijgehouden bevindt dit dossier zich in een afgesloten ruimte/kast. Hiertoe hebben alleen medewerkers toegang die deze gegevens nodig hebben bij het uitvoeren van hun werkzaamheden.

In het IBP-handboek is een overzicht opgenomen van de verschillende functies en welke gegevens zij kunnen inzien en/of wijzigen.

Inloggen tot ParnasSys is alleen voorbehouden aan medewerkers die in dienst zijn van het bestuur en externe zorgbegeleiders. Met de leverancier van ParnasSys is een zogenaamde verwerkersovereenkomst (conform het model van de PO-raad) afgesloten, waarin ook afspraken zijn gemaakt over beveiliging en backup van de data die in ParnasSys wordt opgeslagen.

De uitwisseling met de overheid en andere scholen gebeurt via een beveiligde koppeling met ParnasSys.

Voor digitale leermiddelen en toetsen worden systemen van diverse leveranciers of uitgeverijen gebruikt. Met deze partijen worden of zijn verwerkersovereenkomsten afgesloten. Onderdeel hiervan is dat zij ook voldoen aan de nationale standaarden en voorzieningen met betrekking tot de veilige uitwisseling van persoonsgegevens. In dit kader wordt op termijn gebruik worden gemaakt van de nummervoorziening die het mogelijk maakt om alleen nog maar gepseudonimiseerde gegevens met deze partijen uit te wisselen.

Een overzicht van leveranciers met wie een overeenkomst is afgesloten over de uitwisseling van persoonsgegevens is op te vragen bij het stafkantoor van Vivente.

1.4 Aan wie worden deze gegevens verstrekt?

De gegevens mogen in beginsel niet aan derden worden doorgegeven of door anderen worden ingezien zonder toestemming van de ouders, tenzij de school verplicht is om bepaalde persoonsgegevens te verstrekken, die noodzakelijk zijn voor de uitvoering van een wettelijke plicht. Toestemming van ouders vindt schriftelijk plaats en wordt opgeslagen in het leerlingdossier.

Bij het uitwisselen van gegevens wordt altijd gecheckt of aan de vijf privacy-vuistregels wordt voldaan:

1. Doel en doelbinding
2. Grondslag
3. Dataminimalisatie
4. Transparantie
5. Data-integriteit

De gegevens worden verstrekt aan de volgende externe partijen:

- Externe partijen die in opdracht van de school en met toestemming van de ouders ondersteunen bij het bieden van aanvullende onderwijsbegeleiding voor de leerling.
- Een andere onderwijsinstelling bij verhuizing, overplaatsing of doorstroming naar het V(S)O. Ouders hoeven hiervoor geen toestemming te verlenen. Zij hebben wel recht op inzage. Eventuele opmerkingen van ouders kunnen toegevoegd worden aan het dossier, maar de school is niet verplicht tot wijziging van de gegevens.
- Het Regionaal Samenwerkingsverband. Ook hiervoor hoeven ouders geen toestemming te verlenen. Zij hebben wel recht op inzage. Eventuele opmerkingen van ouders kunnen toegevoegd worden aan het dossier, maar de school is niet verplicht tot wijziging van de gegevens.
- Externe deskundigen uit het MDO (schoolmaatschappelijk werk, schoolarts/ -verpleegkundige, ambulant begeleider, orthopedagoog) op grond van toestemming door de ouders/verzorgers.
- Bewerkers in de zin van leveranciers van onderwijsleermiddelen die in opdracht van de school zorgen voor toegang en beheer van de digitale systemen die bij de begeleiding en zorg voor leerlingen worden gebruikt en waarmee een verwerkersovereenkomst is afgesloten.

1.5 Bewaartermijnen

Vivente hanteert voor persoonsgegevens de wettelijke bewaartermijnen.

2. Privacy van medewerkers

Niet alleen van leerlingen worden persoonsgegevens verwerkt binnen de stichting, maar ook van onze medewerkers. Soms zijn dat gegevens die direct samenhangen met de arbeidsverhouding tussen het bestuur en medewerkers, maar ook worden persoonsgegevens van onze medewerkers verwerkt in systemen die gebruikt worden bij het geven en begeleiden van onderwijs. De informatie over persoonsgegevens van medewerkers is ook van toepassing op stagiaires.
In dit hoofdstuk is te lezen om welke verzamelingen het gaat, waarom die gegevens worden gebruikt, wie ze gebruikt en aan wie ze worden verstrekt.

2.1 Om welke gegevens gaat het?

- Naam, voornamen, geslacht, geboortedatum, adresgegevens en soortgelijke voor communicatie benodigde gegevens, bankrekeningnummer van de medewerker
- Een administratienummer (o.a. BSN)
- Nationaliteit en geboorteplaats
- Gegevens voor digitale communicatie
- Gegevens over de groep waar een medewerker aan gekoppeld is
- Loggegevens over het gebruik van de systemen
- Gegevens over salaris, belasting, premies en andere vergoedingen
- Gegevens over gevolgde en te volgen opleidingen, cursussen en stages
- Gegevens voor personeelsbeoordeling en loopbaanbegeleiding.
- Gegevens over de (voormalige) functie, alsmede over de aard, inhoud en beëindiging van het dienstverband
- Gegevens voor de administratie van aan- en afwezigheid.
- Gegevens die in het belang van de medewerker worden opgenomen met het oog op zijn/haar arbeidsomstandigheden
- Gegevens, waaronder begrepen gegevens over (voormalige) gezinsleden van de medewerker, die noodzakelijk zijn voor een overeengekomen arbeidsvoorwaarde
- Andere dan de hierboven genoemde gegevens waarvan de verwerking wordt vereist vanwege de toepassing van een andere wet

2.2 Wat is het doel van de verzameling van deze gegevens?

Deze gegevens worden verzameld om:

- Onderwijs te geven en leerlingen te begeleiden en volgen, waaronder:
  - Opslag van leer- en toetsresultaten
  - Het terugontvangen van leer- en toetsresultaten om te verwerken in het leerlingvolgsysteem
  - De beoordeling van leer- en toetsresultaten om leerstof en toetsmateriaal te kunnen aanbieden dat is afgestemd op de specifieke leerbehoefte van een leerling
  - Analyse en interpretatie van leerresultaten
  - Het kunnen uitwisselen van leer- en toetsresultaten tussen digitale onderwijsmiddelen
  - Gebruik te maken van specifiek docenteninformatie in de digitale onderwijsmiddelen
- (Digitale) onderwijsmiddelen door leveranciers geleverd te krijgen en in gebruik te kunnen nemen
- Het geven van leiding aan de werkzaamheden van de medewerker
- De behandeling van personeelszaken
- Het berekenen, vastleggen en betalen van salarissen, vergoedingen en andere geldsommen en beloningen in natura
- Het berekenen, vastleggen en betalen van belasting en premies
- De uitvoering van een voor de medewerker geldende arbeidsvoorwaarde
- Opleidingen en scholing van de medewerker
- Bedrijfsmedische zorg en bedrijfsmaatschappelijk werk voor de medewerker

- De interne controle en de bedrijfsvoering
- Het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen
- Het behandelen van geschillen
- Het doen uitoefenen van accountantscontrole
- Het verlenen van ontslag
- Het regelen van aanspraken op uitkeringen in verband met de beëindiging van een dienstverband
- De uitvoering of toepassing van een andere wet
- Toegang tot de systemen te krijgen
- De beveiliging, controle en preventie van misbruik en oneigenlijk gebruik en het bewaken van de consistentie en betrouwbaarheid van de opgeslagen gegevens te verzorgen
- De continuïteit en goede werking van de systemen te waarborgen

Voor de organisatie van het onderwijs en begeleiding van leerlingen wordt gebruik gemaakt van digitale systemen, waarin gegevens over hun prestaties en welbevinden worden vastgelegd. In deze systemen worden ook gegevens van medewerkers vastgelegd, gericht op het kunnen maken van een koppeling tussen leerling en de betrokken medewerker en om de opgeslagen gegevens van de leerlingen in te kunnen zien, aan te vullen en te wijzigen.

Voor het verzorgen van het onderwijs wordt, naast boeken, ook gebruik gemaakt van digitale onderwijsmiddelen. In deze onderwijsmiddelen, die worden afgenomen van externe leveranciers, worden persoonsgegevens verwerkt die nodig zijn voor de toegang tot en het gebruik van deze digitale producten en diensten. Voorbeelden van deze digitale onderwijsmiddelen zijn, digitale (aanvullingen op) lesmethodes, toetssystemen en apps. Ook in deze systemen worden persoonsgegevens van medewerkers opgeslagen.

Tevens worden onderwijsondersteunende ICT-middelen, zoals iPads of andere (draagbare) computersystemen ingezet. Voor systeembeheer, beveiliging, logging en monitoring wordt software op deze middelen geïnstalleerd die persoonsgegevens verzamelen.

2.3 Wie hebben toegang tot de personeelsgegevens en hoe worden deze beveiligd?

Binnen de school hebben de volgende type medewerkers toegang tot (een deel van) de gegevens:

- Leden van het CvB, de directie en het MT (systemen voor organisatie en begeleiding onderwijs en formatieplanning)
- Administratief personeel (systemen voor organisatie en begeleiding onderwijs en formatieplanning)
- Stafmedewerkers bestuursbureau, directiesecretaresses en hoofd bedrijfsvoering (ze hebben alleen toegang tot gegevens die geregistreerd staat bij hun rol).
- Medewerkers salarisadministratie en financiën
- Personeelsadviseurs
- Leidinggevende van de betreffende medewerker

- Hoofd P&O, bedrijfsvoering en financiën
- ICT-ondersteunend personeel

Niet alle rollen hebben tot alle gegevens toegang. Per rol is vastgesteld welke gegevens ingezien en gewijzigd kunnen worden, Gegevens die daarbij niet noodzakelijk zijn, kan die rol ook niet inzien of wijzigen.

Voor personeelsgegevens die in dezelfde systemen worden verwerkt als die van leerlingen, gelden dezelfde maatregelen als in hoofdstuk 1.3. zijn genoemd.

Via AFAS worden verzuimgegevens geregistreerd. Ook hiervoor geldt dat er binnen het bestuur een toegangsbeleid is opgesteld dat jaarlijks wordt gecontroleerd. Met beide partijen worden ook verwerkersovereenkomsten afgesloten.

2.4 Bij het uitwisselen van deze gegevens wordt altijd gecheckt of aan de 5 privacy-vuisregels wordt voldaan

1. Doel en doelbinding
2. Grondslag
3. Dataminimalisatie
4. Transparantie
5. Data-integriteit

De gegevens worden verstrekt aan de volgende externe partijen:

- Bewerkers in de zin van leveranciers van onderwijsleermiddelen en of die in opdracht van de school deze middelen ter beschikking stellen
- Bewerkers die zorgen voor toegang tot de onderwijsleermiddelen in opdracht van de school
- Bewerkers in de zin van leveranciers van onderwijsleermiddelen die in opdracht van de school zorgen voor toegang en beheer van de digitale systemen die worden gebruikt bij de begeleiding en zorg voor leerlingen
- Systemen voor de personeelsadministratie.
- Systemen voor het taakbeleid
- Systemen voor observatie instrumenten

2.5 Inzage en wijziging

Alle medewerkers binnen de stichting hebben een eigen inlog voor het digitale personeelsdossier. Wanneer men vragen heeft over de persoonsgegevens of deze wil wijzigen dan kan de medewerker terecht bij de personeelsadministratie, te bereiken via telefoonnummer: 038-3556570
Wanneer medewerkers de persoonsgegevens wil inzien of wijzigen in de onderwijssystemen van de school, dan kan men hiervoor terecht bij de afdeling administratie via pz@vivente.nu

2.6 Bewaartermijnen

De Vivente-groep hanteert de wettelijke bewaartermijnen.

3. Privacy van derden

In sommige gevallen worden gegevens van derden opgeslagen, die geen leerling, ouder of medewerker zijn. In dit hoofdstuk is te lezen om welke verzamelingen dit gaat, waarom die gegevens worden gebruikt, wie ze gebruikt en aan wie ze worden verstrekt.

3.1. Sollicitanten

De Vivente-groep hanteert in een sollicitatiecode welke is opgenomen in de cao PO.

Binnen het bestuur hebben alleen medewerkers die betrokken zijn bij de sollicitatieprocedure toegang tot de persoonsgegevens van de sollicitanten.

De gegevens worden alleen verstrekt aan externe partijen die namens het bestuur een test of assessment verzorgen. In dat geval worden aan de direct bij de activiteiten betrokken personen slechts die persoonsgegevens verstrekt die noodzakelijk zijn voor de test of assessment.

Bijzonderheden

De persoonsgegevens worden verwijderd op een daartoe strekkend verzoek van de sollicitant en in ieder geval uiterlijk vier weken nadat de sollicitatieprocedure is beëindigd, tenzij de persoonsgegevens met toestemming van de sollicitant langer worden bewaard.

Inzage en wijziging

Alle medewerkers binnen het bestuur hebben een eigen inlog voor het digitale personeelsdossier. Wanneer men vragen heeft over de persoonsgegevens of deze wil wijzigen, dan kan men hiervoor terecht bij de afdeling personeelszaken.

3.2. Extern ingehuurd personeel

Soms wordt gebruik gemaakt van extern personeel, om kennis aan te vullen of om opengevallen plekken tijdelijk op te vullen. Om de contracten en inzet af te handelen, worden gegevens in diverse systemen opgeslagen.

Persoonsgegevens

De gegevens die worden verzameld en opgeslagen zijn:

- Naam, voornamen, geslacht, geboortedatum, adresgegevens en soortgelijke voor communicatie bedoelde gegevens
- Bedrijfsgegevens en bankrekeningnummer van de extern ingehuurde medewerker
- Kopie verstrekte VOG
- De gegevens voor de organisatie en begeleiding van onderwijs zoals vermeld in paragraaf 2.1.

Deze gegevens worden verzameld om:

- De contractuele en financiële verplichtingen af te handelen die samenhangen met de inhuur

- De ingehuurde in staat te stellen de ICT-middelen en software in te zetten die nodig zijn bij de uitvoer van de werkzaamheden
- De correcte uitvoering van een wettelijke verplichting die samenhangt met de inhuur.

Binnen de stichting hebben de volgende type medewerkers toegang tot de gegevens:

- Medewerkers salarisadministratie en financiën
- Personeelsadviseurs
- Opdrachtgever van de betreffende externe medewerker
- Hoofd P&O, bedrijfsvoering en financiën
- ICT-ondersteunend personeel
- Leden van de CVB, directie en MT

Deze gegevens worden verstrekt aan uitzendbureaus en detacheringsbureaus waarmee door het bestuur wordt samengewerkt.

Bijzonderheden
De persoonsgegevens worden verwijderd zo snel mogelijk na beëindiging van de contractperiode, maar maximaal na 2 jaar, tenzij een wettelijke bepaling anders voorschrijft.

3.3. Vrijwilligers

Vrijwilligers, met name ouders van (oud)leerlingen, worden op de verschillende scholen ingezet om te helpen bij schoolactiviteiten.
Van de vrijwilligers worden alleen gegevens verzameld en opgeslagen die nodig zijn om contact met hen te onderhouden. Het betreft naam, adres, telefoonnummer en/of e-mailadres, VOG en de vrijwilligersovereenkomst.

3.4 Oud-leerlingen

Voor het onderhouden van contacten met en het verzenden van informatie aan oud-leerlingen worden de volgende gegevens opgeslagen:

- Naam, voornamen, geslacht, geboortedatum, adresgegevens en soortgelijke voor communicatie bedoelde gegevens
- Gegevens betreffende de schoolloopbaan van de oud-leerling.

4. Inzage en wijzigen

Wanneer de betrokkene/het data-subject de persoonsgegevens wil inzien of wijzigen, dan kan men hiervoor een afspraak maken met de directeur van de betreffende school. Personeel richten aan het stafkantoor.
Ouders krijgen het dossier niet mee, maar hebben wel recht op een kopie

5. Datalekken

Wanneer de kans bestaat dat er persoonsgegevens in handen zijn gekomen van derden die geen toegang zouden moeten hebben tot die gegevens of wanneer de mogelijkheid bestaat dat er

persoonsgegevens verloren zijn gegaan dient dit direct gemeld te worden via de procedure melden datalekken van [bestuur]. Het bevoegd gezag is verantwoordelijk voor eventuele melding van een datalek bij de Autorisatie Persoonsgegevens, indien er onterecht geen melding gedaan wordt kan dit leiden tot fikse boetes. De volledige procedure melden datalekken is opgenomen in het privacy handboek.

6. Klachten

Indien men van mening is dat het privacy protocol niet op de juiste wijze wordt nageleefd binnen het bestuur kan er een klacht worden ingediend bij klachten@vivente.nu
Wanneer deze klacht voor de betrokkene niet leidt tot een acceptabele oplossing kan men zich wenden tot de stichting.

B. Privacystatement voor in de schoolgids en op de website

De Vivente scholengroep en de scholen die onder Vivente vallen vinden privacy belangrijk. Wij gaan zorgvuldig om met persoonsgegevens van leerlingen, ouders en medewerkers. Daarbij houden wij ons aan de eisen uit de privacywetgeving.
Dat betekent bijvoorbeeld dat wij:

- duidelijke vermelden voor welke doeleinden wij persoonsgegevens verwerken;
- het verzamelen van persoonsgegevens beperken tot alleen de persoonsgegevens die nodig zijn voor de doeleinden waarvoor ze worden verwerkt;
- vooraf vragen om uitdrukkelijke toestemming om de persoonsgegevens van betrokkenen te verwerken in gevallen dat toestemming vereist is*;
- kunnen aantonen dat er ook in andere gevallen een wettelijke grondslag voor de verwerking is;
- de gegevens van betrokkenen niet doorgeven aan derde partijen, tenzij dat nodig is om goed onderwijs te kunnen bieden of dat er een wettelijke verplichting is;
- wanneer wij persoonsgegevens van betrokkenen delen, afspraken maken (verwerkersovereenkomst) over het gebruik van deze gegevens*;
- passende beveiligingsmaatregelen nemen om persoonsgegevens te beschermen en dit ook eisen van de partijen die in onze opdracht persoonsgegevens verwerken;
- geheimhouding vragen van medewerkers die met persoonsgegevens werken en ook eisen dat zij zorgvuldig met de persoonsgegevens omgaan*;
- bijhouden in een dataverwerkingsregister welke structurele geautomatiseerde verwerkingen van persoonsgegevens wij doen;
- gegevens niet langer bewaren dan noodzakelijk is of wettelijk mag*;
- een meldpunt hebben voor datalekken en een procedure om schade in voorkomende gevallen te beperken.
- een FG (functionaris gegevensbescherming) hebben aangesteld welke verantwoordelijk is voor de controle op uitvoering van het privacybeleid.
- de rechten van betrokkenen respecteren om op het verzoek van betrokkene inzage te bieden in de verzamelde gegevens, de gegevens te corrigeren wanneer deze niet kloppen of het verwijderen van de gegevens. Dit alles alleen wanneer dit niet in strijd is met de wet.

Contact opnemen naar aanleiding van dit privacystatement, of bij algemene vragen met betrekking tot privacy kan via avg@vivente.nu.
*De met een ster gemarkeerde onderwerpen zijn voor het overgrote deel, maar nog niet volledig op orde. Wij streven ernaar dit na de kerstvakantie 2018 af te ronden.

FG (Functionaris Gegevensbescherming)

De FG van de Vivente scholengroep is dhr. L. Zegers. Hij is bereikbaar op l.r.zegers@goon.nl en in geval van nood op telefoonnummer 06-40751163.
Het FG-registratienummer is FG006477.

Datalek melden?

Neem zo spoedig mogelijk (24/7) contact op met leidinggevende, schooldirecteur of met de FG via l.r.zegers@goon.nl

C. Responsible disclosure beleid Vivente-groep

Bij de Vivente-groep vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is.

Wij vragen je een bijdrage te leveren aan de veiligheid van ict-systemen en het beheersen van de kwetsbaarheid van ict-systemen. Dat kun je doen door de door jou ontdekte kwetsbaarheden op verantwoorde wijze bij de Vivente-groep te melden. Als je een zwakke plek in één van onze systemen hebt gevonden horen wij dit graag zo snel mogelijk, zodat we aanvullende (beveiligings)maatregelen kunnen treffen.

Wij vragen je:

- Je bevindingen te melden via avg@vivent.nu
- De door jou ontdekte kwetsbaarheid niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of (persoons)gegevens van derden in te kijken, te verwijderen of aan te passen.
- Je bevinding/probleem niet met anderen te delen totdat de kwetsbaarheid is verholpen en alle (vertrouwelijke) gegevens die zijn verkregen door de kwetsbaarheid direct na het verhelpen daarvan te wissen.
- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden.
- Voldoende informatie te geven om de kwetsbaarheid te reproduceren zodat wij deze zo snel mogelijk kunnen verhelpen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

Wij zeggen toe dat:

- We reageren zo spoedig mogelijk op jouw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing.
- Als je je aan bovenstaande voorwaarden houdt, wij geen aangifte van een strafbaar feit zullen doen of andere juridische stappen tegen je ondernemen betreffende de melding.*
- Wij jouw melding vertrouwelijk behandelen en je persoonsgegevens zonder jouw toestemming niet zullen delen met derden of verder zullen verwerken, tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Melden onder een pseudoniem is mogelijk.
- Wij je op de hoogte houden van de voortgang van het verhelpen van de kwetsbaarheid.
- In berichtgeving over de gemelde kwetsbaarheid wij je, indien je dit wenst, zullen vermelden als ontdekker van de kwetsbaarheid. Wij streven ernaar alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

* Let op: het feit dat de Vivente-groep geen aangifte tegen jou zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar jouw handelen gehouden kan worden dan wel dat je strafrechtelijk kunt worden veroordeeld.

D. Toestemmingsformulier (voorbeeld)

Toelichting in het kader van privacywetgeving

De gegevens die u heeft ingevuld op het inschrijfformulier, worden opgeslagen in de leerlingadministratie van onze school. Uiteraard worden deze gegevens vertrouwelijk behandeld. Op onze administratie is de Algemene Verordening Persoonsgegevens van toepassing. Dit betekent onder andere dat de gegevens door ons worden beveiligd, en dat de toegang tot de administratie is beperkt tot alleen personeel die de gegevens strikt noodzakelijk nodig heeft. U heeft als ouder het recht om de door ons geregistreerde gegevens in te zien (voor zover die informatie betrekking heeft op uw kind). Als de gegevens niet kloppen, dan mag u van ons verwachten dat wij – op uw verzoek - de informatie verbeteren of aanvullen.
Een aantal vragen in dit inschrijfformulier zijn wij wettelijk verplicht aan u te stellen. Zo vragen wij naar uw opleidingsniveau. Dit heeft te maken met de wettelijke 'gewichtenregeling': het aantal leerkrachten aan onze school is mede afhankelijk van het totaal van het 'leerlinggewicht' van onze leerlingen.
Voor meer informatie over de omgang met de privacy van uw kind(eren), verwijzen wij u naar ons privacyreglement.

Toestemming

In het kader van privacywetgeving, willen wij u toestemming vragen voor het delen van de volgende persoonsgegevens. U mag natuurlijk altijd terugkomen op de door u gegeven toestemming. Ook mag u op een later moment alsnog toestemming geven.

Foto- en videomateriaal

Op onze school laten wij u met foto's en video's zien waar we mee bezig zijn. Opnames worden gemaakt tijdens verschillende gelegenheden. Ook uw zoon/dochter kan op deze foto's (en soms in video's) te zien zijn. Graag willen we daarom uw toestemming voor het gebruik van beeldmateriaal van uw zoon/dochter. Uw toestemming geldt alleen voor foto's en video's die door ons, of in onze opdracht worden gemaakt. Het maken van foto's door ouders is binnen de school niet toegestaan. Het kan voorkomen dat andere ouders foto's maken tijdens schoolactiviteiten die buiten de school plaatsvinden. De school heeft daar geen invloed op. Wij vragen daarom aan ouders om terughoudend te zijn met het maken van foto's en video's en deze niet te delen via sociale media.

Adressenlijst

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

Sociale media

Sociale media spelen een belangrijke rol in het leven van leerlingen en onderwijzend personeel. Het gebruik van sociale media is onderdeel van het gedrag van leerlingen binnen de school. Sociale media kunnen helpen om het onderwijs te verbeteren en de lessen leuker te maken en om contact te onderhouden met vrienden of klasgenoten. Maar sociale media brengen ook risico's met zich mee, zoals pesten en het ongewild delen van foto's of andere gegevens. Op school besteden we in ons lesprogramma hier aandacht aan. Voor het gebruik van sociale media door uw kind(eren), vragen wij uw toestemming.

Hierbij verklaart ondergetekende, ouders/verzorger van ……., dat:

1 foto's en video's WEL gebruikt mogen worden:

- op de app en/of het ouderportaal van de school
- in de (digitale) nieuwsbrief
- in de schoolkalender
- in de schoolgids
- op de website van de school
- in folders en flyers ter promotie van de school
- op sociale-media accounts van de school (Whatsapp, Twitter, Facebook)

(kruis aan waar u toestemming voor geeft)

2 haar/zijn naam, adres en telefoonnummer WEL / NIET * gedeeld mag worden met andere ouders

3 hij/zij onder schooltijd WEL / NIET * gebruik mag maken van sociale media t.b.v. onderwijsdoeleinden

(* streep door wat niet van toepassing is)

	Ouder/verzorger 1	Ouder/verzorger 2
Naam:	_____	_____
Datum:	_____	_____
Plaats:	_____	_____
	_____	_____
Handtekening:	_____	_____

E. Procedure datalekken

Inleiding

Deze procedure maakt integraal onderdeel uit van het privacybeleid van de ons bestuur en is vastgesteld door het college van bestuur.

De procedure bestaat uit verschillende onderdelen voor afzonderlijke doelgroepen, te weten:
A. Medewerkers en leerlingen (meldingen aan ict-coördinator of schoolleider)
B. Ict-coördinator of Directeur (meldingen aan bovenschoolse Functionaris Gegevensbescherming)
C. Functionaris gegevensbescherming (meldingen aan Autoriteit Persoonsgegevens)

Er wordt periodiek (minstens een keer per jaar) gecontroleerd of deze procedure inclusief de onderstaande beschreven stappen adequaat zijn geïmplementeerd.

Waarom deze procedure?
Beveiligingsincidenten kunnen leiden tot informatie en/of gegevens die verloren gaan of onbedoeld gewijzigd worden. Dit kan gevolgen hebben voor de kwaliteit en continuïteit van het onderwijs.

Daarnaast kunnen vertrouwelijke gegevens door beveiligingsincidenten op straat komen te liggen of in verkeerde handen vallen. Voor de verwerking van persoonsgegevens zijn regels vastgelegd Algemene Verordening Persoonsgegevens (AVG). Het niet zorgvuldig omgaan met vertrouwelijke gegevens kan leiden tot boetes en imagoschade.

Als een beveiligingsincident betrekking heeft op persoonsgegevens, moet er binnen 72 uur melding worden gemaakt aan de Autoriteit Persoonsgegevens door de Functionaris Gegevensbescherming.

Definities

Wat is een beveiligingsincident?

Een beveiligingsincident is een gebeurtenis waarbij gegevens:

1. verloren zijn geraakt
2. gestolen zijn
3. beschadigd zijn
4. onbedoeld gewijzigd zijn
5. onrechtmatig toegankelijk zijn voor derden

Wat is een datalek?

Er is sprake van een datalek als er bij een opgetreden beveiligingsincident persoonsgegevens betrokken zijn.

Wat zijn persoongegevens?

Alle gegevens die (evt. gecombineerd met andere gegevens) tot een persoon herleid kunnen worden.

Voorbeelden persoonsgegevens

Naam

BSN

Pasfoto

Geboortedatum

Adres

IP-adres

Etc.

E1 Medewerkers en leerlingen

Onderstaande teksten zijn opgenomen op de website, schoolgids en/of intranet van de scholen binnen ons de Vivente-groep.

Persoonsgegevens gelekt? Meld ze direct!

Als er sprake is van gestolen computers of opslagmedia, virussen of kwijtgeraakte logingegevens waardoor persoonsgegevens toegankelijk zijn voor anderen, meld dit dan zo snel mogelijk bij de schoolleiding van de school. De schoolleiding meldt het datalek aan de Functionaris Gegevensbescherming

Op deze manier hopen we binnen de Vivente-groep veilig en probleemloos met ict te kunnen werken. In ons privacyreglement kunt u lezen hoe wij omgaan met persoonsgegevens.

Voorbeelden

- computer of software die niet werkt of bruikbaar is
- kwijtgeraakte USB-stick
- gestolen laptop
- inbraak door een hacker
- DDOS aanval
- malware- of virusbesmetting
- gestolen logingegevens
- onbeveiligde serverruimte.

Nog 3 belangrijke tips:

1. Deel je logingegevens nooit met anderen en laat ze niet meekijken.
2. Als je een link in je mail niet vertrouwt, klik er dan niet op.
3. Mocht je computer besmet zijn met een virus, sluit de computer dan zo snel mogelijk af en verbreek de internet- of netwerkverbinding, om besmetting te voorkomen.

E2 Directeur

Stap 1 - Analyseer en beoordeel (binnen 8 uur na melding)

Heeft de melding betrekking op persoonsgegevens?
Meld dit direct via avg@vivente.nu en via l.r..zegers@goon.nl de Functionaris Gegevensbescherming binnen ons bestuur. Deze is in noodgevallen te bereiken op het volgende telefoon nr. 06-40751163

Wat is een datalek?
Er is sprake van een datalek als er bij een opgetreden beveiligingsincident Persoonsgegevens betrokken zijn.

Stap 2 - Inventariseer en registreer

Indien er een melding wordt gedaan van een beveiligingsincident, dan worden de volgende gegevens geregistreerd:

Naam:
Datum:
Tijdstip:
Omschrijving incident:
Soort gegevens:
Omvang gegevens: (aantal personen)
Betrokkenen:
Locatie:
Type hardware (tagcode):
Naam software:

Prioriteit: (indien datalek: hoog)
Backup aanwezig?: ja/nee
Zijn de gegevens geëncrypt?: ja/nee

Stap 3 – Neem herstelmaatregelen

Is er sprake van diefstal, verlies of beschadiging?
Dan moet het systeem vervangen worden en/of de backup teruggeplaatst worden (indien aanwezig). Neem hiervoor contact op met de ict-leverancier van de school.

Is er sprake van onrechtmatige toegang?
Dan dient de toegang afgesloten te worden door fysieke beveiliging, een wijziging in de configuratie van het netwerk of in de accounts van computers, netwerkapparatuur of applicaties, zoals wachtwoorden. Pas dit zelf aan de software of neem hiervoor contact op met de ict-leverancier van de school.

Is er sprake van DDOS aanval op servers die in beheer zijn van de school?
Dan dient relevante netwerk apparatuur afgesloten of opnieuw geconfigureerd te worden, eventueel in overleg met leveranciers of externe beheerders. De bovenschoolse ICT- coördinator neemt hiervoor contact op met de ict-leverancier van de school of de leverancier van het betreffende softwarepakket.

Is er sprake van malware of anti-virus aanvallen?
Dan dient de computer of apparatuur uit het netwerk genomen, opgeschoond en hersteld te worden. Indien nodig dienen backups teruggeplaatst te worden. Neem hiervoor contact op met de ict-leverancier van de school.

Stap 4 – Neem preventieve maatregelen en registreer deze bij de melding

De melding kan pas afgesloten worden als de herstelmaatregelen zijn uitgevoerd en er preventieve maatregelen zijn genomen en beschreven om het risico op toekomstige incidenten te vermijden of te verkleinen.

De herstelmaatregelen en preventieve maatregelen worden geregistreerd bij de melding door de Functionaris gegevensbescherming.

N.B. De registratie van meldingen wordt meegenomen in de periodieke evaluatie van het privacybeleid van ons bestuur. In de evaluatie wordt ingegaan op eventuele structurele ontwikkelingen, en of de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen.

E3 Functionaris gegevensbescherming

Dit onderdeel is opgenomen in het procedurehandboek van de bovenschoolse Functionaris gegevensbescherming. Dit betreft een rol die op bovenschools niveau is belegd en belast is met onder andere de volgende taken en verantwoordelijkheden:

- (Laten) uitvoeren risico-analyses
- (Laten) opstellen / bijwerken beleidsplan
- (Laten) opstellen, evalueren en controleren jaarplan
- Rapporteren (relevante) incidenten en datalekken aan directeur/bestuurder

Stap 1 - Controleer en registreer

Controleer of al gegevens zijn geregistreerd over het beveiligingsincident. Vul deze registratie aan met de informatie die uit de volgende stappen naar voren komt.

Stap 2 – Bepaal of er sprake is van een datalek (binnen 8 uur na melding)

Zijn er bij het incident persoonsgegevens verloren gegaan?
Er is geen kopie of backup aanwezig van de persoonsgegevens

Is er bij het incident sprake van onrechtmatige verwerking van persoonsgegevens?
En kan dit niet uitgesloten worden?
Onbevoegden hebben onrechtmatig toegang kunnen krijgen tot de persoonsgegevens

Indien Ja op één van beide → Ga naar stap 3
Indien Nee op beide →Er is geen sprake van een datalek, overleg met systeembeheer over preventieve maatregelen

N.B. Schakel indien nodig een externe deskundige in en informeer de betrokken leverancier(s)! Zie bewerkersovereenkomst voor de afspraken in het kader van datalekken met leveranciers.

Stap 3 – Bepaal of er sprake is van meldplicht

Zijn er persoonsgegevens van gevoelige aard gelekt of leidt de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

Indien Ja → Ga naar stap 4
Indien Nee → Er is geen sprake van meldplicht, overleg met systeembeheer over preventieve maatregelen

Gegevens van gevoelige aard:
Godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap vakvereniging, strafrechtelijke gegevens of over onrechtmatig of hinderlijk gedrag, financiële gegevens of over de economische situatie, gegevens die kunnen leiden tot stigmatisering (schoolprestaties, relatieproblemen), gebruikersnamen en wachtwoorden, gegevens die kunnen worden gebruikt bij identiteitsfraude (BSN)

Nadelige gevolgen:
Misbruik in het criminele circuit van grote databestanden, ingrijpende beslissingen die op basis van (gewijzigde) gegevens worden genomen, gevolgen die binnen ketens van gegevensverwerking kunnen optreden.

Stap 4 – Informeer het college van bestuur en bepaal of betrokkenen ook geïnformeerd dienen te worden.

Ontbreken er technische beschermingsmaatregelen waardoor het datalek (waarschijnlijk) nadelige gevolgen kan hebben voor leerlingen, ouders of personeel?
De gegevens zijn niet voorzien van encryptie of de encryptie is verouderd.

Indien Ja → Ga naar de volgende vraag
Indien Nee → Ga naar stap 5 en informeer het college van bestuur

Zijn er zwaarwegende redenen om de melding aan leerlingen, ouders of personeel achterwege te laten?
Het informeren van de leerlingen, ouders of personeel kan negatieve gevolgen hebben voor de veiligheid van anderen.

Indien Ja → Ga naar stap 5 en informeer het college van bestuur
Indien Nee → Ga naar stap 5 en informeer het college van bestuur en de communicatiemedewerker (zie deel D procedure Melden beveiligingsincidenten en datalekken)

Stap 5 – Meld het datalek bij de Autoriteit (binnen 72 uur na melding)

Verzamel alle benodigde informatie (zie bijlage A voor vragenlijst)

Na toestemming van het college van bestuur wordt door de Privacyfunctionaris een melding gedaan via http://datalekken.autoriteitpersoonsgegevens.nlof (indien de website niet beschikbaar is) via faxnummer 070 - 888 85 01

De melding wordt minimaal 3 jaar bewaard. Informeer indien nodig de leverancier over de melding.

F. Model Bruikleenovereenkomst apparatuur

De ondergetekende: Vivente te Zwolle, in deze vertegenwoordigt door Marco Hart, algemeen beleidsmedewerker, hierna te noemen werkgever
en
[Naam medewerk(st)er], personeelsnummer [nummer], werkzaam als [functie] bij [School],
hierna te noemen werknemer:
Verklaren dat zij een "*Bruikleenovereenkomst apparatuur*", verder te noemen "*apparatuur*", voor de duur van de arbeidsovereenkomst zijn aangegaan. De navolgende voorwaarden zijn op deze overeenkomst van toepassing:

- Werkgever verstrekt aan werknemer de apparatuur ten behoeve van de uitoefening van de werkzaamheden van de dienstbetrekking.
- De apparatuur is eigendom van werkgever en wordt in bruikleen gegeven aan werknemer.
- Deze overeenkomst bepaalt de nadere gebruiksvoorwaarden waaronder werknemer de apparatuur kan gebruiken.
- Door ondertekening aanvaardt werknemer alle voorwaarden van deze overeenkomst.

1. Aard en uitvoering

De apparatuur is door werkgever aangeschaft en ter beschikking gesteld. Zie verder de specificatie "Hardware gegevens".

2. Rechten en plichten werknemer

a. Werknemer verklaart de apparatuur in goede staat te hebben ontvangen en stelt deze niet aan derden ter beschikking, verpandt of vervreemdt deze op enigerlei andere wijze.
b. Werknemer is verantwoordelijk voor het in goede en representatieve staat houden van de apparatuur.
c. Het is werknemer verboden de apparatuur te gebruiken voor activiteiten die in strijd zijn met de bedrijfsdoelstellingen of het aanzien van de werkgever schade (kunnen) berokkenen, dan wel de grenzen van betamelijkheid en fatsoen overschrijden.
d. Werknemer is op de hoogte dat werkgever het gebruik van de apparatuur door de werknemer controleert op het zakelijk gebruik van de apparatuur. Door ondertekening van deze overeenkomst stemt de werknemer in met deze controle. Tevens verklaart werknemer zich bereid alle medewerking te verlenen die noodzakelijk is om het zakelijk gebruik te kunnen onderbouwen.
e. Werknemer verklaart zich akkoord dat, indien gehandeld in strijd met de bepalingen van deze gebruikersovereenkomst of eventuele boeten (bijvoorbeeld bellen in de auto), de naheffingsaanslagen loonheffing en een bedrag ter grootte van de correctienota's werknemersverzekeringen inclusief eventuele boeten en rente die als gevolg van dit handelen worden opgelegd aan werkgever, zullen worden verhaald op werknemer.

3. Diefstal en beschadiging

a. Werknemer dient afdoende beschermingsmaatregelen te treffen, zoals periodieke wachtwoorden, virusscanner, firewall en dergelijke ter bescherming van data op de apparatuur.
b. Werknemer dient alle zorgvuldigheid in acht te nemen ter voorkoming van beschadiging, diefstal of verlies van de apparatuur.
c. In geval van schade of diefstal van de apparatuur is werknemer verplicht dit zo spoedig mogelijk, doch uiterlijk binnen 24 uur bij werkgever te melden. Werknemer dient verder het gebruik onmiddellijk te laten blokkeren via de klantenservice van de provider. (Zie hiervoor Handleiding mobiele telefonie Vivente-groep / EC Adapt)
d. Als contractant draagt werkgever het risico voor misbruik na diefstal, mits aan het hiervoor gestelde is voldaan.
e. Werknemer kan aansprakelijk worden gesteld voor schade aan de apparatuur ontstaan door verwijtbare nalatigheid of onachtzaamheid.

4. Termijn van gebruik

a. Werknemer dient de apparatuur binnen de afgesproken bruikleentermijn dan wel bij beëindiging van het dienstverband of functieverandering op eerste verzoek in volledige staat te retourneren. Bij verzuim hiertoe, verbindt werknemer zich tot betaling van de rest(boek)waarde van de apparatuur aan werkgever.
b. Indien werknemer na het einde van de bruikleenovereenkomst of na opzegging hiervan door werkgever niet onmiddellijk voldoet aan een verzoek van werkgever tot teruggave van de apparatuur, verbeurt werknemer een boete van € 250,00 voor iedere dag, dat werknemer, na bij aangetekende brief door werkgever vermaand te zijn, aan zijn verplichtingen niet voldoet.
c. Indien één van de genoemde gevallen in deze gebruikersovereenkomst zich voordoet, is werkgever bevoegd een geschil betreffende de teruggave van de apparatuur aan het oordeel van de President van de arrondissementsrechtbank te Zwolle, rechtsprekende in kort geding, te onderwerpen.
d. Door ondertekening van deze overeenkomst verklaart werknemer dat hij gevolgen van deze overeenkomst heeft begrepen en zich daarmee akkoord verklaart.

Hardware gegevens

Soort: Telefoon / Laptop / Tablet / Overig:
Merk:
Type:
Serienummer:
Product Key Software:
Accessoires:
Totale kosten:
Direct leidinggevende, naam , is akkoord met de meerprijs boven de € 400,-- JA / NEE
Dit is telefonisch / mondeling /schriftelijk afgestemd (evt. bijlage toevoegen)
Datum ingebruikname:

Aldus verklaard, opgemaakt in tweevoud* en ondertekend te Zwolle,

.....	.....
Namens Vivente: Marco Hart	
Datum:	Datum:

* 1 exemplaar voor werkgever (t.b.v. personeelsdossier) en 1 exemplaar voor werknemer

G. Cameratoezicht

In het belang van de veiligheid, de gezondheid en het welzijn van leerlingen en medewerkers zijn kunnen scholen ervoor kiezen om camera's op te hangen. Met het cameratoezicht worden de volgende doelen nagestreefd:

- Bewaking in verband met toegang, schade door vandalisme en diefstal
- Herkenning of identificatie van personen die bij gebeurtenissen betrokken zijn geweest
- Bevorderen van het gevoel van veiligheid
- Preventief, ter voorkoming van onwenselijk gedrag
- Ondersteuning bij opsporing van strafbare feiten

Informatievoorziening

De camera's zijn zichtbaar opgehangen, er wordt in principe geen gebruik gemaakt van verborgen camera's. In bijzondere gevallen, bij vermoeden van onrechtmatig handelen van leerlingen of personeel, kan tijdelijk een verborgen camera worden geplaatst.

Bij het betreden van de school wordt gewaarschuwd dat er cameratoezicht wordt uitgevoerd.

Bewaartermijn beelden

- De camerabeelden worden maximaal 4 weken bewaard behoudens voor de beelden van de incidenten die in behandeling zijn. Indien er in de periode geen incidenten hebben plaatsgevonden of zijn gemeld bij de schoolleiding worden de beelden verwijderd.
- Bij geconstateerde incidenten worden de daaraan te relateren camerabeelden pas verwijderd nadat het incident is afgehandeld. Camerabeelden die gebruikt worden in het kader van onderzoek, waarvan aangifte is gedaan bij de politie, worden pas vernietigd na overleg met de politie. De termijn van acht weken is in deze gevallen niet van toepassing.
- Incidenten die het bewaren van beelden noodzakelijk maken, worden geregistreerd en gedocumenteerd in een logboek. Als beelden van een incident worden bekeken, wordt daarvan melding gemaakt in een logboek. Het logboek wordt beheerd door de directeur.

Bekijken van beelden

Toestemming voor het bekijken van opgeslagen en/of actuele camerabeelden kan alleen gegeven worden door de directeur van de school.

Beheer systeem

Systeembeheerders zijn alleen gerechtigd benodigde software te installeren en te controleren op het functioneren van het systeem.

Informatie aan ouders

- Ouders van een leerling die een incident meldt dat het bekijken van camerabeelden noodzakelijk maakt, worden hiervan door de schoolleiding op de hoogte gesteld.
- Indien een leerling – in het belang van het oplossen van een incident – wordt verzocht camerabeelden te bekijken, worden ouders hiervan op de hoogte gesteld. Ouders kunnen het bekijken van de beelden desgewenst bijwonen.
- Ouders van een leerling die na het bekijken van de camerabeelden als "dader" wordt geïdentificeerd, worden hiervan door de schoolleiding op de hoogte gesteld en hebben het recht de beelden binnen de bewaartermijn uit dit protocol te bekijken.

Camerabeelden die een incident registeren, dat aangifte bij de politie noodzakelijk maakt, kunnen desgevraagd door de politie worden bekeken. Ook kan de politie beelden opvragen bij vermoeden van een strafbaar feit. Betrokken leerlingen en ouders worden hierover geïnformeerd.

Colofon

Auteurs: Tonny Plas en O21, Gouda 2018
tonnyplas.nl
o21.nu