

# Protocol AVG



**CBS**

Molenwaard

# Inhoudsopgave

<b>1. Inleiding</b>	<b>2</b>
<b>2. Doelstelling</b>	<b>2</b>
<b>3. Verantwoordingsplicht</b>	
<b>4. Systemen van dataverwerking</b>	
<b>5. Persoonsgegevens</b>	<b>7</b>
<b>6. Publiceren beeldmateriaal en/of persoonsgegevens</b>	<b>8</b>
<b>7. Functionaris gegevensbescherming</b>	<b>9</b>
<b>Bijlagen</b>	<b>10</b>

## 1. Inleiding

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (hierna: AVG) in werking getreden. Deze verordening heeft diverse wijzigingen aangebracht in het huidige privacy-recht.

CBS Molenwaard heeft afspraken en werkwijzen omschreven waarmee de persoonsgegevens veilig beschermd en verwerkt worden en aan de AVG wordt voldaan. Gelet op de diverse gegevensverwerkingen binnen onze scholen en de taken die de organisatie uitvoert, zijn de impact van de AVG en de daarbij extra werkzaamheden en beperkingen, best omvangrijk.

In dit protocol worden de afspraken en werkwijzen in het kader van de AVG omschreven en uitgezet binnen de organisatie. Ook wordt beschreven welke risicofactoren het niet naleven van de AVG met zich meebrengt.

Het IBP beleid van alle scholen binnen CBS Molenwaard is volledig uniform ingeregeld.

## 2. Doelstelling

Doel van dit protocol is per 25 mei 2018 te voldoen aan de AVG, waarin integer en veilig onze persoonsgegevens worden verwerkt en beschermd. Daarmee is de kennis omtrent de AVG en zijn de processen omtrent de verwerkingen van persoonsgegevens geborgd binnen de organisatie.

## 3. Verantwoordingsplicht

De AVG legt verantwoordelijkheid bij CBS Molenwaard om aan te tonen dat aan de privacyregels voldaan wordt. Door te voldoen aan deze verantwoordingsplicht (accountability) levert onze organisatie een belangrijke bijdrage aan de bescherming van een grondrecht; namelijk het recht op privacy.

De vastgelegde afspraken zijn van groot belang bij het veilig verwerken en beschermen van de persoonsgegevens. De verantwoordingsplicht houdt in dat CBS Molenwaard kan aantonen dat wordt voldaan aan de regels van de AVG. CBS Molenwaard is verplicht om verantwoording af te leggen over de gegevensverwerkingen wanneer de Autoriteit Persoonsgegevens (AP) daar om vraagt.

De Algemene Verordening Gegevensbescherming (AVG) gaat uit van vijf vuistregels

- Rechtmatigheid;
- Transparantie;
- Doelbinding;
- Juistheid;
- Dataminimalisatie.

Wanneer een gegevensverwerking een hoog privacy-risico kan opleveren voor de betrokkenen (de personen, zoals leerlingen, ouders en medewerkers) zal een verplicht data protection impact assessment (DPIA) worden uitgevoerd. DPIA is een instrument om vooraf de privacy-risico's van een gegevensverwerking in kaart te brengen, om vervolgens maatregelen te kunnen nemen de risico's te verkleinen. In de Nederlandse vertaling van de AVG wordt de term *data protection impact assessment* (DPIA) gegevensbeschermingseffectbeoordeling genoemd.

Of een verwerking een hoog privacy-risico oplevert, wordt door de locatieleider beoordeeld. De Europese privacy-toezichthouders hebben 9 criteria opgesteld die helpen om dat te toetsen. Een DPIA is doorgaans verplicht als uw verwerking voldoet aan 2 of meer van de 9 criteria:

1. beoordelen van mensen op basis van persoonskenmerken;
2. geautomatiseerde beslissingen;
3. stelselmatige en grootschalige monitoring;
4. gevoelige gegevens;
5. grootschalige gegevensverwerkingen;
6. gekoppelde databases;
7. gegevens over kwetsbare personen (bijvoorbeeld kinderen);
8. gebruik van nieuwe technologieën;
9. blokkering van een recht, dienst of contract.

Wanneer een verwerking aan slechts één - of geen - van deze criteria voldoet, moet onderbouwd worden waarom er geen DPIA uitgevoerd is. Dit maakt onderdeel uit van de verantwoordingsplicht.

- Onze scholen moeten aantonen dat bij het gebruik van het leerlingvolgsysteem de regels van de AVG nageleefd worden. (zie 4.1)
- Onze scholen moeten aantonen dat bij het gebruik van het leerlingendossier de regels van de AVG nageleefd worden. (zie 4.2)

### **3.1 Verwerkingsregister**

Het register van verwerkingsactiviteiten bevat informatie over de persoonsgegevens die verwerkt worden en is een onderdeel van onze verantwoordingsplicht. Dit register is opgenomen in de bijlage van dit beleidsstuk.

## 4. Systemen van dataverwerking

Innovatieve, digitale systemen bieden interessante mogelijkheden om de kwaliteit van het onderwijs en de interne werkprocessen te verbeteren. Bijvoorbeeld met digitale toetsprogramma's, leerlingvolgsystemen en het gebruik van sociale media & apps. Deze mogelijkheden van persoonsgegevensverwerking, brengen ook de verantwoordelijkheid van veilig en zorgvuldig verwerken met zich mee.

### Binnen CBS Molenwaard worden onderstaande systemen gebruikt:

Instantie	Aard en doel	Duur
Parnassys	Leerling administratie	
LVS (gekoppeld aan Parn.)	Leerling resultaten volgsysteem	
ZIEN (gekoppeld aan Parn.)	Volgsysteem inzake soc. Emo. Ontw.	
OSO	Digitaal overdracht systeem	
Kijk		
Basispoort		
Mijn schoolteam	Volgsysteem functioneren teamleden	
WMK	Kwaliteitszorg systeem	
YouForce	Administratief datasysteem	
Cupella	Systeem taakurenbeleid	
Acadin		
Centrale eindtoets portal	Portal eindopbrengsten	
Van der Perk Groep BV	Web-site bouwer	
Holmwoods	Digitaal programma Engels	
Bloon	Spelling oefenprogramma	
Office 365		
Dyade	PA administratie	

De bovenstaande genoemde systemen functioneren als 'verwerker' voor CBS Molenwaard om persoonsgegevens (betrokkene, leerling en/of leerkracht) te verwerken. Met elke organisatie is een 'verwerkersovereenkomst' afgesloten. Zo'n verwerkersovereenkomst sluit uit dat de andere partij de persoonsgegevens voor eigen doelen verwerkt. CBS Molenwaard contracteert alleen organisaties die voldoende garantie bieden aan de wettelijke vereisten te voldoen. Bij het uitbesteden van de gegevensverwerking door een externe instanties blijft CBS Molenwaard verantwoordelijk voor de naleving van de AVG.

Onze verwerkersovereenkomsten voldoen aan de gestelde criteria:

- Het onderwerp en de duur van de gegevensverwerking;
- De aard en het doel van de gegevensverwerking;
- Het soort persoonsgegevens;
- De categorieën van betrokkenen;
- De rechten en verplichtingen van de verwerkingsverantwoordelijke.

### 4.1 Het Leerlingvolgsysteem

De scholen van CBS Molenwaard werken ook met een leerlingvolgsysteem zoals de wet dit voorschrijft. Een leerlingvolgsysteem houdt vorderingen en resultaten bij van leerlingen, groepen en van de school als geheel en brengen daarmee de leerprestaties en ontwikkeling van onze leerlingen systematisch in beeld. Ook andere gegevens, zoals verzuimgegevens en gezondheidsgegevens, worden in het leerlingvolgsysteem opgenomen. Gelet op de aard van deze persoonsgegevens en het feit dat kinderen extra kwetsbaar zijn, gaan we zorgvuldig om met de privacy in ons leerlingvolgsysteem.

Inzake de gegevens die in het leerlingvolgsysteem verwerkt worden, zijn de volgende afspraken gemaakt:

- We verwerken alleen gegevens die noodzakelijk zijn voor het doel van het volgen van de leerling in haar of zijn ontwikkeling;
- De gegevens die we verwerken zijn juist en up to date;
- De beveiliging van en de toegang tot het systeem is geregeld in onderstaande afspraken:
  - De teamleden (IB'er en groepsleerkrachten en OAS) die betrokken zijn bij de betreffende leerling hebben toegang tot de persoonsgegevens van die betreffende leerling(en) voor het doel van ontwikkeling monitoring;
  - De locatieleiders hebben toegang tot de persoonsgegevens van alle leerlingen;
  - Een OAS heeft toegang tot de groepen waarbij zij/hij betrokken is;
  - De Algemeen directeur en de management secretaresse hebben beperkte toegang tot de persoonsgegevens van de drie scholen;
  - Ambulant begeleider van het SWV en SOVA-trainer hebben toegang tot de persoonsgegevens van leerlingen waarbij zij betrokken zijn.
- We betrekken de betrokken personen (ouders) bij het versturen van gegevens naar derden. Hier geldt het recht van toestemming.
- De wijze van gegevensverwerking is vastgelegd in het 'verwerkingsregister';
- Gegevens over verzuim en afwezigheid en in- en uitschrijving van een leerling worden tot 5 jaar nadat de leerling is uitgeschreven, zo mogelijk digitaal, bewaard;
- Als dossiers langer bewaard moeten blijven, zal de betrokkene of wettelijk vertegenwoordiger hiervoor toestemming geven.

Elke gebruiker van gegevens dient zich bewust te zijn van een veilig gebruik en verwerking door:

- Documenten met gegevens van betrokkenen niet onbeheerd en open te laten liggen in het klaslokaal, bij de printer of anderszins;
- Bij het niet actief gebruik van documentatiestukken het computerscherm uitzetten of afschermen;
- Uitloggen wanneer geen gebruik wordt gemaakt van een datasysteem;
- Vertrouwelijke (telefoon)gesprekken in afgezonderde ruimten voeren;
- Bij inloggen met algemene inloggegevens, dient men geen persoonlijke wachtwoorden te bewaren.

## 4.2 Het leerlingendossier

In het leerlingendossier worden diverse gegevens zoals privacygegevens, onderzoeksverslagen, verslagen van ontwikkelingen opgeslagen. Er dient zorgvuldig met de verwerking van deze gegevens en dus met het leerlingendossier te worden omgegaan. Inzake de gegevens die in het leerlingendossier verwerkt worden zijn de volgende afspraken gemaakt:

- We verwerken alleen gegevens in het leerlingendossier die noodzakelijk zijn voor het doel van bewaarstukken die nodig zijn;
- We vullen het dossier alleen met gegevens die juist zijn;
- De beveiliging van en de toegang tot de leerlingendossiers is goed geregeld. De IB'er, groepsleerkracht en de locatieleider hebben toegang tot de leerlingendossiers;
- We betrekken de betrokken personen (ouders) bij het versturen van gegevens naar derden. Hier geldt het recht van toestemming;
- De wijze van gegevensverwerking zijn vastgelegd in het 'verwerkingsregister';
- De betrokkene of de wettelijk vertegenwoordiger heeft het recht om het leerlingdossier in te zien.

Men dient hiermee rekening te houden bij het inrichten of samenstellen van het dossier. Het dossier is zo opgebouwd dat een deskundige, collega of waarnemer de professionele relatie kan voortzetten.

Wanneer er over een betrokkene persoonlijke werkaantekeningen zijn gemaakt, dan maken die geen deel uit van het dossier van de betrokkene. Ze vallen daarmee buiten bijvoorbeeld het inzagerecht. Voorwaarde is wel dat het moet gaan om persoonlijke werkaantekeningen. Deze aantekeningen zijn niet bedoeld om te delen en dienen voor eigen geheugensteuntjes en mogen niet toegankelijk zijn voor anderen.

Aantekeningen in het leerlingenadministratiesysteem in het veld 'notities' zijn géén persoonlijke aantekeningen en de betrokkene heeft het recht deze in te zien. Dit zelfde geldt ook voor een

personeelsdossier: zodra er meer medewerkers dan alleen een leidinggevende toegang hebben tot aantekeningen, zijn het geen persoonlijke aantekeningen meer.

Het leerlingendossier van een reguliere leerling die vanuit het PO naar het VO is uitgestroomd of een leerling die vanwege verhuizing is uitgeschreven, wordt tot twee jaar nadat de leerling van onze school is gegaan, bewaard. Het leerlingendossier van een leerling die naar een school voor speciaal (basis)onderwijs is doorverwezen, wordt tot drie jaar nadat de leerling onze school verlaten heeft, bewaard.

## 5. Persoonsgegevens

Binnen CBS Molenwaard wordt veel gebruikgemaakt van dataverwerking. Dit omvat cijfermatige data, zoals binnen de financiële en bedrijfsadministratie, maar ook data als persoonsgegevens zowel van onze leerlingen als van de medewerkers in onze organisatie. Dit AVG-protocol ziet in beginsel op de verwerking van de persoonsgegevens. Deze persoonsgegevens worden op verschillende wijzen verzameld. We verdelen de gegevens in 'direct' en 'indirect' verzamelde persoonsgegevens.

### 5.1 Verzamelen van persoonsgegevens

Ouders worden geïnformeerd over de verwerking van persoonsgegevens die:

- We direct van ouders ontvangen, zoals de NAW-gegevens die middels het inschrijfformulier worden aangeleverd;
- We indirect verzamelen, via openbare informatie, via internet of andere kanalen.

Tenzij het informeren onmogelijk blijkt, veel inspanning vergt of de persoonsgegevens vertrouwelijk moeten blijven vanwege beroepsgeheim of geheimhoudingsplicht.

Ouders worden geïnformeerd over de volgende zaken in het kader van de verwerking van hun persoonsgegevens:

- Identiteit van de persoon die de gegevens verwerkt en de vertegenwoordiger van de organisatie;
- De functionaris voor de gegevensbescherming;
- Het doel van de persoonsgegevens;
- Aan wie de persoonsgegevens worden verstrekt;
- Of gegevens evt. aan derden worden verstrekt;
- Hoe lang we de persoonsgegevens bewaren;
- Wat de rechten van ouders en leerlingen zijn.

Ouders worden beknopt, eenvoudig en begrijpelijk geïnformeerd. De informatie is niet voor tweeërlei uitleg vatbaar. Deze informatie wordt zo mogelijk standaard in de schoolgids gepubliceerd, waarbij opgemerkt kan worden dat een digitale/elektronische vorm ook als schriftelijk beschouwd mag worden.

Wanneer persoonlijke informatie over een leerling of ouder wordt verwerkt, dan wordt dit middels een mailbericht aan de betreffende ouder kenbaar gemaakt.

### 5.2 Bijzondere gegevens en inzage recht

Bijzondere gegevens van leerlingen kunnen bestaan uit gevoelige informatie van leerlingen of ouders, die soms aanwijs-, of aantoonbaar is, maar soms ook vermoedens kunnen zijn. Denk bijvoorbeeld aan dossiervorming bij verdenking van misbruik of kindermishandeling. Dergelijke data worden wel opgenomen in leerling dossier. Het is echter in het belang van het kind om de ouders géén inzage te geven in die informatie en valt daarmee buiten bijvoorbeeld het inzage recht. Dit is echter een grote uitzondering waar terughoudend mee om moet worden gegaan.

### 5.3 Inzage in dossier- en persoonsgegevens

Het verzoek van inzage van de betrokkene kan schriftelijk, digitaal of mondeling worden gedaan. Een verzoek dient schriftelijk te worden vastgelegd door de locatieleider. Omschrijf wat het verzoek is en wanneer dat is ingediend.

In geval van een verzoek van inzage moet allereerst worden nagegaan of de verzoeker de wettelijk vertegenwoordiger is. (Ouder(s) of verzorger(s) moet(en) het gezag hebben over het kind).

- Een antwoord of weigering wordt altijd gemotiveerd in begrijpelijke taal.
- Inzage wordt alleen verleend in de gegevens van de betrokkenen.
- Persoonsgegevens van anderen dienen te worden verwijderd of afgeschermd.

Er is geen inzage mogelijk wanneer dat in het belang van het kind is, zoals in 5.2 omschreven.

### 5.4 Verwerkingsregister

CBS Molenwaard heeft als verantwoordelijke ook de verplichting op een verwerkingsregister op te stellen en te onderhouden. De versie schooljaar 2018-2019 treft u in de bijlage.



## 6. Publiceren beeldmateriaal en/of persoonsgegevens

In het kader van ouderbetrokkenheid, informatievoorziening naar de ouders en PR wordt maandelijks onze nieuwsbrief verstuurd. Daarin worden ouders geïnformeerd over het reilen en zeilen van de schoolactiviteiten. Daarnaast worden op onze schoolsite regelmatig foto's vertoond van onze activiteiten op school. Inzake de publicatie gelden de AVG-regels:

- Ouder(s)/verzorger(s) van leerlingen jonger dan 16 jaar dienen toestemming te hebben gegeven voor het publiceren van dit beeldmateriaal op de schoolsite en vermelding van hun kind(eren) in onze maandbrief;
- Op school is een zichtbaar document van toestemming door de betreffende ouders aanwezig;
- Ouder(s)/verzorger(s) kunnen te allen tijde de toestemming tot publicatie schriftelijk intrekken;
- Toestemming moet vrij en niet onder druk gegeven zijn;
- De leerling of ouder/verzorger mag niet benadeeld worden als er geen toestemming gegeven wordt;
- De toestemming moet ondubbelzinnig zijn. Het moet dus volstrekt helder zijn dát er toestemming is verleend;
- Er mag niet worden uitgegaan van het principe 'wie zwijgt, stemt toe';
- De school vraagt toestemming voor specifieke verwerkingen met een specifiek doel.

De scholen van CBS Molenwaard hebben gekozen voor een eenmalig verzoek tot toestemming voor de publicatie van beeldmateriaal voor meerdere activiteiten gedurende het schooljaar. Dit verzoek zal aan alle ouders aan het begin van het schooljaar worden gedaan. Opgelet moet worden dat van alle ouders een respons moet worden ontvangen.

De school zorgt voor het beschermd/beveiligd opslaan en voorkomt misbruik van het beeldmateriaal; CBS Molenwaard heeft technische en organisatorische maatregelen genomen om het beeldmateriaal van onze leerlingen te beschermen.

We hebben daarin de keuze te publiceren op het algemene deel van onze site, of achter het private deel waarvoor moet worden ingelogd. Dit private deel is met https beveiligd. De beheerder bepaalt in overleg met de leerkracht en of locatieleider waar een bericht of foto gepubliceerd wordt.

## 7. Functionaris gegevensbescherming

Elke schoolbestuur is verplicht een 'functionaris gegevensbescherming' (FG) aan te stellen.

De werkzaamheden van de FG zijn de navolgende:

- De FG werkt samen met en treedt op als contactpersoon met de Autoriteit Persoonsgegevens (AP);
- De FG is onze telefonische helpdesk bij vragen over de AVG;
- De FG verzamelt informatie, maakt analyses, controleert, informeert, adviseert en geeft aanbevelingen in de naleving van de AVG;
- Hij/zij informeert en adviseert de teamleden over de verplichtingen die voortvloeien uit de AVG;
- De FG ziet toe op de naleving van de AVG, het gegevensbeschermingsbeleid van CBS Molenwaard en het toewijzen van AVG-verantwoordelijkheden binnen de organisatie.

CBS Molenwaard heeft via Groenendijk Onderwijsconsultancy (GOC) de beschikking over een FG in de persoon van dhr. Bert Dasselaar. GOC is bekend met de onderwijssector en de nationale en Europese privacywet en -regelgeving over gegevensbescherming. Tevens heeft zij begrip van de gegevensverwerking binnen de onderwijsorganisatie en van informatiebeveiliging.

Jaarlijks wordt de uitvoering van de AVG binnen onze scholen met de FG besproken.

De FG is niet aansprakelijk voor een overtreding van de AVG binnen een organisatie.

## BIJLAGE 1: Gevraagde direct verzamelde persoonsgegevens

Gegevens	Doel	Categorie	Waar/wanneer
<b>NAW-gegevens leerling</b> Naam Adres Woonplaats Geslacht	Basis voor registratie/inschrijving	Administratie	Aanmeldingsformulier
<b>BSN</b>	Verificatie registratie in landelijkstelsel	Administratie	Aanmeldingsformulier
<b>Geb. datum leerling</b>	Indeling van groep en telling	Administratie	Aanmeldingsformulier
<b>Medische gegevens lln.</b> Allergie Beperkingen	Zo nodige begeleiding, medicatieverstrekking <i>(vervolgstappen protocol medicijnverstrekking)</i>	Zorg	Aanmeldingsformulier
<b>Voorschoolse educatie</b>	Overdracht en voorinfo	Ontwikkeling	Aanmeldingsformulier
<b>Nationaliteit</b>	Inschaling weging van lln.	Administratie	Aanmeldingsformulier
<b>NAW-gegevens ouder(s)/verzorger(s)</b> Naam Adres Woonplaats Telefoonnummer Mailadres	Inzake oudercontacten	Contacten	Aanmeldingsformulier
<b>Opleiding ouder(s)/verzorger(s)</b>	Inschaling weging van leerling	Administratie	Aanmeldingsformulier
<b>Beroep ouder(s)/verzorger(s)</b>	Inzake excursies of gastlessen	Ouder-betrokkenheid	
<b>Kerkgenootschap</b>	Monitoring	Administratie	
<b>Noodcontacten</b>	In geval van nood te benaderen	Zorg	aanmeldingsformulier
<b>Huisarts en verzekering</b>	In geval van nood te benaderen	Zorg	aanmeldingsformulier
<b>Burgerlijke staat ouder(s)/verzorger(s)</b>	Inzake dubbele contacten ouders	Administratie	aanmeldingsformulier

**BIJLAGE 2: Gevraagde indirect verzamelde persoonsgegevens**

Gegevens	Doel	Waar/wanneer
<b>Ontwikkeling voorschool</b>	Inschatting beginsituatie voor optimale overgang	Overdracht voorschool
<b>Logopedische, fysio, ontwikkeling</b>	Monitoring ontwikkeling lln.	Contact met logopediste
<b>Ontwikkeling van de leerling bij tussentijdse instroom</b>	Goede inschatting en indeling van groep	Dossier opvraag vorige school
<b>Informatie betreffende ouder(s)/verzorger(s)</b>	Heldere beeldvorming van thuissituatie	Via social media

### **BIJLAGE 3: Brief ouder(s)/verzorger(s), verzoek tot toestemming inzake publiceren beeldmateriaal en vermelding in nieuwsbrief en/of schoolsite**

**Betreft AVG: toestemmingsverklaring ouders.**



Geachte ouder(s)/verzorger(s),

Middels onze nieuwsbrief en onze schoolsite wordt u geïnformeerd over onze schoolactiviteiten. Door het schooljaar heen kunnen dat diverse activiteiten zijn, waarbij uw kind(eren) betrokken is/zijn en waarvan foto's en tekstberichten worden gepubliceerd.

De wet 'algemene verordening gegevensbescherming' geeft aan dat we als school dergelijke berichten en foto's niet zonder toestemming van de betrokken persoon, of in deze situatie wanneer betrokkenen jonger zijn dan 16 jaar van de ouder(s)/verzorger(s), mogen publiceren.

Met dit verzoek tot toestemming wordt u in de gelegenheid gesteld wel of geen toestemming te geven voor het publiceren van tekstbericht in de nieuwsbrief waarin uw kind kan worden genoemd, of foto's op onze schoolsite waar ook uw kind(eren) is/zijn te zien, of het delen van de groepslijst van de groep van uw kind aan de groepsgenoten.

Het zal steeds gaan om tekstberichten en of foto's die te maken hebben met schoolactiviteiten die door school zijn georganiseerd.

Er wordt tevens verschil gemaakt tussen publicatie in het publieke deel of het private deel (achter de inlog) van onze schoolsite.

Daarnaast wordt een dergelijke toestemming gevraagd voor publicatie van dergelijke activiteitenfoto's in de regionale of plaatselijke kranten.

Wettelijk dient onze school bij plaatsing van foto's en berichten een tastbare toestemmings-verklaring in bezit te hebben.

We vragen daarom alle ouders met nadruk bijgaand formulier in te vullen en af te geven op school. Tijdens de oudergespreksavonden op 15 en 19 november a.s. creëren wij hiervoor de gelegenheid. Wij bieden u het formulier aan ter ondertekening en verzamelen ze meteen.

Zo streven wij zorgvuldig om te gaan met uw persoonsgegevens en vragen ook u dit te doen door terughoudend te zijn bij het delen of online plaatsen van foto's/filmmateriaal die u maakt bij schoolactiviteiten.

Met vriendelijke groet,

Renske de Jong, Jaap-Joost Melse, Denise Versluis  
Locatieleiders CBS Molenwaard

**Verklaring van publicatie foto's en tekstberichten en bewaren van dossiers.**

De ouders/verzorgers van: ..... in groep .....

..... in groep .....

..... in groep .....

	Wij geven toestemming	Wij geven geen toestemming
Publicatie van foto's met uw kinderen daarop in het publiek sitedeel.		
Publicatie van foto's met uw kinderen daarop in het private sitedeel.		
Plaatsing van foto's met uw kinderen daarop in een regionale of plaatselijke krant.		
Tekstbericht in de nieuwsbrief met uw kinderen daarin genoemd.		
Delen van de groepslijst met NAW-gegevens aan groepsgenoten.		
Bewaren van het dossier van uw kind langer dan 5 jaar na afscheid van de school.		

Datum: .....

Naam: .....verklaart naar waarheid te hebben ingevuld.

Ondertekening:

#### **BIJLAGE 4: AVG in de schoolgids**

Binnen onze school maken we veel gebruik van diverse gegevens van onze leerlingen. Dit begint al bij de inschrijving als de persoonsgegevens van onze leerlingen en de ouders worden gevraagd en verwerkt in onze administratie. In de loop van de schooljaren worden rapporten, verslagen en notities opgemaakt, met daarin informatie over de ontwikkeling van onze leerlingen. Daarnaast doen we verslag van onze activiteiten in de nieuwsbrief en op onze website. Zo is er binnen onze school en naar buiten druk dataverkeer van gegevens en informatie over onze leerlingen, en dus ook over uw kind(eren).

De omgang met deze gegevens moet zorgvuldig gebeuren om misbruik of datalekken te voorkomen. De zorgvuldige omgang met dergelijke data is vastgelegd in de AVG (Algemene Verordening Gegevensbescherming). Deze verordening geeft strikte regels aan die we bij verwerking van gegevens moeten hanteren.

Voor onze leerlingenadministratie gebruiken we de basis persoonsgegevens van onze leerlingen, zoals de naam, het adres, de geboortedatum en het BSN-nummer. Voor de contacten met thuis gebruiken we de namen, het telefoonnummer en emailadres van de ouders.

Om met zorg zo goed mogelijk aan te sluiten bij de behoeften van onze leerlingen worden medische of ontwikkelingsverslagen van bijv. een logopediste of arts gevraagd en bewaard. Voor noodsituaties wordt een noodcontact of de gegevens van de betreffende huisarts gevraagd. Deze gegevens worden alleen gedeeld met interne teamleden, of met externen die betrokken zijn bij de begeleiding of zorg van de betreffende leerling.

Wanneer de school bovenstaande gegevens voor andere doelen wil gebruiken, zal daarvoor toestemming worden gevraagd van de betrokkenen.

Onze school zorgt er voor dat we al deze gegevens naar de AVG-bepalingen verwerken en bewaren. Bij inschrijving op onze school wordt toestemming van het gebruik van deze gegevens aan de ouders van de betreffende leerling gevraagd.

## BIJLAGE 5: Protocol beveiligingsincidenten

### Inleiding

Voor u ligt het protocol beveiligingsincidenten en datalekken. Dit protocol dient als verlengstuk van het Informatiebeveiligings- en privacy beleid.

Door middel van dit protocol kan er professioneel en adequaat worden gehandeld wanneer er sprake is van een beveiligingsincident en/of een datalek. Door het doorlopen van de juiste procedures worden incidenten op een correcte juridische wijze afgehandeld. Tevens dient dit protocol als ondersteuning voor het voorkomen van beveiligingsincidenten en datalekken.

Dit protocol informatiebeveiliging en datalekken is van toepassing voor alle medewerkers, externen, ouders en leerlingen van CBS Molenwaard.

In dit protocol wordt er gebruikt gemaakt van een aantal termen. Deze zijn nader uitgewerkt.

Gebruikte termen:

- **Beveiligingsincident;** een beveiligingsincident is een gebeurtenis die er voor zorgt of zou kunnen zorgen dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatievoorziening wordt aangetast.
- **Informatievoorziening;** het geheel van mensen, middelen en maatregelen, gericht op de informatiebehoefte van de organisatie.
- **Datalek;** een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden, et cetera). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- **Betrokkene;** de persoon van wie de persoonsgegevens zijn gelekt.

### Wet- en regelgeving

Sinds de invoering van de Wet meldplicht datalekken op 1 januari 2016 zijn ook scholen verplicht om melding te maken bij de Autoriteit Persoonsgegevens wanneer er sprake is van een (ernstig) datalek. Scholen riskeren een boete wanneer zij dit verzaken.

Een voorbeeld van een datalek is als er bij een inbraak servers worden ontvreemd waarop persoonsgegevens zijn opgeslagen. Dit kan gaan om (gevoelige) leerling informatie, maar ook gegevens van medewerkers kunnen persoonsgegevens zijn. Ook het verlies van een smartphone van een leerkracht met daarop de informatie van een klas kan worden aangemerkt als een datalek. Bij een datalek 'is' of 'kan niet worden uitgesloten dat' er persoonsgegevens verloren zijn gegaan.

De meldplicht voor datalekken geldt alleen bij het lekken van persoonsgegevens. En geldt voor de verantwoordelijke van de persoonsgegevens, het schoolbestuur. In veel gevallen kan de school het verwerken van persoonsgegevens uitbesteden aan derden. Deze leveranciers zoals uitgevers of distributeurs treden op als verwerkers van de persoonsgegevens namens de school. Met verwerkers moet een school ook afspraken maken over het melden van datalekken. Dit kan worden opgenomen in de verwerkersovereenkomst.

Bij een datalek, moet binnen 72 uur na ontdekking van het lek melding worden gedaan bij de Autoriteit Persoonsgegevens.



### Afspraken met leveranciers

In een verwerkersovereenkomst worden afspraken gemaakt met betrekking tot de verwerking van de persoonsgegevens namens de school. Afspraken over datalekken worden daarin ook geregeld. Onderwerpen die in deze overeenkomst moeten worden opgenomen zijn:

- Hoe informeer je elkaar over datalekken, en zorg ook voor bereikbaarheid tijdens bijvoorbeeld het weekend en vakanties.
- Wie doet de melding bij de Autoriteit Persoonsgegevens.
- Welke informatie gegevens de bewerker moet geven bij een datalek.
- Welke informatie nodig is voor het doen van een melding, en dat je elkaar informeert over de melding (maak afspraken dat je een kopie van de melding krijgt of doorstuurt).
- De tijd waarbinnen de bewerkers de gegevens moet aanleveren.
- Wie de communicatie met de gebruikers voor haar rekening neemt als dat nodig is.



De afspraken – waaronder de afspraken over datalekken- met de verwerker(s) dienen schriftelijk te worden gemaakt.

## Werkwijze

Om een goed en correct databeveiligingsprotocol te kunnen uitvoeren zijn er een aantal randvoorwaarden. Deze randvoorwaarden betreffen het informatiebeveiligings- en privacy beleid. Deze moet actueel zijn, regelmatig geëvalueerd en zo nodig worden bijgesteld.

Daarnaast is het van belang dat er een actuele gedragscode over het aanvaardbaar gebruik van bedrijfsmiddelen van toepassing is. En een zgn. 'online protocol' met daarin gedragsregels voor het gebruik van ICT, internet en social media.

## De vier rollen

Er zijn ten minste vier rollen die onderscheiden moeten worden om een beveiligingsincident en/of datalek succesvol af te handelen:



▪ **Ontdekker (medewerker)**; degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.



▪ **Meldpunt (servicedesk)**; een centrale locatie waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.



▪ **Melder (functionaris gegevensbescherming)**; degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.



▪ **Technicus (security officer/ict coördinator)**; degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

## De zeven stappen

### 1. Ontdekken

De **ontdekker** merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De **ontdekker** verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij het **meldpunt** via de algemeen directeur a.vanooijen@cbsmolenwaard.nl

### 2. Inventariseren

Het **meldpunt** bepaalt of er voldoende informatie omtrent het beveiligingsincident bekend is. Zo niet, dan zet hij aanvullende vragen uit bij de **ontdekker** en/of de **technicus**.

De volgende informatie wordt vastgelegd in incidentenregister:

- Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
- Datum/periode van het beveiligingsincident
- Aard van het beveiligingsincident
- Wanneer van toepassing (bij een datalek):
  - Omschrijving van de groep betrokkenen
  - Aantal betrokkenen
  - Type persoonsgegevens in kwestie
  - Worden de gegevens binnen een keten gedeeld?

### 3. Beoordelen

Wanneer het **meldpunt** voldoende informatie heeft verzameld, en een datalek vermoed, stuurt deze de **melder** een verzoek om de verzamelde informatie te bekijken. De **melder** beoordeelt de feiten om te bepalen of een melding aan de Autoriteit Persoonsgegevens en/of betrokkenen vereist is.

De volgende informatie wordt vastgelegd door de **melder**:

- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- Wordt het datalek gemeld aan de Autoriteit Persoonsgegevens? Waarom niet?
- Wordt het datalek aan betrokkenen gemeld? Waarom niet?
- Hoe worden meldingen gedaan? Wat is de inhoud van de melding?

Onderstaand schema kan gebruikt worden om de ernst van het incident vast te stellen.



### 4. Repareren

De **technicus** (\*intern of extern) wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De **technicus** legt onderstaande vast:

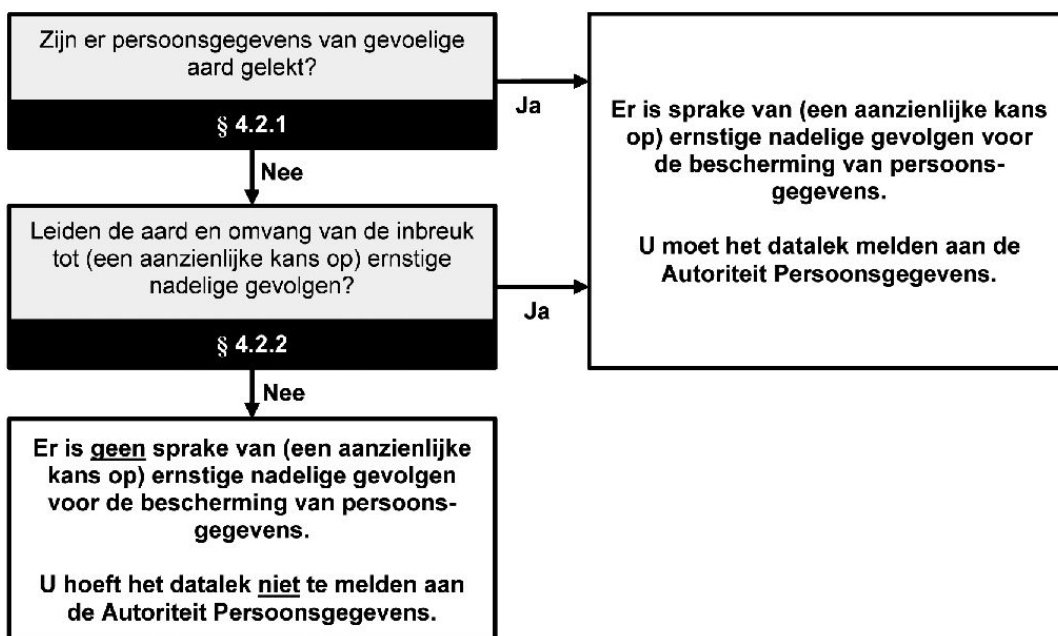
- Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voor zover de oorzaak bekend is.
- Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Zijn gegevens gepseudonimiseerd? Hoe zijn de gegevens versleuteld?

## 5. Melden

Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de [melder](#) dit binnen **72 uur** doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij de Autoriteit Persoonsgegevens.

Om te kunnen inschatten of er sprake is van ernstige nadelige gevolgen moet [de melder](#) rekening houden met diverse factoren. Bijvoorbeeld met informatie over het type persoonsgegevens, de hoeveelheid en de mogelijkheid voor ernstige nadelige gevolgen voor de betrokkene.

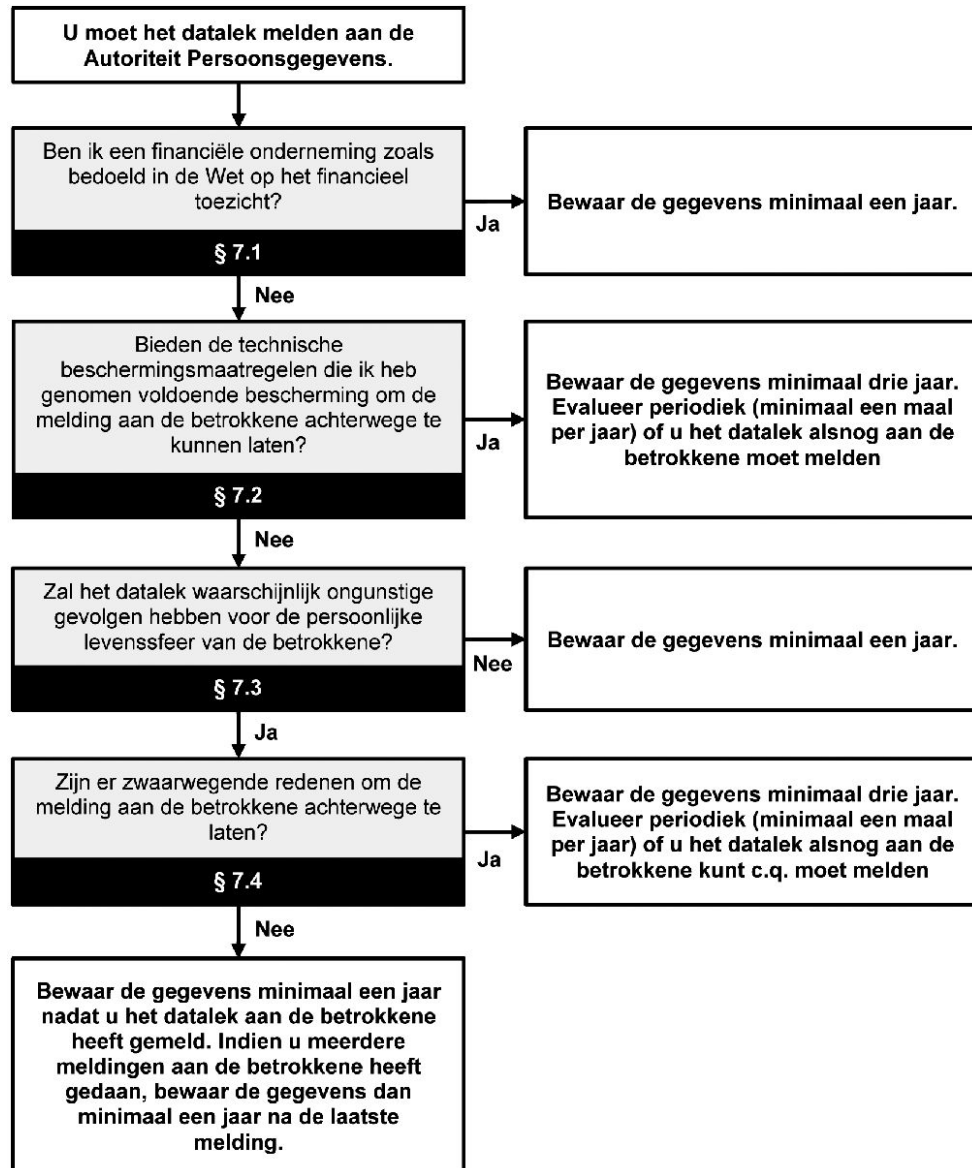
Van die ernstige nadelige gevolgen, of de kans daarom, is bijvoorbeeld sprake wanneer er heel veel gegevens van een betrokkene of gegevens van heel veel betrokkenen gelekt zijn. Maar ook wanneer de gelekte gegevens 'gevoelig' zijn zoals bijvoorbeeld bijzondere persoonsgegevens over gezondheid, over de financiële situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene (denk aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).



Afbeelding afkomstig van '[Richtsnoeren meldplicht datalekken](#)' van de Autoriteit Persoonsgegevens

## 6. Vastleggen

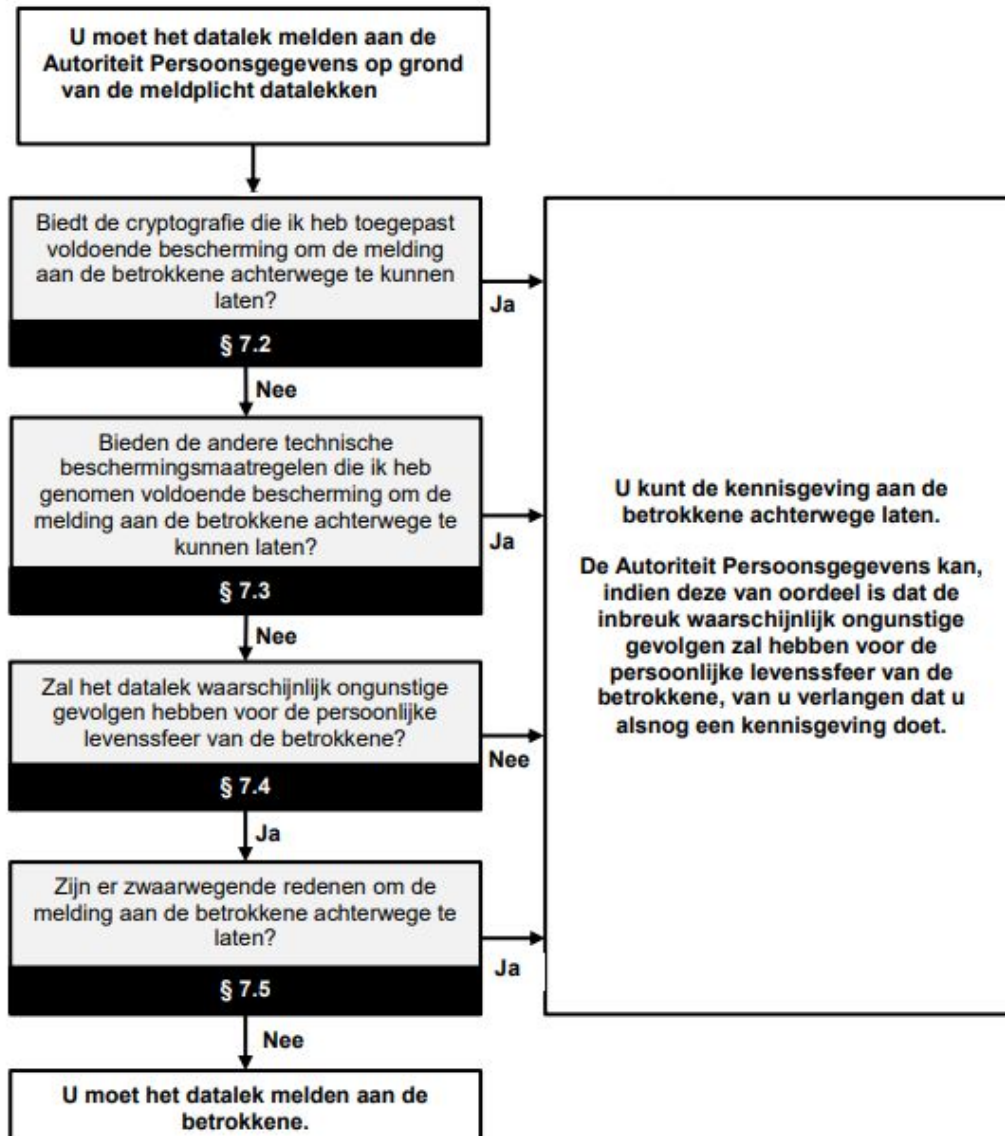
Het [meldpunt](#) is verantwoordelijk voor de juiste afwikkeling van alle verworven informatie en documentatie over het incident. Onder afwikkeling wordt mede verstaan, het informeren van de [ontdekker](#) en archiveren van alle documentatie en bewaren volgens onderstaand schema.



Afbeelding afkomstig van '[Richtlijn meldplicht datalekken](#)' van de Autoriteit Persoonsgegevens

## 7. Informeren betrokkene: leerling en/of de ouders

Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers, leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan er van worden uitgegaan dat het lekken van gevoelige aard gelekt gemeld moet worden bij de betrokkenen. Let op: als er persoonsgegevens zijn gelekt maar die zijn beveiligd of versleuteld, en de gelekte data zijn onbegrijpelijk of ontoegankelijk voor anderen, dan hoeft dat toch niet aan betrokkenen te worden gemeld. Denk aan het lekken van een beveiligde én versleutelde database met gebruikersnamen en wachtwoorden.



Afbeelding afkomstig van '[Richtlijnen meldplicht datalekken](#)' van de Autoriteit Persoonsgegevens

## Communicatie

### Communicatie betrokkenen en pers bij datalekken

Wanneer er sprake is van een ernstig datalek met gevolgen voor betrokkene, dan moet de betrokkene ook worden geïnformeerd over het datalek. Daarna is het vaak een kwestie van tijd voordat de pers berichtgeving daarover naar buiten brengt.

Om dit te monitoren zijn er een aantal vuistregels opgesteld:

1. **Stel een woordvoerder aan**

Door een centraal persoon aan te stellen als woordvoerder blijft de communicatie met betrokkenen en/of pers beheersbaar. Dit kan een verantwoordelijke zijn binnen het MT of de directie van de betreffende school.

2. **Hou geen informatie binnen ‘vier muren’**

Het is onmogelijk om te verwachten dat de communicatie over een datalek binnen vier muren blijft. Wees open in de informatieverstrekking, op die manier is berichtgeving helder en overzichtelijk. Deel daarom de naar buiten gebrachte informatie ook via de website of andere communicatiekanalen.

3. **Meld informatie zodra dit mogelijk is**

Update berichtgeving regelmatig. Voorkom dat er speculaties uit de hand lopen. Meld het ook als er géén nieuwe informatie is.

4. **Social Media**

Blijf zelf actief op social media. Voorkom speculaties door te reageren op onjuistheden en verwijs naar de officiële berichtgeving op bijvoorbeeld de website.

### Signalen van derden over mogelijk datalek

Signalen van derden over een mogelijk datalek kunnen zeer divers van aard zijn. Zorg dat er altijd adequaat op wordt gereageerd om mogelijke gevolgen te beperken of te voorkomen.

1. **In kaart brengen mogelijk datalek**

Breng het mogelijke datalek in kaart. Is er sprake van een datalek? Wat is de omvang van het datalek? Zijn er daadwerkelijk persoonsgegevens verloren gegaan? Inventariseer of er sprake is van verlies van gegevens of dat er sprake is van een onrechtmatige verwerking.

2. **Onderzoek mogelijk datalek**

Onderzoek het mogelijke datalek als zijnde een ‘reguliere ontdekking’ en werk de procedure af zoals eerder in dit protocol beschreven.

3. **Informeren diverse partijen**

Breng de Autoriteit Persoonsgegevens op de hoogte wanneer de meldplicht op het datalek van toepassing is. Afhankelijk van de ernst van het lek; informeer ook eventueel de betrokkenen en derden over het ontdekken van het datalek. Geef aan of, en welke gegevens daarbij betrokken waren en welke gevolgen dit heeft.

## Controle en rapportage

Twee maal per jaar analyseert het meldpunt samen met de Functionaris Gegevensbescherming de geregistreerde meldingen van beveiligingsincidenten en datalekken. Hierbij wordt rekening gehouden met:

- eventuele structurele ontwikkelingen
- de noodzaak bestaat om maatregelen te nemen om herhaling te voorkomen

Het schoolbestuur wordt geïnformeerd over de uitkomsten van de analyse.

## **BIJLAGE 6: Online Protocol**

### **Inleiding**

De huidige 'millennials' en de jonge generatie kunnen zich geen wereld voorstellen zonder. Internet en social media. Ze nemen een belangrijke rol in, niet alleen in het leven van de leerlingen maar ook van onderwijzend personeel en andere medewerkers. Internet kan bijdragen om lessen leuker en uitdagender te maken, maar brengt ook risico's met zich mee. Het is belangrijk om iedereen te beschermen tegen pesten, ongewild delen van foto's of gegevens en andere bedreigingen van het internet.

Dit 'online protocol' zorgt ervoor dat leerlingen en medewerkers bewust zijn van de gevaren en daardoor op een goede manier met het internet en sociale media om kunnen gaan. Er kan in de klas, of thuis worden besproken wat er wel mogelijk is op internet en wat 'not done' is.

De afspraken zijn van toepassing op alle leerlingen van CBS Molenwaard, voor het gebruik van sociale media op mobiele telefoons en andere (mobiele) devices. Niet alleen op school en in de klas, maar ook in het mediagebruik buiten de school.

Onder het gebruik van sociale media wordt verstaan; het gebruik van programma's waarmee online informatie kan worden opgezocht, gedeeld en gepresenteerd. Denk bijvoorbeeld aan Facebook, Twitter, Instagram, YouTube, Snapchat maar ook alle (nieuwe) hiermee vergelijkbare programma's en apps.

We hopen dat dit protocol een goed richtsnoer is en voor iedereen begrijpelijk is. Zodat iedereen op een leuke en veilige manier gebruik kan maken van internet en de social media.

De directie

\*, \* april 2018

## **Reglement**

### **Toepassing**

Dit protocol is bedoeld voor alle *betrokkenen* die deel uitmaken van CBS Molenwaard. Onder betrokkenen wordt verstaan: alle medewerkers, leerlingen, ouders / verzorgers en mensen die op een andere manier verbonden zijn aan CBS Molenwaard.

De richtlijnen in dit protocol hebben enkel betrekking op school gerelateerde berichten of wanneer er een overlap is tussen school, werk en privé, onafhankelijk van de plaats waar zij hun sociale media gebruiken.

### **Uitgangspunten**

1. CBS Molenwaard onderkent het belang van sociale media.
2. Dit protocol draagt bij aan een goed en veilig school- en onderwijsklimaat;
3. Dit protocol bevordert dat de instelling, medewerkers, leerlingen en ouders op internet en de sociale media communiceren in het verlengde van de missie en visie van de onderwijsinstelling en de reguliere fatsoensnormen. In de regel betekent dit dat we respect voor de school en elkaar hebben en iedereen in zijn waarde laten;
4. De gebruikers van sociale media dienen rekening te houden met de goede naam van de school en van een ieder die betrokken is bij de school;
5. Het protocol dient de onderwijsinstelling, haar medewerkers, leerlingen en ouders tegen zichzelf en anderen te beschermen tegen de mogelijke negatieve gevolgen van de sociale media.

### **Sancties bij overtreding**

Wanneer geconstateerd wordt dat de afspraken niet worden nageleefd, wordt dit eerst met de betrokkene besproken. Bij een ernstige overtreding kan de directie van CBS Molenwaard besluiten een maatregel op te leggen.

1. Medewerkers die in strijd handelen met dit protocol maken zich mogelijk schuldig aan plichtsverzuim. Alle correspondentie omtrent dit onderwerp wordt opgenomen in het personeelsdossier.
2. Afhankelijk van de ernst van de uitlatingen, gedragingen en gevolgen worden naar medewerkers toe rechtspositionele maatregelen genomen welke variëren van waarschuwing, schorsing, berisping, ontslag en ontslag op staande voet;
3. Leerlingen en / of ouders / verzorgers die in strijd met dit protocol handelen maken zich mogelijk schuldig aan verwijtbaar gedrag. Alle correspondentie omtrent dit onderwerp wordt opgenomen in het leerlingendossier.
4. Afhankelijk van de ernst van de uitlatingen, gedragingen en gevolgen worden naar leerlingen en / of ouders / verzorgers toe maatregelen genomen welke variëren van waarschuwing, schorsing en verwijdering van school.
5. Indien de uitlating van leerlingen en / of ouders / verzorgers en medewerkers mogelijk een strafrechtelijke overtreding inhoudt zal door CBS Molenwaard aangifte bij de politie worden gedaan.

### **DNS veiligheid-shield (filter)**

Op de internetrouter van de school is een dns-filter ingeschakeld. Dit filter is geïnstalleerd met de bedoeling om zoveel als technisch mogelijk de meeste websites die bekend staan als porno, racisme, proxy-omleiding en phishing te blokkeren.



## **Internet en gebruik schoolnetwerk**

### **Omgangsvormen**

We behandelen elkaar netjes en met respect, en laten iedereen in zijn waarde. Daarom pesten, kwetsen, stalken, bedreigen, beschadigen we elkaar niet en maken we elkaar niet zwart.

### **Smartphone / Telefoongebruik tijdens de les**

[De leerkracht moet vooraf toestemming geven om een mobiele telefoon of sociale media in de les te gebruiken. Tijdens toetsen gelden aangepaste regels.]

of:

[Het meenemen van mobiele telefoon en daarmee vergelijkbare communicatieapparatuur op school is [wel/niet] toegestaan. Een leerkracht kan in verband met het leerproces leerlingen toestemming geven om een mobiele telefoon mee te nemen en te gebruiken in de klas.]

### **Acceptabele doeleinden**

Internet en sociale media worden alleen gebruikt voor acceptabele doeleinden. Het is daarom niet toegestaan om op school:

1. sites te bezoeken of informatie te downloaden en te verspreiden die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend zijn.
2. hacken en ongeoorloofd toegang te krijgen tot niet-openbare sites of programma's;
3. informatie, foto's of video's te delen waarvan duidelijk is dat die niet bedoeld zijn om verder te verspreiden. Hou je wachtwoorden geheim;
4. verzonden berichten versturen of een fictieve naam gebruiken als afzender;
5. iemand lastig vallen, te achtervolgen of te 'flamen'.

Als iemand over de voorgaande punten informatie krijgt aangeboden, wordt dat gemeld aan de leerkracht of de directeur.

### **Gebruik schoolnetwerk**

Bij gebruik van internet en sociale media via het netwerk van de school, mag dat de kwaliteit van het (draadloze) netwerk niet in gevaar brengen of schade aan personen of instellingen veroorzaken. Het hacken, overmatig downloaden of overbelasten van het netwerk is verboden.

### **Spelregels op internet voor leerlingen**

#### **E-mail:**

- Geef nooit persoonlijke informatie door op internet, zoals namen, adressen en telefoonnummers, zonder toestemming van de leerkracht.
- Leg nooit verdere contacten met iemand zonder toestemming van je leerkracht.
- Verstuur bij e-mail berichten nooit foto's van jezelf of anderen zonder toestemming van je leerkracht.
- Beantwoord nooit e-mail waarbij je je niet prettig voelt of waar dingen in staan waarvan je weet dat dat niet hoort.
- Verstuur ook zelf dergelijke mailtjes niet.
- Verstuur geen verzonden berichten of met fictieve namen als afzender.
- Val niet iemand lastig door overmatig veel berichten te zenden.

#### **Internet:**

- Bezoek geen andere soorten sites dan die door je leerkracht zijn toegestaan.
- Spreek van tevoren met je leerkracht af wat je op internet wilt gaan doen.
- Vertel het je leerkracht als je informatie tegenkomt waardoor je je niet prettig voelt of waarvan je weet dat dat niet hoort.

- Internet wordt gebruikt voor het opzoeken van informatie die je nodig hebt voor je werkstuk. Anders spreek je van tevoren af met je leerkracht wat je op internet wil gaan doen.
- Hacken en ongeoorloofd toegang krijgen tot niet-open sites of programma's is niet toegestaan.
- Overmatig downloaden of overbelasten van het netwerk is niet toegestaan.

### **Spelregels voor leerkrachten**

De leerkracht wordt geacht ook voor e-mail- en internetgebruik een voorbeeldfunctie te vervullen.

#### **E-mail:**

- Ook voor e-mail geldt het briefgeheim, maar op grond van hun pedagogische verantwoordelijkheid mogen de leerkrachten e-mail van leerlingen bekijken.

#### **Internet:**

- Voor de leerling moet duidelijk zijn welke sites zijn toegestaan:
  - a. door voorselectie (onderwijs-portals, digilessen, selectie ICT-er of leerkracht),
  - b. door duidelijke, door de leerkracht gegeven, aanwijzingen v.w.b. de inhoud.
- Internet wordt gebruikt voor opbouwende educatieve doeleinden.
- Er wordt aan de leerlingen uitgelegd waarom zij bepaalde sites wel of niet mogen bekijken.
- De leerkracht draagt zorg voor een omgeving waarin leerlingen open kunnen vertellen wanneer zij op een ongewenste, onbedoelde site komen. Het is meestal immers niet hun schuld.
- Regels en wetten met betrekking tot copyright worden in acht genomen.
- Informatie die terug te voeren is op leerlingen mag niet op het openbare deel van het net terechtkomen.
- De leerkracht gebruikt een veilig wachtwoord, d.w.z. minimaal 8 karakters, minimaal één hoofdletter, één leesteken en één cijfer; de persoonlijke mobiele telefoon moet beschikken over een vergrendelingscode.

## **Social media**

### **Verantwoordelijkheid bij ‘delen’**

Iedereen is verantwoordelijk voor wat hij/zij zelf plaatst op sociale media, en kan daarop aangesproken worden. Ook het doorsturen (*forwarden*) en herplaatsen (*retweeten*) zijn handelingen waar je op aangesproken kunt worden.

### **Bekendheid social media platform**

Zorg dat je weet hoe de sociale media werken voordat je ze gebruikt, zorg dat de instellingen goed staan en je niet meer informatie deelt dan je wilt. Alles wat wordt gecommuniceerd via internet en sociale media blijft nog lang vindbaar.

### **Goede naam van CBS Molenwaard**

Bij het gebruik van internet en sociale media houden we rekening met de goede naam van CBS Molenwaard en iedereen die daarbij betrokken is zoals leerkrachten, onderwijsondersteunend personeel en ouders.

### **Verstandige omgang ‘socials’**

We helpen elkaar om goed en verstandig met sociale media om te gaan en we spreken elkaar daarop aan. Als dat niet lukt, dan vragen we daarvoor hulp aan onze leerkracht.

### **Privacy van anderen**

We respecteren elkaars privacy. Bij het gebruik van internet en sociale media worden er daarom geen informatie, foto's of video's verspreid over anderen, als zij daar geen toestemming voor hebben gegeven, of als zij daar negatieve gevolgen van kunnen ondervinden.

### **‘Vrienden’ maken / uitnodigen**

[Het leggen van contact, het volgen van elkaar of ‘vriend worden’, is een bewuste keuze waar goed over nagedacht is. We weten wie de andere persoon is.]

en/of:

[Leerlingen en medewerkers van school worden geen ‘vrienden’ met elkaar op sociale media, tenzij het gaat om een door de medewerkers gebruikt professioneel account (waar geen persoonlijke informatie over de medewerker op is geplaatst).]

### **Spelregels voor alle betrokkenen**

1. Het is medewerkers en leerlingen niet toegestaan om tijdens de lessen actief te zijn op sociale media tenzij door de schoolleiding respectievelijk leerkrachten hiervoor toestemming is gegeven.
5. Het is betrokkenen toegestaan om kennis en informatie te delen, mits het geen vertrouwelijke of persoonlijke informatie betreft en andere betrokkenen niet schaadt.
6. De betrokkene is persoonlijk verantwoordelijk voor de inhoud welke hij of zij publiceert op de sociale media.
7. Elke betrokkene dient zich ervan bewust te zijn dat de gepubliceerde teksten en uitlatingen voor onbepaalde tijd openbaar zullen zijn, ook na verwijdering van het bericht.
8. Het is voor betrokkenen niet toegestaan om foto-, film- en geluidsopnamen van school gerelateerde situaties op de sociale media te zetten tenzij betreffende persoon of personen hier uitdrukkelijk toestemming voor plaatsing hebben gegeven;

9. Medewerkers die een persoonlijk account hebben en gebruiken op social media moeten zich er van bewust zijn dat ze ook medewerker zijn van de school. Gezond verstand bij het plaatsen van berichten en toelaten van “vrienden” is leidraad bij het privégebruik van privé account.
10. Alle betrokkenen nemen de fatsoensnormen in acht. Als fatsoensnormen worden overschreden neemt de onderwijsinstelling passende maatregelen.

### **Spelregels voor leerkrachten en medewerkers**

1. Medewerkers hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media: privémeningen van medewerkers kunnen eenvoudig verward worden met de officiële standpunten van de onderwijsinstelling.
2. Indien een medewerker deelneemt aan een discussie die (op enigerlei wijze) te maken heeft met CBS Molenwaard, dient de medewerker te vermelden dat hij/zij medewerker is van CBS Molenwaard.
3. Als online communicatie dreigt te ontsporen dient de medewerker direct contact op te nemen met zijn/haar leidinggevende om de te volgen strategie te bespreken.
4. Bij twijfel of een publicatie in strijd is met deze richtlijnen neemt de medewerker contact op met zijn/haar leidinggevende.
5. Het is de medewerker toegestaan om school gerelateerde onderwerpen te publiceren mits het geen vertrouwelijke of persoonsgebonden informatie over de school, zijn medewerkers, leerlingen, ouders / verzorgers en andere betrokkenen betreft. Tevens mag de publicatie de naam van CBS Molenwaard niet schaden.

## BIJLAGE 7: Reglement Functionaris Gegevensbescherming

### Regeling taken en verantwoordelijkheden Functionaris voor Gegevensbescherming

#### Artikel 1: definities

AVG	Algemene Verordening Gegevensbescherming
FG	Functionaris voor gegevensbescherming zoals genoemd in artikel 37 van de AVG
Verwerkingsverantwoordelijke	Het bestuur van CBS Molenwaard
Verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, bedrijf, organisatie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (betrokkene) waarbij als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon
Verwerking van persoonsgegevens	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens
Personeel	Medewerkers in loondienst en/of extern ingehuurde medewerkers die in opdracht van de Verwerkingsverantwoordelijke werkzaamheden verrichten

#### Artikel 2: Taken

1. De FG heeft de volgende taken:

- a. het houden van toezicht op verwerkingen van persoonsgegevens;
  - b. toezicht op wijzigingen in bestaande verwerkingen en/of het aanleggen van nieuwe verwerkingen met persoonsgegevens binnen CBS Molenwaard;
  - c. geven van (ongevraagd) advies en doen van aanbevelingen over privacy in het algemeen en de toepassing van de AVG;
  - d. overleg met (de contactpersoon van) de Autoriteit Persoonsgegevens;
  - e. Organiseren, inrichten en/of onderhouden van het verwerkingsregister met alle verwerkingen persoonsgegevens binnen CBS Molenwaard;
  - f. OPTIONEEL: jaarlijks opstellen van een verslag van zijn werkzaamheden;
  - g. het (laten) afhandelen van klachten inzake privacy;
  - h. Overige door het bestuur of directie van CBS Molenwaard aan de FG opgedragen werkzaamheden aangaande privacy.
2. Het personeel meldt bij de FG alle (nieuwe) verwerkingen van persoonsgegevens alsmede eventuele incidenten met betrekking tot privacy.

### **Artikel 3: Bevoegdheden**

1. De FG is bevoegd, zo nodig met medeneming van de benodigde apparatuur, elke plaats in de gebouwen op de terreinen die bij CBS Molenwaard in gebruik zijn en waar persoonsgegevens worden verwerkt, te betreden.
11. De FG is bevoegd inlichtingen te vorderen van een ieder die onder gezag of in opdracht van CBS Molenwaard werkzaam is of overeenkomstig voor of namens CBS Molenwaard persoonsgegevens verwerkt.
12. De FG is bevoegd inzage te vorderen van zakelijke gegevens en bescheiden waarin persoonsgegevens zijn verwerkt.
13. De FG is bevoegd van de gegevens en bescheiden kopieën te maken.
14. Indien het maken van kopieën niet ter plekke kan gebeuren, is hij bevoegd de gegevens en bescheiden voor maximaal één werkdag mee te nemen.
15. De FG is bevoegd tot het geven van een opdracht tot
  - a. het aanmaken van een registratie van persoonsgegevens in overeenstemming met de AVG;
  - b. vernietiging van persoonsgegevens, waarvan de bewaartermijn is overschreden of indien de gegevensverwerking onrechtmatig is.
16. De FG is bevoegd zich te laten vergezellen en bijstaan door personen die daartoe door hem zijn aangewezen.
17. De FG maakt van de bevoegdheden als bedoeld in dit artikelen slechts gebruik voor zover dit redelijkerwijs voor de uitoefening van de taak noodzakelijk is.

### **Artikel 4: Weigering**

1. Een ieder, die werkzaam is bij en/of in opdracht werkt van de verantwoordelijke, is verplicht aan de FG medewerking te verlenen, die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden.
18. Indien de medewerking aan de uitoefening van de bevoegdheden van de FG zoals bedoeld in artikel 3, wordt geweigerd, kan CBS Molenwaard, op een met redenen omkleed verzoek, toestemming verlenen aan de FG de benodigde handelingen zelfstandig uit te voeren in weerwil van de weigering tot medewerking.
19. Het bestuur en/of directie van CBS Molenwaard wordt zo spoedig mogelijk in kennis gesteld over de uitvoering van het bepaalde in dit artikel.

### **Artikel 5: Geheimhouding**

1. De FG is verplicht tot geheimhouding van al hetgeen hem op grond van deze regeling bekend is geworden, tenzij de betrokkene in bekendmaking toestemt.

### **Artikel 6: Regeling**

1. Deze regeling wordt vastgesteld en gewijzigd bij besluit van de Verwerkingsverantwoordelijke.
20. Deze regeling treedt in werking op \*DATUM en zal intern aan het personeel bekend worden gemaakt door

\*

Vastgesteld door het bestuur van CBS Molenwaard op \*DATUM, versie \*VERSIENUMMER.