Handboek Informatiebeveiliging en Privacy

Stichting Bravoo
Kaatsheuvel, 14 juni 2019
Versie juli 2021
Versie februari 2022

Aanpassingen document:

- Naar aanleiding van de evaluatie door de werkgroep IBP op 13 juli 2021, zijn er een aantal kleine wijzigingen doorgevoerd. Dit document wordt met een samenvatting van de evaluatie doorgestuurd naar alle personeel, RvT en GMR.
- De Security Officer heeft in februari 2022 een aantal wijzigingen doorgevoerd m.b.t.

- Hfd.4 en Bijlage 4: Bijlage 4 is verwijderd en een gedeelte van die tekst is toegevoegd aan hfd.4 toestemming gebruik persoonsgegevens. De voorbeeldbrieven zijn weggehaald en de tekst aangepast omdat de toestemmingen voor leerlingen worden geregeld via het ouderportaal. Afbeelding toegevoegd van Parro/Parnassys.
- Hfd.4 en Bijlage 5: Bijlage 5 is verwijderd en een gedeelte van die tekst is toegevoegd aan hfd.4 onder toestemmingen voor medewerkers. Omdat de toestemmingen via Afas Insite zijn geregeld zijn de formulieren weggehaald en een voorbeeld van Afas Insite toegevoegd.
- Hfd.5 en bijlage 7b: Rechten van betrokkenen: toevoeging reactietermijn bij inzage van 4 weken.
- Bijlage 6: weggehaald, omdat de toestemming social media via digitaal ouderportaal loopt.
- Hfd.12: toevoeging beschrijving beveiligd mailen.
- Bijlage 9: data op toegangsmatrix Parnassys aangepast.
- Bijlagenummering aangepast in hele document vanwege het verdwijnen van bijlages 4 en 5

  Voorheen:
  Bijlage 1 Persoonsgegevens
  Bijlage 2 Privacyreglement
  Bijlage 3 Privacyverklaring
  Bijlage 4 Toestemming gebruik beeldmateriaal leerlingen
  Bijlage 5 Toestemming gebruik beeldmateriaal medewerkers
  Bijlage 6 Toestemming sociale media
  Bijlage 7 Procedure rechten van betrokkenen
  Bijlage 7a Inzage tabel rechten van betrokkenen
  Bijlage 7b Genomen stappen rechten van betrokken
  Bijlage 8 Protocol datalekken
  Bijlage 9 Toegangsmatrix
  Bijlage 10 Gedragscode ICT en Internet

  Nu:
  Bijlage 1 Persoonsgegevens
  Bijlage 2 Privacyreglement
  Bijlage 3 Privacyverklaring
  Bijlage 4 Gedragsprotocol voor ICT, social media en telefoon – versie leerlingen
  Bijlage 5 Procedure rechten van betrokkenen
  Bijlage 5a Inzage tabel rechten van betrokkenen
  Bijlage 5b Genomen stappen rechten van betrokkenen
  Bijlage 6 Protocol datalekken
  Bijlage 7 Toegangsmatrix
  Bijlage 8 Gedragscode ICT en Internet

Inhoudsopgave

Hoofdstuk 1 Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. De hoeveelheid informatie, waaronder persoonsgegevens, neemt toe door o.a. ontwikkelingen als gepersonaliseerd leren met ICT Het is belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. De afhankelijkheid van ICT en persoonsgegevens brengt nieuwe kwetsbaarheden en risico's met zich mee. Het goed regelen van informatiebeveiliging en privacy (afgekort tot IBP) in een IBP-beleid is noodzakelijk om de gevolgen van deze risico's tot een aanvaardbaar niveau te reduceren en de voortgang van het onderwijs en de bedrijfsvoering optimaal te kunnen waarborgen.
Hiervoor is er binnen Stichting Bravoo een IBP-beleidsplan opgesteld. Het IBP-beleidsplan is vastgesteld door de GMR en is te vinden via: https://www.stichtingbravoo.nl/beleid/privacy

Dit handboek is bedoeld als informatiebron voor alle medewerkers van Stichting Bravoo Hierin staan de afspraken die we met elkaar gemaakt hebben over informatiebeveiliging en privacy. Hierbij hebben wij naast de wettelijke basis, ook onze visie op onderwijs en onze normen en waarden als uitgangspunt genomen.

Hoofdstuk 2 De basis van de privacywetgeving

Privacy is een lastig en vaag begrip. Privacy op school gaat over de bescherming van gegevens over leerlingen, hun ouders en medewerkers. Dit wordt geregeld in de Algemene Verordening Gegevensbescherming (AVG). Als we praten over de AVG dan praten we over persoonsgegevens.

Wat zijn persoonsgegevens?

Een persoonsgegeven is informatie die direct iets over een persoon zegt of op een bepaalde manier herleidbaar is naar die persoon. Een andere manier om de term persoonsgegevens te omschrijven is: de gegevens waarmee je een specifiek persoon binnen een bepaalde groep kunt aanwijzen. Dat zijn bijvoorbeeld je naam, je adres en je geboortedatum. Bij een veelvoorkomende naam, zullen er meestal wat gegevens moeten worden gecombineerd om een specifieke persoon aan te wijzen. Dat verandert niets aan het feit dat een naam altijd een persoonsgegeven is. In **bijlage 1** is te zien met welke type persoonsgegevens je te maken kunt hebben.

Grondslagen voor verwerking van persoonsgegevens

Je mag niet zomaar persoonsgegevens bewaren, verspreiden, bewerken etc. Dat mag alleen als er een grondslag op van toepassing is. Een grondslag is simpel gezegd een gegronde reden op basis waarvan je bevoegd bent om met de persoonsgegevens aan de slag te gaan. De AVG-wet noemt 6 grondslagen. Er moet altijd minimaal 1 grondslag van toepassing zijn voor je überhaupt iets mag doen met persoonsgegevens!

Om persoonsgegevens te mogen verzamelen hebben we dus een grondslag nodig. Deze zijn:

1. **Toestemming** van de betrokkene
   Foto's, gebruik digitale middelen (sociale media), begeleiding leerling door externe onderwijsspecialist;
2. Noodzakelijk voor de **uitvoering van de overeenkomst**
   Met de ouders/verzorgers. Bijvoorbeeld voor de TSO (tussenschoolse opvang) van kinderen, personeel de arbeidsovereenkomst;
3. Noodzakelijk voor voldoen aan een **wettelijke verplichting**
   Bijvoorbeeld voor bekostiging, inspectie, overdrachtsdossier;
4. Een **vitaal belang** te beschermen
   De gegevensverwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen, bijvoorbeeld allergie;
5. Vervulling taak van **algemeen belang** of openbaar gezag
   Bijvoorbeeld de uitwisseling van informatie met samenwerkingsverbanden (let op: geen BSN);
6. **Gerechtvaardigd belang**
   Zoals het goed laten werken van digitale leermiddelen. Bijvoorbeeld voor Basispoort en educatieve uitgeverijen.

Vuistregels bij verzamelen en verstrekken van persoonsgegevens

Als er een grondslag is en je dus persoonsgegevens mag verwerken dan zijn de volgende vuistregels van belang:

1. Doelbepaling doelbinding

Worden de persoonsgegevens alleen gebruikt voor dat doel dat wij vooraf hebben vastgelegd? Persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld.
De belangrijkste doelen zijn voor het onderwijs:

- de organisatie of geven van onderwijs;
- het leren en begeleiden van leerlingen/studenten;
- het verstrekken of ter beschikking stellen van leermiddelen;
- het bekend maken van informatie over de hierboven genoemde organisatie en leermiddelen; het bekend maken van informatie over leerlingen, deelnemers of studenten (bijv. de eigen website);
- het bekend maken van de activiteiten van de instelling of het instituut op de eigen website;
- het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen;
- het behandelen van geschillen;
- het doen uitoefenen van accountantscontrole;
- de uitvoering of toepassing van een andere wet.

2. Dataminimalisatie

Gebruiken we die gegevens die noodzakelijk zijn om het vastgestelde doel te verwezenlijken? Kunnen we met minder of bijvoorbeeld anonieme gegevens werken? Bewaren we de gegevens niet langer dan nodig?

3. Transparant

Hebben we de leerlingen of hun ouders vooraf helder geïnformeerd over het doel van de gegevensverwerking? Hebben we uitgelegd welke gegevens worden gebruikt en met wie deze worden gedeeld? Deze informatievoorziening vindt ongevraagd plaats.

4. Juistheid

Kloppen de persoonsgegevens die we gebruiken nog steeds? De persoonsgegevens moeten correct zijn en blijven.

5. Opslagbeperking

Bewaren we de gegevens niet te lang? Houden we ons aan de bewaartermijnen?

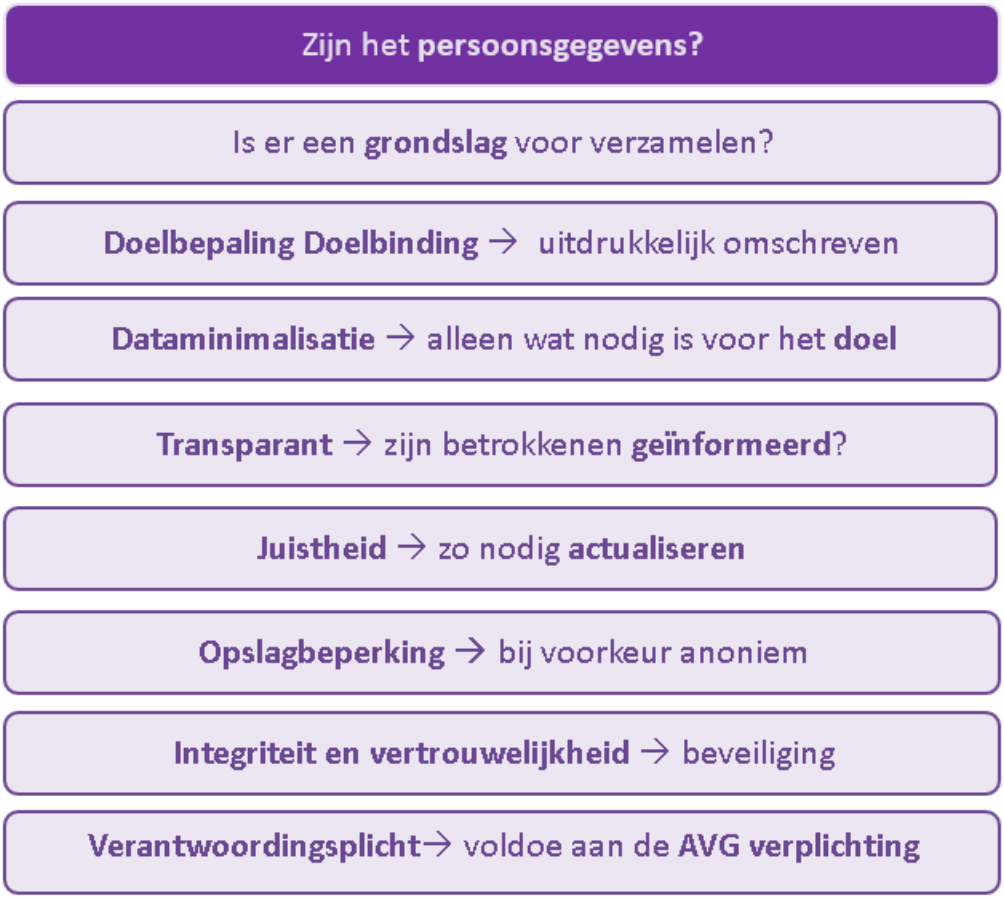
6. Integriteit en vertrouwelijkheid

Staan de gegevens op de juiste plaats en voor de juiste mensen beschikbaar? Hebben er niet te veel mensen toegang tot deze gegevens?

7. Verantwoordingsplicht

Kan de dataverantwoordelijke (bestuurder) aan deze regels te voldoen? En kan de bestuurder dit aantonen?

Binnen Stichting Bravoo spreken we met elkaar af dat we altijd checken of we aan deze vuistregels voldoen bij het verzamelen en verstrekken van persoonsgegevens. Hiervoor gebruiken we onderstaand schema.



Hoofdstuk 3 Privacyreglement en verklaring

Het privacyreglement is een document waarin nauwkeurig en op een begrijpelijke manier beschreven is welke persoonsgegevens binnen de organisatie worden verwerkt en met welk doel.

Ook is hierin te lezen wie toegang heeft tot deze gegevens, hoe de gegevens zijn beveiligd en met wie ze uitgewisseld mogen worden. Met het reglement voldoet het bestuur aan haar wettelijke informatieplicht, mits deze ook actief wordt aangeboden aan de ouders en medewerkers. Alle betrokkenen, zoals ouders en medewerkers, moeten daarom het privacyreglement kunnen inzien. Het privacyreglement is vastgesteld door de (G)MR en voor medewerkers als **bijlage 2** toegevoegd bij dit handboek.

Ouders moeten tijdens de aanmelding geïnformeerd worden over de gegevens die verzameld worden door de school en wat er met die gegevens gedaan wordt. Dit is opgenomen in de privacy verklaring/toelichting. De privacyverklaring is vastgesteld door de (G)MR en te vinden als **bijlage 3.**

Medewerkers en ouders kunnen het reglement en de verklaring inzien op de website https://www.stichtingbravoo.nl/beleid/privacy. Op de sites van de scholen wordt verwezen naar dit adres zodat altijd de actuele informatie beschikbaar is.

Hoofdstuk 4 Toestemming foto's/video's en online diensten/en andere persoonsgegevens

Toestemming leerlingen

Richtlijn voor het gebruik en toestemming beeldmateriaal

Privacy wordt in Nederland de Algemene Verordening Gegevensbescherming. Foto's en video's van leerlingen zijn persoonsgegevens en vallen daarmee onder deze wet. Daarom gelden er aangescherpte eisen voor het gebruik van beeldmateriaal. Het gaat om alle vormen van gebruik, zoals:

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

De Autoriteit Persoonsgegevens (AP), is in Nederland toezichthouder op de uitvoering van de privacywetgeving. De AP heeft een aantal richtlijnen opgesteld voor het juist gebruik van beeldmateriaal op school.

Als een school foto's of video's van leerlingen gebruikt, dan is daar altijd toestemming van ouders voor nodig. Als de leerling 16 jaar of ouder is, moet de leerling daar zelf toestemming voor geven. Hierbij gelden de volgende voorwaarden:

De toestemming moet in **vrijheid** worden gegeven. Hiermee wordt bedoeld dat ouders en leerlingen altijd moeten kunnen weigeren, zonder dat daar sancties aan zijn verbonden. De inschrijving van een leerling op school mag bijvoorbeeld niet afhankelijk zijn van de toestemming om beeldmateriaal te gebruiken.
De toestemming moet '**ondubbelzinnig zijn'**. Dit betekent dat toestemming altijd nodig is. Als er geen reactie is op je vraag mag je niet aannemen dat de ouders het goed vinden dat je beeldmateriaal gebruikt. Wie zwijgt, stemt dus niet toe. Ook mag je de toestemming niet verbergen in de voorwaarden bij inschrijving of in de schoolregels. Je moet de toestemming namelijk altijd kunnen aantonen.
De toestemming is **specifiek**. Dit houdt in dat het duidelijk is voor de leerling en zijn ouders waar toestemming voor wordt gegeven. Bij het vragen van toestemming is duidelijk hoe het beeldmateriaal wordt gebruikt: bijvoorbeeld op de website, nieuwsbrief of sociale media), en wat het doel is (bijvoorbeeld informeren van de ouders en leerlingen of promotie van de school).

De beleidsregels van de AP benadrukken dat scholen het vragen om toestemming serieus moeten nemen. Ook al leidt dat tot extra administratieve rompslomp. De toestemmingen worden bij de inschrijving van het kind aangegeven. Toestemming die eenmaal is gegeven, mag op **ieder moment worden ingetrokken**. En natuurlijk gebruik je het beeldmateriaal niet als er (nog) geen toestemming is gegeven.
De toestemmingen worden direct overgenomen in Parnassys. Zodra de ouders hun account in Parro geactiveerd hebben kunnen zij de instellingen daar terugvinden.
Ouders krijgen aan de start van ieder schooljaar een bericht via het ouderportaal en een oproep in de nieuwsbrief om voor een bepaalde datum de privacy instellingen te controleren en aan te passen. Daarna zetten wij de mogelijkheid tot aanpassen dicht. Ouders kunnen op ieder moment kenbaar maken dat ze een wijziging willen aan de betreffende leerkracht, maar het

dan niet meer zelf aanpassen. Zo voorkomen we dat de ouders een wijziging doorvoeren zonder dat de leerkracht hiervan op de hoogte is.
De leerkracht maakt namelijk na de sluitingsdatum een groepsoverzicht met de kinderen die niet op de foto mogen. Het zou vervelend zijn als ouders iets wijzigen zonder dat de leerkracht dat weet. Ook is het niet werkbaar als de leerkracht bij ieder foto moment weer moet controleren wie er wel of niet op de foto mag. Op deze manier kan er niemand tussendoor glippen door een onverwachte tussentijdse wijziging.

Fotograferen van ouders

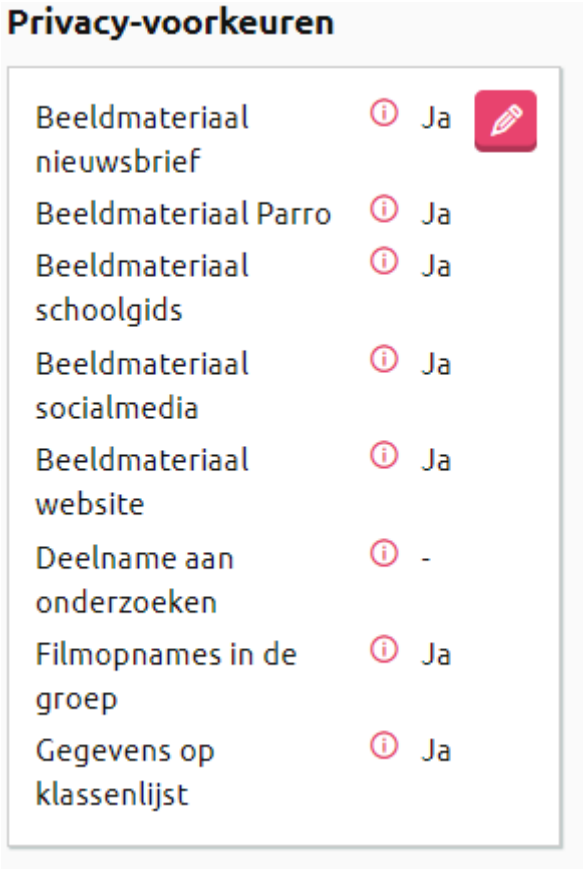
Uiteraard zijn er in de school ook ouders die foto's of video's maken bijvoorbeeld bij feestelijke gelegenheden. De school moet een veilige omgeving zijn voor alle kinderen (en hun ouders) en zij moeten niet het risico lopen ongewenst gefotografeerd te worden.
Wanneer er activiteiten georganiseerd worden op een externe locatie, zoals bijvoorbeeld bij een excursie, sportdag of schoolreisje is het echter lastig om het maken van beeldopnames door ouders te verbieden.

Wij vragen daarom de ouders ook terughouden te zijn met fotograferen en alleen hun eigen kinderen te fotograferen. Ook vragen wij ouders geen foto van andere leerlinge op hun eigen sociale media te plaatsen.

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 (privé) account 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. Hiervoor heeft de school een verwerkersovereenkomst


Privacy-voorkeuren
Beeldmateriaal nieuwsbrief
Ja
Beeldmateriaal Parro
Ja
Beeldmateriaal schoolgids
Ja
Beeldmateriaal socialmedia
Ja
Beeldmateriaal website
Ja
Deelname aan onderzoeken
-
Filmopnames in de groep
Ja
Gegevens op klassenlijst
Ja

Toestemming medewerkers

Richtlijn voor het gebruik en toestemming beeldmateriaal

Privacy wordt in Nederland de Algemene Verordening Gegevensbescherming. Foto's en video's van leerlingen zijn persoonsgegevens en vallen daarmee onder deze wet. Daarom gelden er aangescherpte eisen voor het gebruik van beeldmateriaal. Het gaat om alle vormen van gebruik, zoals:

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

De Autoriteit Persoonsgegevens (AP), is in Nederland toezichthouder op de uitvoering van de privacywetgeving. De AP heeft een aantal richtlijnen opgesteld voor het juist gebruik van beeldmateriaal op school.

Als een school foto's of video's van leerlingen gebruikt, dan is daar altijd toestemming van ouders voor nodig. Als de leerling 16 jaar of ouder is, moet de leerling daar zelf toestemming voor geven. Hierbij gelden de volgende voorwaarden:

De toestemming moet in **vrijheid** worden gegeven. Hiermee wordt bedoeld dat ouders en leerlingen altijd moeten kunnen weigeren, zonder dat daar sancties aan zijn verbonden. De inschrijving van een leerling op school mag bijvoorbeeld niet afhankelijk zijn van de toestemming om beeldmateriaal te gebruiken.
De toestemming moet '**ondubbelzinnig zijn'**. Dit betekent dat toestemming altijd nodig is. Als er geen reactie is op je vraag mag je niet aannemen dat de ouders het goed vinden dat je beeldmateriaal gebruikt. Wie zwijgt, stemt dus niet toe. Ook mag je de toestemming niet verbergen in de voorwaarden bij inschrijving of in de schoolregels. Je moet de toestemming namelijk altijd kunnen aantonen.
De toestemming is **specifiek**. Dit houdt in dat het duidelijk is voor de leerling en zijn ouders waar toestemming voor wordt gegeven. Bij het vragen van toestemming is duidelijk hoe het beeldmateriaal wordt gebruikt: bijvoorbeeld op de website, nieuwsbrief of sociale media), en wat het doel is (bijvoorbeeld informeren van de ouders en leerlingen of promotie van de school).
Toestemming die eenmaal is gegeven, mag op **ieder moment worden ingetrokken**. En natuurlijk gebruik je het beeldmateriaal niet als er (nog) geen toestemming is gegeven.

De beleidsregels van de AP benadrukken dat scholen het vragen om toestemming serieus moeten nemen. Ook al leidt dat tot extra administratieve rompslomp. Ten minste jaarlijks zal gewezen moeten worden op de toestemming die wel of niet is gegeven. Door het hele jaar heen moet het mogelijk zijn de toestemmingen aan te passen. Hierop worden medewerkers via het bestuurskantoor en hun directeuren minstens 1x per jaar op gewezen.
Bij stichting Bravoo kunnen medewerkers digitaal via Afas Insite aangeven of zij wel dan niet toestemming verlenen.

Toestemming persoonsgegevens

☐

Naam en email

☐

Naam en adres

☐

Naam en mobiel telefoonnummer

Toestemming foto's

☐

Klassenfoto

☐

Teamfoto

☐

Individuele foto

Toestemming beeldmateriaal

☐

Op de website van de school en Stichting Bravoo

☐

In de (digitale) nieuwsbrief, folders en brochures

☐

Op social media accounts van Stichting Bravoo

Hoofdstuk 5 Rechten van betrokkenen en klachten over privacy

Het is belangrijk om 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.
Hiervoor hebben we een **procedure** opgesteld.
Het verzoek komt doorgaans binnen bij de leerkracht. Deze speelt het verzoek direct door aan de directeur. De directeur neemt het verzoek in behandeling. Bij vragen kan de directeur terecht bij de Functionaris voor Gegevensbescherming (FG). Het is niet noodzakelijk om meteen het dossier te overhandigen. Het gestelde termijn voor de AVG-wetgeving is binnen 4 weken.

Betrokkenen kunnen een verzoek indienen bij de school of bij de verwerkingsverantwoordelijke (schoolbestuur).
Betrokkenen kunnen verzoeken doen, die zijn gebaseerd op de volgende rechten:

1. Recht op informatie
2. Recht op inzage in de gegevens
3. Recht op kopie van de gegevens
4. Recht op correctie en aanvulling (rectificatie)
5. Recht op vergetelheid (wissen van gegevens)
6. Recht om gegevens over te (laten) dragen (dataportabiliteit)
7. Recht op beperking van de verwerking
8. Recht om bezwaar te maken tegen de verwerking van gegevens

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

- Als **medewerker** kun je jouw vraag stellen aan de **directeur**.
- Een **ouder** of ander gezaghebbende die jou deze vraagt stelt, verwijs je door naar de **directeur**.(zie protocol bijlage 7)

In alle gevallen kan er ook altijd rechtstreeks contact opgenomen worden met de Functionaris voor Gegevensbescherming. De contactgegevens staan op de website.

Voor de directeuren is de uitgebreide procedure rechten van betrokkenen beschikbaar **(bijlage 5)** Een overzicht van welke ouder recht heeft op welke informatie (gezag kwesties) (**bijlage 5a**) Tevens is er voor de directeuren een registratieformulier beschikbaar om de genomen stappen te bewaken en aantoonbaar te maken. **(bijlage 5b)**

Hoofdstuk 6 Functionaris voor Gegevensbescherming

Een Functionaris voor Gegevensbescherming (FG) is iemand die controleert of een school zich aan de regels van de Algemene Verordening Gegevensbescherming (AVG) houdt. Een schoolbestuur is verplicht een FG aan te wijzen. Scholen of vestigingen die onder een schoolbestuur vallen hoeven geen eigen FG aan te wijzen.

Naast een controlerende taak beoordeelt een FG beveiligingsincidenten en datalekken, adviseert het bestuur en maakt medewerkers bewust van het belang van informatiebeveiliging en privacy. De FG is dé vraagbaak als het gaat om verwerking van persoonsgegevens.

Daarnaast is de FG de contactpersoon voor de externe toezichthouder: de Autoriteit Persoonsgegevens. Binnen Stichting Bravoo hebben wij een Functionaris voor Gegevensbescherming aangesteld in de persoon van Angela Groen, tel. 010-4071998, a.groen@cedgroep.nl in principe lopen alle vragen via onze interne Security Officer, Mechi de Veer die bereikbaar is via privacy@stichtingbravoo.nl en 0416-283103.
Het is ook mogelijk indien gewenst om rechtstreeks contact op te nemen met de Functionaris voor Gegevensbescherming. De regeling taken en verantwoordelijkheden Functionaris voor Gegevensbescherming zijn met instemming van de GMR vastgesteld en op te vragen bij het bestuur.

Hoofdstuk 7 Verwerkersovereenkomsten en verwerkersregister

Wat is een verwerkersovereenkomst?

In de nieuwe privacywet is bepaald dat de school afspraken moet maken met alle leveranciers van de school die leerlinggegevens verwerken in zogenaamde Verwerkersovereenkomsten. Het gaat bijvoorbeeld om uitgevers van digitaal lesmateriaal, leveranciers van toetsen, onderwijsadviesdiensten, etc.
Het belangrijkste hierbij is dat scholen, als gegevensverantwoordelijke, de regie hebben en houden over wat er gebeurt met de persoonsgegevens. Dit mag je niet overlaten aan de leverancier (verwerker). De school beslist wat de leverancier wél en niet met de gegevens mag doen.

Uitwisseling van gegevens met samenwerkingsverband

Een uitzondering hierop is de uitwisseling van gegevens met het samenwerkingsverband in het kader van passend onderwijs. Het samenwerkingsverband is een zelfstandige organisatie die zelf verantwoordelijk is voor de gegevens van leerlingen. De wet regelt dat een school gegevens uitwisselt met het samenwerkingsverband. Hiervoor hoeft daarom geen verwerkersovereenkomst afgesloten te worden. Het blijft natuurlijk wel belangrijk om de gegevens op de juiste manier uit te wisselen. (zie verder document)

Het afsluiten van een verwerkersovereenkomst

De verwerkersovereenkomsten worden bovenschools afgesloten. Hiervoor is een inventarisatie gedaan van de lopende contracten van de scholen binnen Stichting Bravoo Wanneer een school een contract afsluit met een nieuwe leverancier zal er een nieuwe verwerkersovereenkomst gesloten moeten worden. Voordat de school een nieuw contract afsluit neemt de school eerst contact op met de Security Officer. Deze kijkt of het bestuur al een contract met deze leverancier heeft en zorgt anders eerst voor de verwerkersovereenkomst alvorens de school kan starten met de software. De privacy bijsluiters (deze zijn toegevoegd als bijlage bij een verwerkersovereenkomst) moeten inzichtelijk zijn voor ouders indien zij hierom vragen. Dit kan opgevraagd worden via privacy@stichtingbravoo.nl.
Voor het afsluiten van verwerkersovereenkomsten wordt gebruik gemaakt van het meest actuele model verwerkersovereenkomst, die te vinden is via https://www.privacyconvenant.nl

Verwerkersregister

Iedere verwerkingsverantwoordelijke moet een register van de verwerkingsactiviteiten die onder de verantwoordelijkheid van de verwerkingsverantwoordelijke vallen, in een register bijhouden (art. 30 AVG).

Het bestuur houdt de volgende gegevens in het register bij:

- de naam en de contactgegevens van de verwerkingsverantwoordelijke(n) en de functionaris voor gegevensbescherming;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen (Van wie worden persoonsgegevens verwerkt? Bijvoorbeeld leerlingen, ouders, medewerkers, oud-medewerkers,);
- een beschrijving van de categorieën van persoonsgegevens (Wat voor persoonsgegevens worden er verwerkt? Bijvoorbeeld BSN, financiële gegevens etc.);
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;

- doorgiften van persoonsgegevens aan een derde land of internationale organisatie (indien van toepassing);
- indien mogelijk een algemene beschrijving van de technische en organisatorische maatregelen die genomen zijn om te beveiligen.

Wanneer er een nieuwe verwerking plaatsvindt, moet deze in het register komen te staan. Het register en de verwerkersovereenkomsten zijn in te zien via het bestuur.

Hoofdstuk 8 Procedure 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 zouden mogen hebben, of wanneer er persoonsgegevens onbedoeld verloren zijn gegaan.

Voorbeelden van datalekken zijn:
- een e-mail die aan een verkeerd persoon geadresseerd is
- verlies of diefstal van waardepapier, dossier, usb-stick, tablet of andere gegevensdragers, of inloggegevens die openbaar zijn geworden
- een gestolen telefoon
- een gehackte computer
- een phishing mail

Is er mogelijk sprake van een datalek, dan ben je als medewerker verplicht dit zo snel mogelijk te melden bij de Security Officer van Stichting Bravoo en bij je direct leidinggevende (ook als je twijfelt). Je kunt hiervoor het volgende emailadres gebruiken: privacy@stichtingbravoo.nl.
Als er persoonsgegevens verloren, beschadigd of onrechtmatig ingezien zijn, dan moet er mogelijk binnen 72 uur een melding gedaan worden bij de Autoriteit Persoonsgegevens. De FG doet de melding in overleg met de verwerkingsverantwoordelijke.

Het bestuur van de school (bevoegd gezag) is verwerkingsverantwoordelijk 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 boete opgelegd worden aan het bestuur (bevoegd gezag).

In **bijlage 6** is de volledige procedure melden datalekken opgenomen.

Hoofdstuk 9 Toegangsbeleid

Binnen de organisatie zijn veel persoonsgegevens aanwezig. Zowel van medewerkers als van leerlingen. Niet alle medewerkers hebben toegang nodig tot alle leerlinggegevens. Per rol is vastgesteld welke gegevens kunnen worden ingezien en gewijzigd, waarbij is gekeken wat iemand in die rol nodig heeft aan gegevens om zijn of haar werkzaamheden uit te kunnen voeren. Gegevens die daarbij niet noodzakelijk zijn, kan die rol ook niet inzien of wijzigen.
Een leerkracht krijgt de toegang tot zijn/ haar eigen groep. Daarbij heeft de leerkracht de mogelijkheid tijdelijke toegang te vragen, dit wordt door het systeem direct verleend. De leerkracht moet hiervoor wel de reden voor de toegang invullen. Dit wordt gelogd.

De directeur van de school is verantwoordelijk voor het verstrekken van de juiste toegang (accounts met de juiste rollen en rechten). 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.

De toegang tot gegevens van de medewerkers is beperkt tot de direct leidinggevende en diens vervanger en de HRM afdeling van het bestuur. In **bijlage 7** vind je de toegangsmatrix.

Hoofdstuk 10 Gedragscode

Voor een veilig schoolklimaat is het belangrijk dat de afspraken rondom informatiebeveiliging en privacy door alle werknemers en leerlingen worden nageleefd en uitgedragen. Daarom is er een Gedragscode ICT en Internet opgesteld waaraan alle medewerkers van Stichting Bravoo zich dienen te houden.
Er is een gedragsprotocol ICT, social media en telefoon voor de leerlingen van stichting Bravoo opgesteld en toegevoegd als **bijlage 4.**

De Gedragscode ICT en Internet is vastgesteld door de GMR en toegevoegd als **bijlage 8.**

Hoofdstuk 11 Uitwisselen van gegevens

Om ervoor te zorgen dat we binnen de school gegevens op de juiste wijze uitgewisseld worden hebben we een schema gemaakt wanneer er toestemming gevraagd moet worden en hoe de gegevens uitgewisseld worden.
In deze tabel staat met wie je gegevens uit mag wisselen en op welke wijze. Staat jouw doel er niet bij informeer dan altijd even bij de Functionaris voor Gegevensbescherming (FG).

Persoonsgegevens-verstrekken aan:	Het doel is:	Heb je toestemming nodig?
Overstap van PO naar andere basis-, SO/SBO of VO school	Overdracht (OKR,) leerlingdossier (na aanmelding) **W**	**NEE** maar ouders hebben wel inzage en de mogelijkheid hun zienswijze toe te voegen.
Overstap van VO naar VSO of andere VO school	Overdracht (OKR,) leerlingdossier (na aanmelding) **W**	**JA** ouders mogen bezwaar maken tegen deze uitwisseling. Ze moeten inzage gehad hebben en toestemming gegeven.
Dienst Uitvoering Onderwijs (DUO)	Bekostiging **W**	**NEE**
Inspectie van het Onderwijs	Toezicht **W**	**NEE**
Leerplicht gemeente	Controle verzuim **W***	**NEE**
Administratiekantoor	Salarisadministratie en HRM	**NEE,** wel verwerkersovereenkomst
Samenwerkingsverband (SWV)	Advies, arrangement, Toelaatbaarheids-verklaring (TLV) (gegevens uit OPP) **W**	**NEE,** wel ouders informeren, **géén** BSN uitwisselen
Samenwerkingsverband (SWV)	Aanvullende gegevens op de OPP, voor TLV of advies of arrangement Bijv. onderzoekverslagen of informatie thuissituatie voor inzet jeugdhulp.	**JA,** voor alle medische verslagen is toestemming van de ouders nodig!
Samenwerkingsverband (SWV)	Thuiszitters tegengaan **W**	**NEE**
Educatieve uitgeverijen, Basispoort, Entree Federatie	Gebruik digitale middelen	**NEE**, wel verwerkersovereenkomsten met uitgeverijen
Educatieve apps (niet in beheer van de leerkracht of ICT)	Ondersteuning Onderwijs	**JA,** dit geldt als ze nadat de leerling school verlaten heeft de app nog gebruikt kan worden.
Externe onderwijs specialisten	Zorgbegeleiding (onderzoeken)	**JA**
Stagiaires (gegevens)	Opleiding	**NEE,** wel stage overeenkomst

Persoonsgegevens-verstrekken aan:	Het doel is:	Heb je toestemming nodig?
Stagiaires (foto's/video)	Opleiding	**NEE** indien het materiaal binnen de school blijft. **JA** indien het materiaal buiten de school gebruikt wordt.
TSO/BSO	Tussenschoolse opvang, Buitenschoolse opvang	**JA**
GGD/JGZ*	Er mag **niet uitgewisseld** worden door de school!	**n.v.t***

W = Wettelijk verplicht
W*= Wettelijk verplicht en uitbesteed bij gemeente
***** De GGD wisselt uit met DUO. Op dit moment werkt de uitwisseling via DUO nog niet overal goed. Indien de vraag toch komt overleggen met FG.

Deze tabel is niet uitputtend. Staat het type persoonsgegevensverstrekking er niet bij, vraag dit dan na bij de Functionaris voor Gegevensbescherming (FG)

Hoofdstuk 12 Richtlijnen veilig mailen

E-mail is niet een bijzonder veilig medium. Mail kan onderweg onderschept worden. Je mailaccount kan natuurlijk gehackt worden, maar dat is iets dat ook bij andere uitwisselmedia kan gebeuren. Zeker zo belangrijk is dat een e-mail per ongeluk bij de verkeerde persoon terecht kan komen. Om daar de nadelige gevolgen van te voorkomen, kun je een aantal maatregelen treffen.

1. **Check altijd of je inderdaad het goede e-mailadres ingevuld hebt.**
   Let dus op wanneer je e-mailprogramma een adres automatisch aanvult.

2. **Vul het e-mailadres pas op het laatst in, nadat je je bericht geschreven hebt.**
   Dan kan de mail niet per ongeluk verstuurd worden.

3. **Neem in je e-mailbericht niet meer informatie op dan noodzakelijk is.**
   Persoonsgegevens mogen namelijk niet bij de verkeerde persoon terecht komen. Om toe te lichten wat je wel en wat je beter niet in je mail opneemt, zie je hieronder twee voorbeelden.

Voorbeeld 1

Leerkracht mailt aan andere leerkracht:

> *'Daan Verstraete gaat morgen niet mee zwemmen omdat hij oorontsteking heeft.'*

Zowel de volledige naam als de vermelding van medische informatie zijn **persoonsgegevens** waarmee je zorgvuldig moet omgaan. Het is daarom beter dit bericht als volgt te formuleren:

> *'Daan gaat morgen niet mee zwemmen.'*

In bijna alle gevallen weten de betrokkenen wel om welke Daan het gaat en de reden is minder belangrijk. Is de reden wel belangrijk, of is het noodzakelijk om andere persoonsgegevens te vermelden, mail dan **beveiligd**.

Voorbeeld 2

Leraar mailt aan ouder:

> *'De afgesproken intelligentietest bij uw dochter Hilde Özgül zal afgenomen worden op woensdag 5 oktober om 13.30 uur.'*

Ook hier bevat de mail persoonsgegevens die niet in verkeerde handen terecht mogen komen. Een betere mail is daarom:

> *'De afgesproken test bij uw dochter zal afgenomen worden op woensdag 5 oktober om 13.30 uur.'*

Binnen Stichting Bravoo werken we met Office 365, hiermee is het mogelijk versleuteld te mailen. In de E-learningmodules van de Schoolupdate academie is dit onderwerp opgenomen en in de map Bravoo-medewerkers in Teams is deze korte uitleg te vinden.

Hoofdstuk 13 Bewaartermijnen

Archivering: bewaartermijnen
Op dit moment wordt er door Kennisnet in samenspraak met het ministerie van OC&W gekeken naar bewaartermijnen van persoonsgegevens. Naar verwachting zal daar binnenkort meer duidelijk over worden. Zolang hier nog geen duidelijkheid over is houdt Stichting Bravoo vast aan de bewaartermijnen voor leerlinggegevens zoals hieronder aangegeven, tenzij de wet anders voorschrijft.

Dit zijn de voorlopige bewaartermijnen onderwijs

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn	Afwijkende bewaartermijn
Gegevens over in– en uitschrijving	5 jaar	datum van uitschrijving	
Gegevens over verzuim en afwezigheid	minimaal 5 jaar	datum van uitschrijving	
Gegevens die nodig zijn om de bekostiging te berekenen	minimaal 7 jaar	na afloop van het schooljaar waarop de bekostiging betrekking heeft	
Gegevens leerling na overstap naar speciaal onderwijs	3 jaar	datum van uitschrijving	5 jaar*
Camera en videobeelden	maximaal 4 weken, dan wel na afhandeling van geconstateerde incidenten	moment van opname	
Het onderwijskundig dossier	maximaal 2 jaar	datum van uitschrijving	5 jaar*
Gezondheidsgegevens die nodig zijn voor speciale begeleiding of voorzieningen	maximaal 2 jaar	datum van uitschrijving	5 jaar*
Adresgegevens	maximaal 2 jaar	datum van uitschrijving	5 jaar*

*I.v.m. de inspectie uitdraaien hanteren wij de afwijkende bewaartermijn van 5 jaar wij volgen hiermee het advies van kennisnet en de PO/VO raad.
Indien de ouder hierom verzoekt kan er eerder verwijderd worden. Hiervoor is het verstandig de FG ingeschakeld worden.

Bewaartermijnen personeel:

Document / gegevens	Wettelijke bewaartermijn	Ingangsdatum bewaartermijn	Afwijkende bewaartermijn
Sollicitatiebrieven, - formulieren, correspondentie omtrent de sollicitatie, getuigschriften	4 weken zonder toestemming, 1 jaar met toestemming van de sollicitant	na beëindiging sollicitatie-procedure	
VOG	1 jaar	einde dienstverband	2 jaar i.v.m. de accountants-controle
Arbeidsovereenkomst en wijzigingen	2 jaar	einde dienstverband	
BSN	7 jaar	einde dienstverband	
Loonbelastingverklaringen en kopieën van identiteitsbewijzen	5 jaar	einde dienstverband	
Verslagen van functioneringsgesprekken	2 jaar	einde dienstverband	
Loonbeslagen	Tot opheffing	Tot opheffing	
Opleiding	5 jaar	einde dienstverband	
Personeelsdossier, Nationaliteit NAW, contactgegevens, geslacht, levensloop	7 jaar	einde dienstverband	
Correspondentie over benoemingen, promotie, demotie en ontslag	2 jaar	einde dienstverband	
Financiële gegevens salarisadministratie	7 jaar	einde dienstverband	

Hoofdstuk 14 Jaarplan privacy

Bij het bestuur en op elke school is een jaarplan aanwezig met punten die elk jaar aan de orde komen qua privacy. Denk hierbij aan verwijderen van leerlingdossiers en personeelsdossiers. Het nakijken van de rechten, het wijzigen van de wachtwoorden etc.
Dit overzicht is in te zien via de directeur of op te vragen bij het bestuur.

Bijlagen

Bijlage 1 Persoonsgegevens
Bijlage 2 Privacyreglement
Bijlage 3 Privacyverklaring
Bijlage 4 Gedragsprotocol voor ICT, social media en telefoon – versie leerlingen
Bijlage 5 Procedure rechten van betrokkenen
Bijlage 5a Inzage tabel rechten van betrokkenen
Bijlage 5b Genomen stappen rechten van betrokkenen
Bijlage 6 Protocol datalekken
Bijlage 7 Toegangsmatrix
Bijlage 8 Gedragscode ICT en Internet

Bijlage 1 Persoonsgegevens

Bijlage 2 Privacyreglement

Privacyreglement Stichting Bravoo

Bron
Kennisnet

Bewerkt door:
Stichting Bravoo

Versie	Status	Datum	Auteur	Omschrijving
0.1	Concept	06-03-2018	Kennisnet en bewerkt door Naam	Concept ter goedkeuring
0.2	Herzien	08-10-2018	Mechi de Veer	Opmerkingen verwerkt, gereed gemaakt voor review FG
0.3	Geëvalueerd	13-07-2021	Mechi de Veer	Geen aanpassingen n.a.v. evaluatie

Vastgesteld door Stichting Bravoo:

Versie	Datum	Naam	Functie
0.2	08-10-2018	Drs. R. Venema	Voorzitter College van Bestuur

Privacyreglement voor Stichting Bravoo

1. Toepasselijkheid	Dit reglement geldt voor de gehele organisatie die deel uitmaakt van Stichting Bravoo. Stichting Bravoo is gevestigd aan Dodenauweg 2, 5171 NG Kaatsheuvel
2. Definities	
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'), zoals bijvoorbeeld naam, adres, geboortedatum, titel(s), geslacht, adres, telefoonnummer, e-mailadres, functie, personeelsnummer, medische rapportages, inhoud van e-mails, prestaties/cijfers, brieven, klachten, foto's, video's, IP-adressen, tracking cookies, loginnamen en wachtwoorden.
Verwerking van persoonsgegevens	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, geautomatiseerd of handmatig, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Bijzondere persoons-gegevens	Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken, genetische gegevens (DNA/RNA) of biometrische gegevens (bijv. foto's) met het oog op de unieke identificatie van een persoon, en gegevens over gezondheid, of iemands seksueel gedrag of seksuele gerichtheid.
Betrokkene	Degene op wie een persoonsgegeven betrekking heeft, en die al dan niet wordt vertegenwoordigd door een wettelijk vertegenwoordiger. Betrokkenen kunnen bijvoorbeeld zijn: leerlingen, ouders, medewerkers en bezoekers.
Wettelijk vertegenwoordiger	Degene die het ouderlijk gezag over een minderjarige uitoefent. Meestal zal dit een ouder zijn, maar het kan ook gaan om een voogd. Als een leerling 16 jaar of ouder is, beslist hij in voorkomende gevallen zelf over zijn privacy.
Verwerkingsverantwoordelijke	De entiteit die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. In het kader van dit reglement is Stichting Bravoo, vertegenwoordigd door het College van Bestuur, de verwerkingsverantwoordelijke.
Verwerker	De natuurlijke persoon of rechtspersoon die ten behoeve van de verwerkingsverantwoordelijke (Stichting Bravoo) persoonsgegevens verwerkt, zoals bijvoorbeeld de leverancier van een leerlingvolgsysteem of leerling-administratiesysteem. Een verwerker heeft een uitvoerende taak, ten behoeve van de activiteiten van de verwerkingsverantwoordelijke.
Derde	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, de verwerkingsverantwoordelijke, de verwerker, of de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om persoonsgegevens te verwerken.
Bevoegd gezag	Stichting Bravoo, de verwerkingsverantwoordelijke in de zin van dit reglement.
3. Reikwijdte en doelstelling	1. Dit reglement stelt regels over de verwerking van persoonsgegevens van alle betrokkenen bij de organisatie, waaronder leerlingen en hun wettelijk vertegenwoordigers, medewerkers, bezoekers en externe relaties (bijv. leveranciers en opdrachtnemers). 2. Dit reglement is van toepassing op alle persoonsgegevens van de betrokkene die door de Stichting Bravoo worden verwerkt. Het reglement heeft tot doel:

a. de persoonlijke levenssfeer van de betrokkenen te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens;
b. vast te stellen met welk doel en op welke (juridische) grondslag persoonsgegevens binnen Stichting Bravoo worden verwerkt;
c. ook overigens te borgen dat persoonsgegevens binnen Stichting Bravoo rechtmatig, transparant en behoorlijk worden verwerkt;
d. de rechten van betrokkenen vast te leggen en te borgen dat deze rechten door Stichting Bravoo worden gerespecteerd.

4. Doelen van de verwerking van persoonsgegevens

Bij de verwerking van persoonsgegevens houdt Stichting Bravoo zich aan de relevante wet- en regelgeving waaronder de Algemene Verordening Gegevensbescherming (AVG), de uitvoeringswet AVG en de onderwijswetgeving.

Doelen

1. De verwerking van persoonsgegevens vindt plaats voor:
   a. de organisatie of het geven van het onderwijs, de begeleiding van leerlingen, het voorzien in hun (extra) ondersteuningsbehoefte, dan wel het geven van studieadviezen;
   b. het verstrekken en/of ter beschikking stellen van leermiddelen;
   c. het bewaken van de veiligheid binnen de scholen en het beschermen van eigendommen van medewerkers, leerlingen en bezoekers;
   d. het bekend maken van informatie over de organisatie en leermiddelen als bedoeld, onder a en b, alsmede van informatie over de leerlingen op de eigen website;
   e. het bekend maken van de activiteiten van de organisatie, bijvoorbeeld op de website van Stichting Bravoo of van de scholen, in brochures of de schoolgids of via social media;
   f. het berekenen, vastleggen en innen van inschrijvingsgelden, school- en lesgelden en bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten, waaronder begrepen het in handen van derden stellen van vorderingen;
   g. het aanvragen van bekostiging, het behandelen van geschillen daarover en het doen uitoefenen van accountantscontrole;
   h. het onderhouden van contacten met oud-leerlingen;
   i. het aangaan en uitvoeren van arbeidsovereenkomsten, samenwerkingsrelaties met opdrachtnemers en contracten met leveranciers;
   j. de uitvoering of toepassing van wet- en regelgeving;
   k. juridische procedures waarbij Stichting Bravoo betrokken is.
2. De verwerking van persoonsgegevens mag ook plaatsvinden voor doelen die verenigbaar zijn met de doelen zoals beschreven in lid 1.

5. Doelbinding

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

6. Soorten persoonsgegevens

De categorieën van persoonsgegevens zoals deze binnen Stichting Bravoo worden verwerkt, worden geregistreerd in een verwerkingsregister.

7. Grondslag verwerking

Verwerking van persoonsgegevens gebeurt alleen indien aan een van de onderstaande voorwaarden is voldaan:

a. De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan Stichting Bravoo is opgedragen.
b. De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op Stichting Bravoo rust.
c. De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is (bijvoorbeeld de arbeidsovereenkomst) of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen.
d. De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van Stichting Bravoo of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen, met name wanneer de betrokkene een kind is; in het kader van deze grondslag zal dus een belangenafweging moeten plaatsvinden.
e. De verwerking is noodzakelijk om de vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen (levensbelang).
f. De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden.

8. Bewaartermijnen

Stichting Bravoo bewaart persoonsgegevens niet langer dan noodzakelijk is voor het doel waarvoor deze worden verwerkt, tenzij het langer bewaren van de persoonsgegevens op grond van wet- of regelgeving verplicht is.

9. Toegang

Binnen de organisatie van Stichting Bravoo geldt dat personen slechts toegang hebben tot persoonsgegevens voor zover dat daadwerkelijk nodig is. De toegang van medewerkers tot persoonsgegevens is dan ook beperkt tot de gegevens die noodzakelijk zijn voor de goede uitoefening van hun functie en (dus) hun werkzaamheden. Verder wordt slechts toegang verschaft tot de in de administratie en systemen van de school opgenomen persoonsgegevens aan:

a. de verwerker die van Stichting Bravoo de opdracht heeft gekregen om persoonsgegevens te verwerken, maar alleen voor zover dat noodzakelijk is in het licht van de gemaakte afspraken;
b. derden voor zover uit de wet voortvloeit dat Stichting Bravoo verplicht is om toegang te geven of sprake is van een (andere) grondslag voor deze verwerking, bijvoorbeeld de vervulling van een taak van algemeen belang.

10. Beveiliging en geheimhouding

1. Stichting Bravoo neemt passende technische en organisatorische beveiligingsmaatregelen om te voorkomen dat de persoonsgegevens worden beschadigd, verloren gaan of onrechtmatig worden verwerkt. Deze maatregelen zijn er mede op gericht om niet noodzakelijke verzameling en verdere (niet noodzakelijke) verwerking van persoonsgegevens te voorkomen.
2. Bij de beveiligingsmaatregelen wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van betrokkenen.
3. Een ieder die betrokken is bij de verwerking van persoonsgegevens binnen Stichting Bravoo is verplicht tot geheimhouding van de betreffende persoonsgegevens, en zal deze gegevens slechts verwerken voor zover dat noodzakelijk is voor de

uitoefening van de betreffende functie, werkzaamheden of taak.

11. Verstrekken gegevens aan derden

Stichting Bravoo kan persoonsgegevens aan derden verstrekken als daarvoor een grondslag bestaat in de zin van artikel 7 van dit reglement.

12. Sociale media

Voor het gebruik van persoonsgegevens in sociale media, zijn aparte afspraken gemaakt in het sociale mediaprotocol van Stichting Bravoo.

13. Rechten betrokkenen

1. Stichting Bravoo erkent de rechten van betrokkenen, handelt daarmee in overeenstemming en bewerkstelligt dat betrokkenen deze rechten daadwerkelijk kunnen uitoefenen. Het betreft in het bijzonder de volgende rechten:

Inzage

a. Een betrokkene heeft recht op inzage van de door Stichting Bravoo verwerkte persoonsgegevens die op hem betrekking hebben, behalve voor zover het gaat om werkdocumenten, interne notities en andere documenten die uitsluitend bedoeld zijn voor intern overleg en beraad. Indien en voor zover dit recht op inzage ook de rechten en vrijheden van anderen raakt, bijvoorbeeld als in de documenten ook persoonsgegevens van anderen dan de betrokkene zijn vermeld, kan Stichting Bravoo het recht op inzage beperken.

Bij het verstrekken van de betreffende gegevens verschaft Stichting Bravoo voorts informatie over:

- de verwerkingsdoeleinden;
- de categorieën van persoonsgegevens die worden verwerkt;
- de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- (indien van toepassing) ontvangers in derde landen of internationale organisaties;
- (indien mogelijk) hoe lang de gegevens worden bewaard;
- dat de betrokkene het recht heeft om te verzoeken dat de persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van de persoonsgegevens wordt beperkt, alsmede dat hij het recht heeft om bezwaar te maken tegen de verwerking van de persoonsgegevens;
- het feit dat de betrokkene een klacht kan indienen bij de Autoriteit Persoonsgegevens;
- de bron van de persoonsgegevens, indien de persoonsgegevens niet van de betrokkene zelf zijn verkregen;
- het eventueel toepassen van geautomatiseerde besluitvorming en de betreffende onderliggende logica en het belang en de gevolgen voor de betrokkene;
- de passende waarborgen indien de persoonsgegevens worden doorgegeven aan een derde land of een internationale organisatie.

Verbetering, aanvulling, verwijdering

b. Stichting Bravoo verbetert de persoonsgegevens van een betrokkene in het geval de betrokkene terecht heeft aangegeven dat de gegevens onjuist zijn, en Stichting Bravoo vult de persoonsgegevens van een betrokkene aan indien de betrokkene terecht om aanvulling heeft verzocht. Voorts kan de betrokkene verzoeken om verwijdering van zijn persoonsgegevens. Stichting Bravoo gaat daartoe over indien

is voldaan aan een wettelijke grondslag voor het verzoek, tenzij het onmogelijk is om aan het verzoek te voldoen of dit een onredelijke inspanning zou vergen.

Bezwaar

c. Indien Stichting Bravoo persoonsgegevens verwerkt op de grondslag van artikel 7 onder a of artikel 7 onder d van dit reglement, kan de betrokkene bezwaar maken tegen de verwerking van zijn persoonsgegevens. In dat geval staakt Stichting Bravoo de verwerking van de betreffende persoonsgegevens, behalve als naar het oordeel van Stichting Bravoo het belang van Stichting Bravoo, het belang van derden of het algemeen belang in het betreffende concrete geval zwaarder weegt.

Beperken verwerking

d. De betrokkene kan voorts verzoeken om de verwerking van zijn persoonsgegevens te beperken, namelijk indien hij een verzoek tot verbetering heeft gedaan, indien hij bezwaar heeft gemaakt tegen de verwerking, als de persoonsgegevens niet meer nodig zijn voor het doel van de verwerking of als de gegevensverwerking onrechtmatig is. Stichting Bravoo staakt dan de verwerking, tenzij de betrokkene toestemming heeft gegeven voor de verwerking, Stichting Bravoo de gegevens nodig heeft voor een rechtszaak of de verwerking nodig is ter bescherming van de rechten van een andere persoon of vanwege gewichtige redenen.

Kennisgevingsplicht

e. Als Stichting Bravoo op verzoek van een betrokkene een verbetering of verwijdering van persoonsgegevens heeft uitgevoerd, of de verwerking van persoonsgegevens heeft beperkt, zal Stichting Bravoo eventuele ontvangers van de betreffende persoonsgegevens daarover informeren.

Procedure

2. Stichting Bravoo handelt een verzoek van een betrokkene zo spoedig mogelijk, maar uiterlijk binnen een maand na ontvangst van het verzoek, af. Afhankelijk van de complexiteit en van het aantal verzoeken kan die termijn indien nodig met twee maanden worden verlengd. Als deze verlenging plaatsvindt, wordt de betrokkene daarover binnen een maand na de ontvangst van het verzoek geïnformeerd. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt. Wanneer Stichting Bravoo geen gevolg geeft aan het verzoek van de betrokkene, deelt Stichting Bravoo onverwijld en uiterlijk binnen een maand na ontvangst mede waarom het verzoek niet wordt ingewilligd en informeert hij de betrokkene over de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens of beroep bij de rechter in te stellen.

Intrekken toestemming

3. Indien voor de verwerking van persoonsgegevens voorafgaande toestemming vereist is, kan deze toestemming te allen tijde door de betrokkene of zijn wettelijk vertegenwoordiger worden ingetrokken. Als de toestemming wordt ingetrokken, staakt Stichting Bravoo de verwerking van persoonsgegevens, behalve als er een andere grondslag (zoals bedoeld in artikel 7) voor de gegevensverwerking is. Het intrekken van de toestemming tast de rechtmatigheid van verwerkingen die reeds hebben plaatsgevonden niet aan.

14. Transparantie

Stichting Bravoo informeert de betrokkene(n) actief over de verwerking van hun persoonsgegevens, in ieder geval door middel van een laagdrempelige

privacyverklaring. In de privacyverklaring wordt in ieder geval de volgende informatie vermeld:

a. de contactgegevens van Stichting Bravoo;
b. de contactgegevens van de functionaris voor gegevensbescherming van Stichting Bravoo;
c. de doeleinden van de gegevensverwerking en de grondslagen voor de verwerking;
d. een omschrijving van de belangen van Stichting Bravoo indien de verwerking wordt gebaseerd op het gerechtvaardigd belang van Stichting Bravoo;
e. de (categorieën) ontvangers van de persoonsgegevens, zoals verwerkers of derden;
f. in voorkomend geval: of de persoonsgegevens worden verzonden aan landen buiten de Europese Economische Ruimte (EER);
g. hoe lang de persoonsgegevens zullen worden bewaard;
h. dat de betrokkene het recht heeft om Stichting Bravoo te verzoeken om inzage, verbetering of verwijdering van persoonsgegevens, en dat hij het recht heeft om te verzoeken om beperking van de verwerking, om bezwaar te maken of om een beroep te doen op het recht van gegevensoverdraagbaarheid;
i. dat de betrokkene het recht heeft om zijn toestemming in te trekken, als de gegevensverwerking is gebaseerd op toestemming;
j. dat de betrokkene het recht heeft om een klacht in te dienen bij de Autoriteit Persoonsgegevens;
k. of de verstrekking van de persoonsgegevens een wettelijke of contractuele verplichting is, dan wel een noodzakelijke voorwaarde is om een overeenkomst te kunnen sluiten, en of de betrokkene verplicht is om de persoonsgegevens te verstrekken en wat de gevolgen zijn indien hij de persoonsgegevens niet verstrekt;
l. het bestaan van geautomatiseerde besluitvorming, vergezeld van nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

15. Meldplicht datalekken

Een ieder die betrokken is bij een verwerking van persoonsgegevens is verplicht om een datalek per ommegaande te melden bij het meldpunt (privacy@StichtingBravoo.nl), conform het protocol beveiligingsincidenten en datalekken van Stichting Bravoo. Een datalek is elke inbreuk waarbij persoonsgegevens zijn vernietigd of verloren, gewijzigd, verstrekt of toegankelijk zijn gemaakt.

16. Klachten

1. Wanneer een betrokkene van mening is dat het doen of nalaten van Stichting Bravoo niet in overeenstemming is met de AVG, dit reglement of (andere) toepasselijke wet- of regelgeving, dan kan een klacht worden ingediend overeenkomstig de binnen Stichting Bravoo geldende klachtenregeling. Een betrokkene kan zich eveneens wenden tot de functionaris voor gegevensbescherming van Stichting Bravoo.
2. Als een klacht naar de mening van betrokkene door Stichting Bravoo niet correct is afgewikkeld, kan hij zich wenden tot de rechter of de Autoriteit Persoonsgegevens.

17. Onvoorziene situatie

Indien zich een situatie voordoet die niet beschreven is in dit reglement, neemt het College van Bestuur van Stichting Bravoo de benodigde maatregelen, en wordt beoordeeld of dit reglement dientengevolge moet worden aangevuld of aangepast.

18. Wijzigingen reglement

1. Dit reglement is na instemming van de Gemeenschappelijke Medezeggenschapsraad (GMR) vastgesteld door het College van Bestuur van

Stichting Bravoo. Het reglement wordt gepubliceerd op de website van Stichting Bravoo en de websites van de scholen. Het reglement wordt verder actief onder de aandacht gebracht, bijvoorbeeld door middel van verwijzing in de schoolgids.

2. Het College van Bestuur kan dit reglement wijzigen na instemming van de GMR.

19. Slotbepaling

Dit reglement wordt aangehaald als het privacyreglement van Stichting Bravoo en treedt in werking op 10 oktober 2018.

Bijlage 3 Privacyverklaring

Privacy toelichting ; Hoe gaat Stichting Bravoo om met persoonsgegevens

- Contactgegevens Security Officer Stichting Bravoo:
  Mechi de Veer, Postbus 79, 5144 ND Kaatsheuvel, Dodenauweg 2, 5171 NG Kaatsheuvel, Tel. 0416-283103, privacy@stichtingbravoo.nl
- Verwerkingsverantwoordelijke:
  Drs. R. Venema, voorzitter College van Bestuur
- Contactgegevens Functionaris voor Gegevensbescherming:
  Angela Groen, CED-Groep, Dwerggras 30, 3068 PC Rotterdam, Postbus 8639, 3009 AP Rotterdam, Tel. 010-4071998, a.groen@cedgroep.nl

Stichting Bravoo verwerkt van al zijn leerlingen persoonsgegevens. Stichting Bravoo vindt een goede omgang met persoonsgegevens van groot belang en is zich bewust van de privacywetgeving. Stichting Bravoo is verantwoordelijk voor het zorgvuldig omgaan met de persoonsgegevens van uw kind. In deze privacy toelichting leggen wij u graag uit hoe wij met de persoonsgegevens van uw kind omgaan.

Waarom verwerken wij gegevens van uw kind

Stichting Bravoo verwerkt persoonsgegevens van uw kind om onze verplichtingen als onderwijsinstelling te kunnen nakomen. Zo hebben wij bijvoorbeeld de gegevens nodig om uw kind aan te melden als leerling op onze school, om de studievoortgang bij te houden en om uw kind in staat te stellen op een goede manier het basisonderwijs af te sluiten. Daarnaast hebben wij de wettelijke verplichting om bepaalde gegevens door te sturen naar andere partijen, zoals DUO (ministerie van Onderwijs) en leerplicht.
Wij verwerken gegevens van uw kind voor het uitvoeren van de onderwijsovereenkomst die we met uw kind hebben en/of voor het nakomen van onze wettelijke verplichtingen.
Gegevens die hier niet aan voldoen zullen wij alleen met uw toestemming verwerken. Als voor het verwerken van gegevens toestemming wordt gevraagd zoals voor het gebruik van beeldmateriaal (foto's en video's) dan kunt u de toestemming op elk moment intrekken of alsnog geven. (Wijziging van toestemming is niet van toepassing op inmiddels gepubliceerd beeldmateriaal).

Welke gegevens verwerken wij van uw kind

Wij verwerken diverse soorten gegevens, waarvan wij de meeste gegevens rechtstreeks van u als ouders hebben gekregen. U kunt hierbij denken aan contactgegevens en geboorteplaats. Als u weigert de voor ons noodzakelijke gegevens te verstrekken, kunnen wij onze verplichtingen niet nakomen. De verstrekking van deze gegevens is dan ook een voorwaarde om uw kind in te kunnen schrijven bij Stichting Bravoo.

Welke persoonsgegevens wij van uw kind verwerken kun u terugvinden onderaan deze toelichting bij *Categorieën van persoonsgegevens*.
Op uw eigen verzoek en met uw uitdrukkelijke toestemming verwerken wij ook medische gegevens van uw kind. Dit beperkt zich enkel tot gegevens die nodig zijn om in noodgevallen goed te kunnen handelen. U kunt bijvoorbeeld doorgeven dat uw kind epilepsie heeft, zodat wij adequaat kunnen optreden in noodsituaties. Stichting Bravoo zal u nooit dwingen dergelijke gegevens te overleggen.

Hoe gaan wij om met de gegevens van uw kind

Bij het verwerken van de gegevens gaan wij altijd uit van noodzakelijkheid, wij zullen niet meer gegevens verwerken dan noodzakelijk is om onze rechten en plichten als onderwijsinstelling na te komen. Dit betekent ook dat de gegevens niet zullen gebruiken voor andere doeleinden dan wij in deze toelichting noemen.

In een aantal gevallen zijn wij, zoals eerder aangegeven, verplicht om gegevens van uw kind te delen met andere organisaties. Dit zijn onder andere DUO, leerplicht, de onderwijsinspectie, GGD/schoolarts, samenwerkingsverband en accountant.

Wij kunnen commerciële derde partijen verzoeken om te ondersteunen bij het verwerken van de gegevens voor de eerder genoemde doeleinden. Denk hierbij aan applicaties om leerlingen in de les te ondersteunen, een administratie systeem waarbij de gegevens niet op ons eigen netwerk worden opgeslagen, maar bij een andere organisatie of een lesroosterprogramma. Dit gebeurt altijd in opdracht en onder de verantwoordelijkheid van Stichting Bravoo. Met deze organisaties sluiten we overeenkomsten af, waarin o.a. is vastgelegd welke gegevens er verwerkt worden en hoe deze gegevens beveiligd worden.
Wij zullen de gegevens van uw kind niet delen met commerciële derde partijen voor andere doeleinden. Ook zullen wij de gegevens van uw kind nooit verkopen of verhuren aan derde partijen.

De persoonsgegevens worden zoveel mogelijk gecodeerd bewaard en alleen die medewerkers kunnen bij de gegevens, die dat ook voor de uitvoering van hun werk nodig hebben. Daarnaast bewaren wij de gegevens niet langer dan noodzakelijk is. Wij hanteren hiervoor verschillende bewaartermijnen die wettelijk geregeld en vastgesteld zijn. Als u er belangstelling voor heeft kunnen wij u een overzicht hiervan geven.

Welke rechten hebben een leerling en ouders van leerlingen jonger dan 16 jaar

Als ouders heeft u een aantal rechten als het gaat om persoonsgegevens. Deze rechten zijn in de wet vastgelegd. Leerlingen en/of ouders kunnen op elk moment gebruik maken van deze rechten. Dit betekent bijvoorbeeld dat u altijd een verzoek kunt indienen om inzage te krijgen in de gegevens die wij van uw kind verwerken.
Daarnaast kunt u ook een verzoek indienen om gegevens te rectificeren, te beperken of helemaal te wissen uit de systemen van Stichting Bravoo. U heeft altijd het recht om onjuiste gegevens aan te vullen of te verbeteren. Wij zullen er vervolgens voor zorgen dat deze gegevens ook bij organisaties waarmee wij deze gegevens van uw kind delen en/of uitwisselen worden aangepast.
Als u ons verzoekt om gegevens van uw kind te beperken of te wissen, zullen wij toetsen of dit mogelijk is. In deze toets houden wij ons aan de wettelijke voorschriften en kijken wij bijvoorbeeld of wij geen wettelijke plicht hebben om de gegevens te bewaren.
Tevens heeft u het recht om te vragen om de gegevens, die wij van uw kind verwerken en wij van u hebben ontvangen, aan u over te dragen of op uw verzoek aan een andere organisatie over te dragen.
Stichting Bravoo zal geen besluiten nemen over uw kind, die alleen gebaseerd zijn op geautomatiseerde verwerking van gegevens (profiling). Beslissingen worden nooit zonder menselijke tussenkomst genomen.

Als u het niet eens bent met hoe wij omgaan met de gegevens van uw kind, dan kunt u altijd opheldering vragen bij onze Functionaris voor Gegevensbescherming (zie de contactgegevens

bovenaan deze toelichting). Indien uw probleem volgens u niet goed wordt opgelost, dan kunt u dat melden bij Autoriteit voor de Persoonsgegevens (www.autoriteitpersoonsgegevens.nl).

Opsomming van de categorieën van persoonsgegevens:

Categorie	**Toelichting**
• Contactgegevens	1a: naam, voornaam, e-mail, opleiding (bv. sector techniek); 1b: geboortedatum, geslacht; 1c: overige gegevens te weten: adres, postcode, woonplaats, telefoonnummer en eventueel andere voor communicatie benodigde gegevens, alsmede ook een bankrekeningnummer voor het afhandelen van betalingen;
• Leerling nummer een administratie-nummer dat geen andere informatie bevat dan bedoeld onder categorie 1	
• Nationaliteit en geboorteplaats	
• Ouders, voogd	contact gegevens van de ouders/verzorgers van leerlingen (naam, voornaam, adres, postcode, woonplaats, telefoonnummer en eventueel e-mailadres)
• Medische gegevens	gegevens die noodzakelijk zijn met het oog op de gezondheid of het welzijn van de leerling, voor zover deze van belang zijn bij het nemen van aanvullende maatregelen om goed onderwijs te kunnen volgen (bv. extra tijd bij toetsen);
• Godsdienst	gegevens betreffende de godsdienst of levensovertuiging van de leerling, voor zover die noodzakelijk zijn voor het te volgen onderwijs (bijvoorbeeld: leerling vrij op bepaalde dag).
• Studievoortgang	gegevens betreffende de aard en het verloop van het onderwijs en de behaalde studieresultaten te weten: • Begeleiding leerling (inclusief ontwikkelperspectief OPP) • Aanwezigheidsregistratie • Medisch dossier (papier) • Klas, leerjaar, opleiding
• Onderwijsorganisatie	gegevens met het oog op het organiseren van het onderwijs en het verstrekken of ter

Categorie	Toelichting
	beschikking stellen van leermiddelen; hieronder vallen ook lesroosters, boekenlijsten, schoolpasjes enz.
• Financiën	gegevens voor het berekenen, vastleggen en innen van inschrijvingsgelden, school- en/of lesgelden, bijdragen of vergoedingen voor leermiddelen en buitenschoolse activiteiten. (denk hierbij aan een bankrekeningnummer van de ouders)
• Beeldmateriaal	foto's en videobeelden (met of zonder geluid) van activiteiten van de school op basis van toestemming. **Let op**: Voor pasfoto voor identificatie-doeleinden is geen toestemming nodig (schoolpas en als aanvulling op het dossier).
• Docent /zorgcoördinator/ intern begeleider/ decaan / mentor	gegevens van docenten en begeleiders, voor zover deze gegevens van belang zijn voor de organisatie van de instelling en het geven van onderwijs, opleidingen en trainingen
• BSN (PGN)	In het onderwijs heet het BSN het persoonsgebonden nummer (PGN). Ook wel onderwijsnummer genoemd. Het PGN is hetzelfde nummer als het BSN. Scholen zijn verplicht het PGN te gebruiken in hun administratie.
• Keten-ID (Eck-Id)	Unieke iD voor de 'educatieve contentketen'. Hiermee kunnen scholen gegevens delen, zonder dat ze direct herleidbaar zijn naar leerlingen of docenten
• Overige gegevens, te weten ….	andere dan de onder 1 tot en met 13 bedoelde gegevens waarvan de verwerking wordt vereist of noodzakelijk is met het oog op de toepassing van een andere wet. Deze zullen apart vermeld en toegelicht worden.

Bijlage 4 Gedragsprotocol ICT, social media en telefoon leerlingen stichting Bravoo

Gedragsprotocol voor ICT, social media en telefoon – versie leerlingen Stichting Bravoo

We vinden het van groot belang dat je bij ons op school als leerling zo veilig mogelijk online kunt werken. Je kunt daar zelf aan meewerken door de richtlijnen in dit overzicht te volgen. Volg je ze niet dan breng je jezelf of anderen op school in gevaar en je zult daar op worden aangesproken.

Lees de richtlijnen goed door.

Internet en e-mail

1. Je gebruikt internet om informatie te zoeken over een onderwerp of opdracht voor school.
2. Je vraagt toestemming van je juf of meester, als je:
   a. een online game wilt spelen,
   b. persoonlijke gegevens (naam, adres en telefoonnummer) moet invullen op een website,
   c. bestanden wilt downloaden of delen,
   d. een e-mail wilt versturen,
   e. een chat in MS Teams wilt starten met iemand anders dan van de eigen klas.
3. Je deelt geen wachtwoorden met anderen.
4. Je logt niet in onder een account van een ander.
5. Je verstuurt geen anonieme berichtjes
6. Je gaat voorzichtig om met mails die je niet vertrouwt, of waarvan je de afzender niet kent. Bij twijfel klik je geen linkjes aan.
7. Je vertelt het direct aan je juf of meester als je informatie tegenkomt die je niet prettig vindt of waarvan je weet dat dat niet hoort.
8. Je weet bij wie je op school en buiten school terecht kunt als je iets onprettigs hebt meegemaakt op het internet waarbij je je niet veilig voelt.
9. Je zoekt op internet niet met zoekwoorden die te maken hebben met grof taalgebruik, agressie, seks of discriminatie.
10. Je bekijkt informatie op internet kritisch, want je weet dat er veel nepnieuws op internet staat. Als je het niet zeker weet vraag je het je juf of meester.
11. Je gaat zorgvuldig om met alle inloggegevens die een relatie hebben met school. Wachtwoorden deel je alleen met je leerkracht en ouders.

Sociale media

Sociale media gebruik je zonder andere personen of de school te schaden. Dat lukt je als je de volgende richtlijnen volgt:

1. Je plaatst op sociale media alleen foto's en video's van een ander, of verhalen over die ander, als die ander jou daarvoor toestemming geeft.
2. Je plaatst geen kwetsende foto's, video's, verhalen of opmerkingen op sociale media. Ook gebruik je geen grove taal.
3. Je doet niet mee aan pesten via WhatsApp of andere apps en programma's. Als je nare berichten ontvangt van iemand, dan vertel je dit op school of thuis.
4. Als je iemand niet begrijpt via WhatsApp of andere berichten, dan vraag je hem of haar rechtstreeks om verduidelijking.
5. Je gaat zorgvuldig om met je eigen persoonlijke gegevens. Je beseft dat je altijd terug te vinden ben op internet.

ICT-apparatuur

Het gebruik van computers en het netwerk moet passen binnen de doelstellingen van de school. Dit houdt in dat er alleen werk op wordt gedaan dat met school te maken heeft. De ICT-apparatuur op school (computer, laptop, tablet, 3D-printer, digibord, scanner, enz.) is duur, daarom moet je hier voorzichtig mee omgaan. Volg deze richtlijnen.

1. Je gebruikt alleen ICT-apparatuur, software en apps wanneer je juf of meester daar toestemming voor heeft gegeven. Dat geldt ook voor meegebrachte smartphones, tablets, spelcomputers, enz.
2. Je gaat voorzichtig om met de ICT-apparatuur van school die je mag gebruiken.
3. Je gebruikt geen meegebrachte USB-sticks van thuis in ICT-apparatuur van de school. Is dit toch echt nodig, dan vraag je het eerst aan je juf of meester.
4. Je downloadt of installeert geen software, spelletjes, films of muziek zonder toestemming van je juf of meester.
5. Je probeert niet het schoolnetwerk te hacken of op een andere manier te misbruiken.
6. Je wijzigt niets aan de instellingen op de ICT-apparatuur van school. Denk aan het bureaublad, de bureaubladachtergrond, het startmenu, opstartbestanden enz.
7. Je weet dat je zelf of je ouders mogelijk de kosten moet(en) betalen die het gevolg zijn van het niet zorgvuldig omgaan met ICT-apparatuur door jou.

Mobiele telefoons en smartwatches

1. Breng je een mobiele telefoon, smartwatch, tablet of laptop mee naar school dan is dat voor eigen risico. Alleen met toestemming van je juf of meester mag je eigen apparaten onder schooltijd gebruiken.
2. Deze apparaten gebruik je ook niet bij activiteiten buiten de school. Het mag alleen als je juf of meester hier toestemming voor gegeven heeft.
3. Je mobiele telefoons is standaard uit [1] in de klas.
4. Een smartwatch gebruik je tijdens de les alleen als horloge , dus om de tijd te weten.

Als je de richtlijnen niet volgt, dan wordt je mobiele telefoon, smartwatch of ander apparaat ingenomen. Je ouders mogen dan de telefoon op komen halen.[2]

[1] Of naar keuze: op stil.
[2] Of naar keuze: de telefoon krijg je eind van de dag weer terug. Of een andere oplossing.

Bijlage 5 Procedure rechten van betrokkenen

Procedure binnen de school

Wie behandelt een verzoek?

Het verzoek komt doorgaans binnen bij de leerkracht. Deze speelt het verzoek direct door aan de directeur. De directeur neemt het verzoek in behandeling.

Beoordeling van het verzoek

Beoordeel wat voor soort verzoek het is. Dit gebeurt door de directeur van de school of diens vervanger. Gaat het alleen om inzage, of ook om rectificatie, aanvulling, verwijdering of een beperking van de verwerking? Betrokkenen kunnen soms andere termen gebruiken, dus wees hier alert op. Afhankelijk van het soort verzoek moeten andere acties ondernomen worden. Denk hierbij aan het inschakelen van de functionaris voor Gegevensbescherming.
Betrokkenen kunnen een verzoek indienen bij de school of bij de verwerkingsverantwoordelijke (schoolbestuur).
Betrokkenen kunnen verzoeken doen, die zijn gebaseerd op de volgende rechten:

1. Recht op informatie
2. Recht op inzage in de gegevens
3. Recht op kopie van de gegevens
4. Recht op correctie en aanvulling (rectificatie)
5. Recht op vergetelheid (wissen van gegevens)
6. Recht om gegevens over te (laten) dragen (dataportabiliteit)
7. Recht op beperking van de verwerking
8. Recht om bezwaar te maken tegen de verwerking van gegevens

Voer een identiteitscontrole uit

Controleer de identiteit van de aanvrager voordat het verzoek verder in behandeling genomen wordt. Deze check moet **zwaarder** zijn naarmate het om meer gevoelige of zelfs bijzondere gegevens gaat. Voorkomen moet worden dat er een 'fake'-inzageverzoek gedaan wordt om zo gegevens te verzamelen. De controle kan al plaats gevonden hebben door de leerkracht als het verzoek bijvoorbeeld mondeling is binnen gekomen. De leerkracht heeft doorgaans contact met de ouder en kan een face to face verzoek controleren. Controleer of de verzoeker het gezag heeft. Ook een ouder zonder gezag heeft recht op informatie (Art. 1:377 b en c BW)[3].
Indien de identiteit niet direct kan worden vastgesteld, registreer dan wanneer en welke vragen er gesteld zijn om de identiteit vast te stellen. Overleg eventueel met de Functionaris voor Gegevensbescherming.

Behandel het verzoek

[3] Het Burgerlijk Wetboek bepaalt dat de school verplicht is een ouder die niet het ouderlijk gezag heeft, als hij of zij daarom vraagt, van beroepshalve beschikbare informatie te voorzien over belangrijke feiten en omstandigheden die het kind of de verzorging en opvoeding van het kind betreffen. Er zijn op deze regel twee uitzonderingen:

- de informatie wordt niet verstrekt als de school de informatie niet op dezelfde manier aan de ouder met het ouderlijk gezag zou verstrekken;
- de informatie wordt niet verstrekt als het belang van het kind zich daartegen verzet.

De directeur houdt toezicht op de termijn waarin het verzoek afgehandeld moet worden. De directeur geeft aan wie het verzoek afhandelt. Dit kan de leerkracht zijn, de IB'er of de directeur zelf.
De directeur bepaalt of de Functionaris voor Gegevensbescherming wordt geraadpleegd of ingeschakeld.

Verwerk verzoek (anoniem) in register
Alle verzoeken die binnen een kalenderjaar geweest zijn worden door de directeur vastgelegd. Dit gebeurt in een klein overzicht waarin de volgende gegevens worden opgenomen:

- datum van afhandeling;
  omschrijving van het verzoek;
- door wie het is afgehandeld;
- of de Functionaris voor Gegevensbescherming er bij betrokken is.
- eventuele bijzonderheden.

In het register worden geen gegevens opgenomen die herleidbaar zijn naar een persoon.

Bijlage 5a Inzage tabel

Welke ouder heeft recht op welke informatie?
Hieronder vindt u een schema waarin de soorten verbintenissen tussen ouders zijn omschreven. Je kunt zo gemakkelijk zien welke ouder recht heeft op welke informatie.

		Voor wie	**Alle informatie**	**Beperkte informatie** *(erkend)*
A		Ouders die met elkaar zijn getrouwd; voor vader en moeder geldt:	**X**	
B		Ouders die zijn gescheiden; Voor vader en moeder geldt:	**X N.B.** geen informatie geven die mogelijk gebruikt kan worden om voordeel ten koste van de andere ouder te behalen	
C		Ouders die hun partnerschap hebben laten registreren	**X**	
D		Ouders die niet met elkaar zijn getrouwd, maar via goedkeuring van de rechtbank het gezamenlijk gezag uitoefenen	**X**	
E		Ouder die **niet** met het gezag is belast		X artikel 1:377c BW
F		In geval van samenwonen, vader heeft kind erkend, **niet** ingeschreven in gezagsregister; voor **vader** geldt:		X artikel 1:377c BW
G		In geval van samenwonen, vader heeft kind erkend en ingeschreven in gezagsregister; **voor vader en moeder** geldt:	**X**	
H		Stel heeft samengewoond, nu uit elkaar, kind is erkend, ingeschreven in gezagsregister; voor **vader en moeder** geldt:	X **N.B.** geen informatie geven die mogelijk gebruikt kan worden om voordeel ten koste van de andere ouder te behalen	
I		Stel heeft samengewoond, nu uit elkaar, kind is erkend, maar niet ingeschreven in het gezagsregister; voor **vader** geldt:		X artikel 1:377c BW

		Voor wie	**Alle informatie**	**Beperkte informatie** *(erkend)*
J		Ouders beide uit de ouderlijke macht gezet, kind is onder voogdij geplaatst; voor **vader en moeder** geldt:		X artikel 1:377c BW
K		Voogd	**X**	
L		Biologische vader, die zijn kind niet heeft erkend		
M		Grootouders die de verzorging van het kind op zich nemen omdat de ouders spoorloos zijn.		

L: Voor de biologische vader, die zijn kind niet heeft erkend, geldt dus: helemaal geen informatie.
M: Voor grootouders, die de verzorging van de kinderen op zich nemen, omdat de ouders spoorloos zijn geldt: **in principe geen** informatie.

Bijlage 5b Genomen stappen rechten van betrokken

Rechten van betrokken genomen stappen

Verzoek:

- ☐ **Inzage**
- ☐ **Copy**
- ☐ **Correctie**
- ☐ **Aanvulling**
- ☐ **Mening toevoegen**
- ☐ **Overdracht**
- ☐ **Wijziging**
- ☐ **Vernietiging**
- ☐ **Beperking**

Betreft ll dossiernummer:
Intern nummer:

Stap/vraag	Datum	Omschrijving / vraag	Uitgevoerd door
Ontvangst verzoek			
Controle identiteit*			
Overleg leerkracht/ bestuurder /			
Verzoek behandelen			
Overleg FG			

Controle identiteit kan bijvoorbeeld als er een verzoek binnen is gekomen per mail; check uitvoeren of dit mail adres bekend is in het LAS systeem.
In sommige gevallen (bij verzoeken om bijzondere persoonsgegevens) kan controle door middel van ID wenselijk zijn.

FG inschakelen bij complexe zaken en de termijn van reageren ligt binnen 4 weken.

Bijlage 6 Protocol datalekken

Protocol beveiligingsincidenten en datalekken stichting Bravoo

Stichting Bravoo
Kaatsheuvel, 28 mei 2019
Versie juli 2021

Inhoudsopgave

Inleiding

Dit protocol biedt een handleiding voor de professionele melding, beoordeling en afhandeling van beveiligingsincidenten en datalekken. Het doel hiervan is het voorkomen van beveiligingsincidenten en datalekken.
Dit protocol is van toepassing op alle scholen binnen Stichting Bravoo, zoals vermeld in het IBP-beleid en al haar medewerkers.

Gebruikte termen:

- **Beveiligingsincident**: Een gebeurtenis die ervoor 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 school.
- **Datalek:** Een beveiligingsincident waarbij persoonsgegevens verloren raken of onrechtmatig worden bewerkt (opgeslagen, aangepast, verzonden enzovoorts). Alle datalekken zijn beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken.
- **Betrokkene:** De persoon van wie de persoonsgegevens zijn gelekt.

Wet- en regelgeving datalekken

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

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

Beveiligingsincident datalek

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 in zo'n geval informatie 'gelekt'.

Voorbeelden van beveiligingsincidenten zijn:

- Verlies of diefstal van waardepapier, dossier, usb-stick, tablet of andere gegevensdragers
- Niet naleven van beleid of richtlijnen
- Inbreuk op fysieke beveiligingsvoorzieningen
- Toegangsovertredingen
- Opzettelijk foutief handelen (fraude, diefstal)
- Beschadigen of vernielen van (kritische) apparatuur
- Virusbesmetting als gevolg van het aanklikken van een onbetrouwbare bijlage
- Onbevoegd inzien van vertrouwelijke informatie
- Onbedoelde openbaarmaking van vertrouwelijke informatie
- Geen gescreend personeel
- Illegale licenties
- Illegaal kopiëren van gegevens
- E-mail met onversleutelde vertrouwelijke informatie
- Kenbaar maken van of onzorgvuldig omgaan met wachtwoorden

Maar ook cyberaanvallen zoals een DDoS-aanval, computerhacking of besmetting met ransomware, alsmede het technisch falen van apparatuur, stroomuitval, wateroverlast en dergelijke zijn aan te merken als incidenten.

Uitgangssituatie
- Er is een actueel informatiebeveiligings- en privacybeleid;
- Er is een actueel document betreffende het aanvaardbaar gebruik van bedrijfsmiddelen en/of gedragscode ict en internetgebruik.

De vier rollen

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

1. **A: Ontdekker (medewerker):** Degene die het beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
   B: Ontdekker (externe): Een ouder of verwerker die een beveiligingsincident of datalek op het spoor komt en het proces in werking stelt.
2. **Meldpunt (Security Officer of Functionaris voor Gegevensbescherming):** Een aanspreekpunt binnen de school waar alle beveiligingsincidenten worden geregistreerd en verder worden verwerkt.
3. **Melder (Functionaris voor Gegevensbescherming):** Degene die verantwoordelijk is voor het melden van een datalek bij de Autoriteit Persoonsgegevens.
4. **Technicus (Security Officer of externe ict-dienstverlener):** Degene die de oorzaak van het datalek kan vinden en kan (laten) repareren.

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is het College van Bestuur. De FG doet in overleg met de verantwoordelijke (bestuurder) de melding. De verwerker kan een melding doen, echter dit is dan afgesproken met de verantwoordelijke.

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

De stappen

a) 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 Security Officer: **privacy@stichtingbravoo.nl**

b) Inventariseren

Het Meldpunt bepaalt aan de hand van een formulier 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 in het formulier vastgelegd:

Samenvatting van het beveiligingsincident, wat er met de gegevens is gebeurd, wat voor gegevens het zijn (bijzondere gegevens of van gevoelige aard)

Datum/periode van het beveiligingsincident

Aard van het beveiligingsincident

Wanneer van toepassing (bij een datalek):

a. Omschrijving van de groep betrokkenen
b. Aantal betrokkenen
c. Type persoonsgegevens
d. Worden de gegevens binnen een keten (bijvoorbeeld een samenwerkingsverband) gedeeld?

c) Beoordelen

Wanneer het Meldpunt (Security Officer) voldoende informatie heeft verzameld en een datalek vermoedt, stuurt deze de Functionaris voor Gegevensbescherming (FG) een verzoek om de verzamelde informatie te bekijken. De FG beoordeelt de feiten om te bepalen of een melding aan de Autoriteit persoonsgegevens en/of betrokkene(n) vereist is.

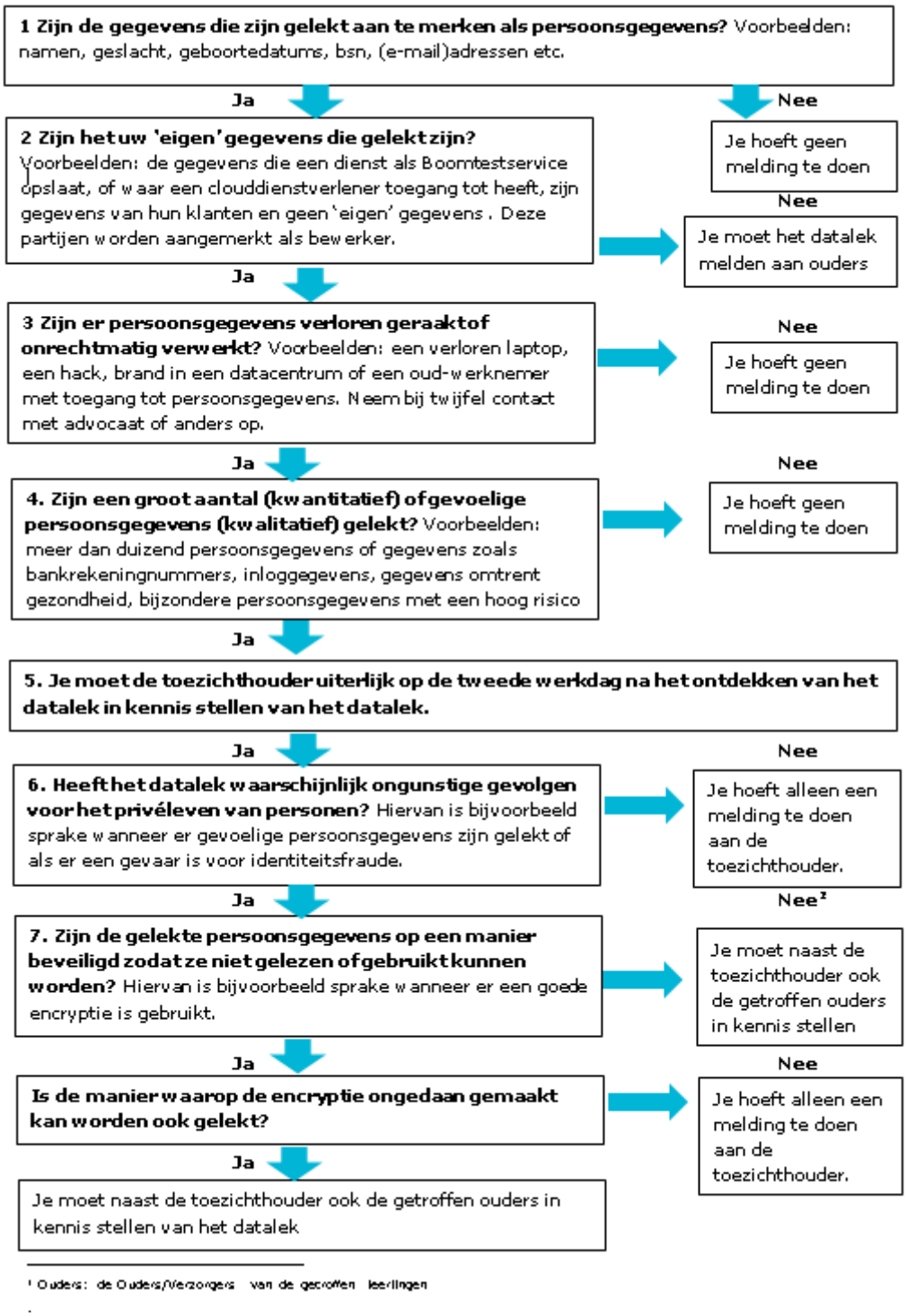
De volgende informatie wordt vastgelegd door de Functionaris voor Gegevensbescherming (FG):

- Impact van de melding
- Type gegevens dat verloren gegaan is
- Mogelijke gevolgen voor de persoonlijke levenssfeer van de betrokkenen
- Aard van de inbreuk
- Zijn de gegevens uitbesteed aan een verwerker?
- Aantal 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?
- Wordt er melding gedaan via de pers?

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', wordt er rekening gehouden met het type en de hoeveelheid gegevens.
Indien het datalek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens, **moet** er gemeld worden.
Van die ernstige nadelige gevolgen of de kans op ernstige nadelige gevolgen 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 of economische situatie van de betrokkene, of als de gegevens kunnen leiden tot stigmatisering van de betrokkene.

Jaarlijks worden zowel de raad van toezicht als de GMR ingelicht over het aantal meldingen en de genomen maatregelen. Indien er sprake is van een ernstig en/of 'groot' datalek zal de raad van toezicht en de GMR eerder ingelicht worden.

De beslisboom op de volgende pagina kan worden gebruikt:


1 Zijn de gegevens die zijn gelekt aan te merken als persoonsgegevens? Voorbeelden: namen, geslacht, geboortedatums, bsn, (e-mail)adressen etc.
Ja
Nee
Je hoeft geen melding te doen
2 Zijn het uw 'eigen' gegevens die gelekt zijn? Voorbeelden: de gegevens die een dienst als Boomtestservice opslaat, of waar een clouddienstverlener toegang tot heeft, zijn gegevens van hun klanten en geen 'eigen' gegevens. Deze partijen worden aangemerkt als bewerker.
Nee
Je moet het datalek melden aan ouders
Ja
3 Zijn er persoonsgegevens verloren geraakt of onrechtmatig verwerkt? Voorbeelden: een verloren laptop, een hack, brand in een datacentrum of een oud-werknemer met toegang tot persoonsgegevens. Neem bij twijfel contact met advocaat of anders op.
Nee
Je hoeft geen melding te doen
Ja
4. Zijn een groot aantal (kwantitatief) of gevoelige persoonsgegevens (kwalitatief) gelekt? Voorbeelden: meer dan duizend persoonsgegevens of gegevens zoals bankrekeningnummers, inloggegevens, gegevens omtrent gezondheid, bijzondere persoonsgegevens met een hoog risico
Nee
Je hoeft geen melding te doen
Ja
5. Je moet de toezichthouder uiterlijk op de tweede werkdag na het ontdekken van het datalek in kennis stellen van het datalek.
Ja
6. Heeft het datalek waarschijnlijk ongunstige gevolgen voor het privéleven van personen? Hiervan is bijvoorbeeld sprake wanneer er gevoelige persoonsgegevens zijn gelekt of als er een gevaar is voor identiteitsfraude.
Nee
Je hoeft alleen een melding te doen aan de toezichthouder.
Ja
7. Zijn de gelekte persoonsgegevens op een manier beveiligd zodat ze niet gelezen of gebruikt kunnen worden? Hiervan is bijvoorbeeld sprake wanneer er een goede encryptie is gebruikt.
Nee[2]
Je moet naast de toezichthouder ook de getroffen ouders in kennis stellen
Ja
Is de manier waarop de encryptie ongedaan gemaakt kan worden ook gelekt?
Nee
Je hoeft alleen een melding te doen aan de toezichthouder.
Ja
Je moet naast de toezichthouder ook de getroffen ouders in kennis stellen van het datalek
[1] Ouders: de Ouders/Verzorgers van de getroffen leerlingen

d) Repareren

- De Security Officer wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De Security Officer legt onderstaande vast:
- Technische en organisatorische maatregelen die genomen zijn om de inbreuk te verhelpen en verdere inbreuk te voorkomen. Voorgaande voor zover de oorzaak bekend is.
- Zijn de gelekte gegevens onbegrijpelijk voor degenen die er kennis van heeft kunnen nemen? Hoe zijn de gegevens onbegrijpelijk gemaakt (versleuteld)?

Herstelaanpak datalekken

- Bij de herstelaanpak wordt rekening gehouden met de volgende twee vragen:
- Hoe herstel je de schade bij betrokkenen?
    - Wat kun je doen om betrokkenen te ondersteunen in het beperken van de schade door een datalek?
    - Op welke wijze ga je deze nazorg leveren?
    - Wie worden hierbij betrokken? *(denk aan leverancier, bestuurder, HRM)*
- Hoe herstel je de schade van de school?
    - Op welke wijze kan de schade van de school beperkt blijven dan wel hersteld worden?
    - Wie worden hierbij betrokken? *(leverancier, MT en bestuurder, HRM)*
    - Maakt het datalek de uitvoering van een bedrijfsproces onmogelijk en bestaat daarvoor een alternatieve werkwijze?
    - Wat voor acties ga je ondernemen om de reputatieschade te beperken en om de reputatie te herstellen?
    - Wat voor acties ga je ondernemen rondom de afwikkeling van aansprakelijkheidsstelling en boetes?
    - Welke acties worden ondernomen ter voorkoming en voor de communicatie aan medewerkers?

e) Melden

Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan moet dat worden doorgegeven aan de Security officer, Mechi de Veer, via privacy@stichtingbravoo.nl, 0416-283103 en aan de leidinggevende van de school. Mocht Mechi niet bereikbaar zijn, dan mag de melding rechtstreeks gedaan worden aan de Functionaris voor Gegevensbescherming: Angela Groen: a.groen@cedgroep.nl, 010-4071998. De Functionaris voor Gegevensbescherming (FG) zal de melding binnen 72 uur in overleg met de bestuurder doen. De melding bevat alle verzamelde informatie en de getroffen incidentele en structurele technische en organisatorische maatregelen. Het lek wordt gemeld bij het meldloket datalekken: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.

f) Vastleggen

Alle informatie die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de Functionaris voor Gegevensbescherming (FG) waarmee het incident is afgesloten. De FG verstuurt een samenvatting van de genomen maatregelen aan de Security Officer en deze stuurt door naar de Ontdekker.

g) Informeren betrokkenen

Heeft het datalek waarschijnlijk ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkenen? Dan moet het datalek ook aan de betrokkenen zelf worden gemeld. Dat zijn medewerkers en leerlingen (of hun ouders als zij jonger zijn dan 16 jaar). In principe kan ervan worden uitgaan dat lekken van gevoelige aard gemeld moeten worden bij de betrokkenen.

Let op: als er persoonsgegevens zijn gelekt maar deze 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.

Stappenplan

Onderstaande stappen wordt gebruikt voor communicatie naar de medewerkers.

	Procedurestap	Termijn	Wie
1	**Beveiligingsincident** 1. Verlies USB stick 2. Verlies iPad, smartphone, laptop 3. Verzending naar verkeerd mailadres 4. Verlies dossier 5. Onbevoegde die toegang had tot netwerk of bestand 6. Phishing 7. Hacking		Ontdekker lek
1	**Beveiligingsincident** melden bij Security Officer en direct leidinggevende **privacy@stichtingbravoo.nl**	Direct	Ontdekker lek
1a	Indien telefoon verloren etc. direct gaan blokkeren (ook privé telefoon)	Direct	Security Officer
1b	Ook persoonsgegevens gelekt? Dan ook melden bij functionaris gegevensbescherming (FG) **FG:** Angela Groen a.groen@cedgroep.nl	Direct	Ontdekker lek / Security Officer/ Directeur
2	In behandeling nemen beveiligingsincident	Direct	FG
3	Maatregelen treffen om datalek te stoppen	Direct	Security Officer i.o.m. FG
3a	Informeren bestuurder over datalek	Direct	FG
4	Beoordelen of er sprake is van een datalek dat gemeld moet worden aan de Autoriteit Persoonsgegevens (AP) • Of er sprake is van een datalek dat gemeld moet worden aan de Autoriteit Persoonsgegevens (AP) • Of betrokkene(n) van wie gegevens gelekt zijn geïnformeerd moet(en) worden • Of er actie ondernomen moet worden naar derden: 1. Informatie 2. Maatregelen 3. Onderzoek • Of de rvt e/o GMR geïnformeerd moeten worden • Of externe communicatie nodig is	Binnen 72 uur na ont-dekken van lek	FG in overleg met: 1. Medewerker /Directeur 2. Direct leidinggevende 3. Bestuurder
5	Informeren bestuurder over stand van zaken en beoordeling	Binnen 72 uur	FG
6	Bij meldingsplichtig datalek: melden bij AP via meldloket: https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0	Binnen 72 uur	FG
7	Als betrokkene(n) van wie gegevens gelekt zijn geïnformeerd moet(en) worden, versturen kennisgeving met vermelding van: 1. Aard inbreuk 2. Contactgegevens 3. De maatregelen die betrokkene kan nemen om negatieve gevolgen te beperken	Zo snel mogelijk, uiterlijk binnen 72 uur	FG in overleg met medewerker / directeur die gegevens verwerkt

	Afhankelijk van de omvang van het datalek overwegen om andere kanalen in te zetten.		FG in overleg met bestuurder
7a	Externe communicatie (indien nodig)	Zo snel mogelijk	Bestuurder/ directeur /FG en PR/communicatie
7b	Controle op effectiviteit van de afhandeling van incidenten en datalekken per kwartaal	FG	Per kwartaal
7c	Jaarlijkse rapportage over aantal datalekken aan rvt en GMR	Per jaar	FG i.o.m. bestuurder

Bijlage 7 Toegangsmatrix

Stichting Bravoo heeft de afweging gemaakt om in 2020-2021 gefaseerd over te stappen van ESIS naar Parnassys. De toegangsmatrix van Parnassys wordt hier opgenomen.

Toegangsmatrix Parnassys

Functies/rollen	**Rol in ParnasSys**	**Werkzaamheden**	**Niveau van toegang**	**2FA**
Bovenschools				
Algemene directie	Monitororganisatie beheerder	Sturing en beleid	Stichting	Ja, uitrol in 2022
Accountbeheerder ParnasSys*	Monitororganisatie beheerder Accountbeheerder	Beheer	Stichting	Ja, uitrol in 2022
School				
Leerkrachten	Leerkracht	Verzorgen onderwijs	Groep	Ja, uitrol in 2022
Onderwijsassistent	Leerkracht	Verzorgen onderwijs	Groep	Ja, uitrol in 2022
Invalleerkracht (>1 week)	Leerkracht	Verzorgen onderwijs	Groep	Ja, uitrol in 2022
Lio-stagiaire	Leerkracht Beperkt	Verzorgen onderwijs	Groep	Ja, uitrol in 2022
Directeur	Schooladministrateur	Sturing en beleid	School	Ja, uitrol in 2022
Intern begeleider	Intern Begeleider	Leerlingzorg Overdracht leerlingdossier via OSO	School of (sub)-groep	Ja, uitrol in 2022
Administratief medewerker	Administratie Schooladministrateur Inschrijven OSO Uitschrijven BRON	Administratie-taken	School	Ja, uitrol in 2022
Applicatiebeheerder schoolniveau Deze rol kan bij Directeur, IB-er of ICT-er belegd worden, afhankelijk van het taakbeleid van de school.	Beheer digitaal rapport Beheer evt. ouderportaal Beheer toetsen en vakken Map	Beheer	School	Ja, uitrol 2022
Verantwoordelijke absentieregistratie	Verzuimcoördinator	Beheer absentie en verzuim	School	Ja, uitrol in 2022

* Dit is een rol binnen de organisatie die als enige de accounts kan aanmaken en verwijderen.
** Deze rol is nodig voor het kunnen uitwisselen met OSO (Overstap Service Onderwijs).

Bijlage 8 Gedragscode ICT en Internet

Gedragscode voor verantwoord gebruik van bedrijfsmiddelen/ICT voor medewerkers van de scholen van stichting Bravoo

Stichting Bravoo
Kaatsheuvel, 28 mei 2019
Versie juli 2021

Deze gedragscode sluit aan bij het informatiebeveiliging en privacy beleid (IBP-beleid) van Stichting Bravoo.
De gedragscode geeft aan wat het IBP-beleid voor medewerkers in de praktijk betekent en legt vast wat er van de medewerkers verwacht wordt met betrekking tot het gebruik van de ter beschikking gestelde bedrijfsmiddelen en de inzet van eigen devices voor schoolwerkzaamheden.

- Hoofdstuk 1 'Inleiding' beschrijft wat onder bedrijfsmiddelen verstaan wordt, de uitgangspunten van de gedragscode en de driedeling van gegevens (openbaar, intern en vertrouwelijk) die verwerkt worden.
- Hoofdstuk 2 'Gedragscode' bevat de 'bouwstenen' waarmee de afspraken kunnen worden vastgelegd die relevant zijn voor de gewenste gedragscode van een school. Elke school kan met de bijbehorende paragrafen een gedragscode 'op maat' maken.
- Per onderwerp en/of per onderdeel (bullet) binnen een onderwerp kunnen keuzes en aanpassingen gemaakt worden.
- Hoofdstuk 3: 'Controle gebruik bedrijfsmiddelen' beschrijft de voorwaarde van controle, de uitvoering ervan, de eventuele sancties en de mogelijkheid van bezwaar maken.
- Hoofdstuk 4: 'GMR' laat de rol van de (G)MR zien.
- Hoofdstuk 5: 'Slotbepaling' toont de datum van de eerstvolgende evaluatie en eventuele aanpassing van de gedragscode.

Inhoud

Inleiding

Het gebruik van internet, computernetwerk, en e-mail is voor alle medewerkers van de school noodzakelijk om de werkzaamheden te kunnen verrichten. Bij deze werkzaamheden wordt gebruik gemaakt van veel gegevens, waaronder persoonsgegevens. De (ict)faciliteiten en de verschillende gegevens worden in dit document bedrijfsmiddelen genoemd.
Onder bedrijfsmiddelen worden in ieder geval verstaan:

- Hardware: *pc, laptop, tablet, telefoon, hardware token (tag).*
- Software (of -systemen): *alle applicaties voor het uitvoeren van de werkzaamheden, zoals de school e-mailomgeving, Microsoft Office, administratiesystemen en (online)digitaal lesmateriaal maar ook apps op (mobiele) devices.*
- Informatie en (persoons)gegevens: *rapportages, leerling dossiers, gegevens in e-mails. Hierbij vraagt de verwerking van persoonsgegevens vanuit de privacywetgeving extra maatregelen.*
- Internetgebruik: *het bezoeken van het World Wide Web, het gebruik van e-mail en diensten als FTP en maar ook sociale media zoals Facebook, LinkedIn, Instagram en Twitter.*

Aan het gebruik van deze bedrijfsmiddelen zijn risico's verbonden, waardoor het noodzakelijk is om hierover afspraken te maken. Van medewerkers van Stichting Bravoo wordt verwacht dat zij verantwoord omgaan met de beschikbaar gestelde bedrijfsmiddelen. Dit wordt ook verwacht als medewerkers hun eigen middelen inzetten om werkzaamheden voor de school uit te voeren.

De afspraken in dit document gelden voor alle locaties van waaruit (school)werkzaamheden worden verricht en voor alle devices waarmee het werk wordt uitgevoerd. Ze gelden voor iedereen die werkzaam is bij Stichting Bravoo, ook voor uitzendkrachten en tijdelijke werknemers.

Uitgangspunten gedragscode

Deze gedragscode legt regels vast voor het gebruik van de bedrijfsmiddelen door medewerkers en over de controle op de naleving hiervan.
Het doel van deze gedragscode is om de normen en uitgangspunten vast te leggen ten aanzien van:

- systeem- en netwerkbeveiliging, inclusief beveiliging tegen schade en misbruik
- het tegengaan van seksuele intimidatie, discriminatie en andere strafbare feiten
- de bescherming van privacy gevoelige informatie waaronder persoonsgegevens van het schoolbestuur, haar medewerkers, leerlingen en hun ouders en daarmee het beschermen van de privacy en veiligheid van alle betrokkenen
- de bescherming van vertrouwelijke informatie van het schoolbestuur, haar medewerkers, leerlingen en hun ouders
- het voorkomen en tegengaan van misbruik van de bedrijfsmiddelen
- de bescherming van de intellectuele eigendomsrechten van het schoolbestuur en derden
- het voorkomen van negatieve publiciteit
- kosten- en capaciteitsbeheersing

De controle op het gebruik van bedrijfsmiddelen is een verwerking van persoonsgegevens in de zin van de privacywetgeving. Stichting Bravoo zal dan ook de controle en handhaving van deze regels conform de privacywetgeving en het algemene arbeidsrechtelijk kader uitvoeren. Hierbij is het uitgangspunt een goede balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers op de werkplek. Gegevens worden alleen

verzameld en gebruikt voor deze doelen. In het bijzonder zal het bestuur de bij controle vastgelegde gegevens beveiligen tegen ongeautoriseerde toegang (via Insite, Miloo, etc.). Bij het aangaan van een dienstverband bij stichting Bravoo wordt tevens akkoord gegaan met geheimhouding van vertrouwelijke gegevens volgens de algemene wet en regelgeving.

Het schoolbestuur streeft in het kader van handhaving van dit document naar maatregelen die inzage in privacygevoelige informatie of persoonsgegevens van individuele medewerkers zo veel mogelijk beperken. Zij zal waar mogelijk slechts geautomatiseerd controleren of filteren zonder daarbij zichzelf of andere personen inzage te geven in het gedrag van individuele personen.

Eigen verantwoordelijkheid en privégebruik

Het gebruik van door Stichting Bravoo verstrekte bedrijfsmiddelen is persoonlijk en blijft de verantwoordelijkheid van de medewerker. Alle devices die voor schoolwerk worden gebruikt (inclusief eigen devices 'Own Device') worden niet uitgeleend of aan anderen ter beschikking gesteld zonder aanvullende (beveiligings)maatregelen. Het niet voldoen aan de regels voor informatiebeveiliging en privacy kan leiden tot disciplinaire maatregelen.

Verschillende soorten gegevens

Stichting Bravoo is verantwoordelijk voor het regelen van informatiebeveiliging en privacy. Het belangrijkste doel van informatiebeveiliging en privacy is het beschermen van gegevens. Stichting Bravoo onderscheidt drie typen gegevens:

- Openbare gegevens; dit zijn gegevens die juist voor publicatie bedoeld zijn.
- Interne gegevens; dit zijn gegevens die alleen voor gebruik en verwerking binnen Stichting Bravoo bedoeld zijn. Denk na voordat je deze gegevens deelt met externen.
- Vertrouwelijke gegevens; dit zijn gegevens die alleen voor specifieke, hiervoor geautoriseerde medewerkers binnen Stichting Bravoo toegankelijk zijn. Denk hierbij aan (bijzondere) persoonsgegevens, personeelsgegevens of aanbestedingsgegevens.

Persoonsgegevens verdienen bijzondere aandacht. Dit zijn gegevens die een persoon betreffen én waardoor een persoon geïdentificeerd of identificeerbaar is. Denk hierbij aan naamgegevens, emailadressen maar ook telefoonnummers van zowel collega's als leerlingen en ouders van leerlingen.

De privacywetgeving verplicht elk individu om zorgvuldig met persoonsgegevens om te gaan. Een onderdeel van de wettelijke verplichting is dat Stichting Bravoo schriftelijk afspraken maakt met leveranciers van (online)applicaties, waarbij persoonsgegevens worden verwerkt (denk hierbij aan inloggegevens, wachtwoorden en het opslaan van gemaakt werk).
Stichting Bravoo beschikt intern over een Security Officer en extern over een Functionaris gegevensbescherming. Deze communiceren intern de gedragsregels die horen bij het verwerken van persoonsgegevens. Persoonsgegevens moeten altijd met uiterste zorgvuldigheid verwerkt en gedeeld worden.

Als persoonsgegevens toegankelijk en of inzichtelijk zijn voor personen, die geen toegang behoren hebben tot deze gegevens is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Een dergelijk incident kan schadelijke gevolgen hebben voor de betrokkene(n) en Stichting Bravoo.
Om op een veilige, verantwoorde en werkbare manier met deze gegevens om te gaan maakt Stichting Bravoo afspraken over:

- de verwerking en verspreiding van vertrouwelijke- en persoonsgegevens. Er worden niet meer gegevens verwerkt dan noodzakelijk om het doel te bereiken
- de uitwisseling van gegevens, waarbij aan de ontvanger wordt aangegeven wat de ontvanger wel of niet mag doen met de gegevens
- opslag en verspreiding van gegevens, waarbij alléén gebruik gemaakt wordt van door Stichting Bravoo aangeschafte bedrijfsmiddelen.

Van medewerkers van Stichting Bravoo en/of externe medewerkers, die uit hoofde van hun functie toegang hebben tot de digitale informatiesystemen en hiermee tot bv. personeelsdossiers, vertrouwelijke enquêtegegevens, zorgdossiers et cetera wordt verwacht dat zij zorgvuldig omgaan met de functioneel aan hen beschikbaar gestelde informatie. Dat zij de privacywetgeving hanteren en op geen enkele wijze informatie, waarvan redelijkerwijze kan worden aangenomen dat deze vertrouwelijk of privacygevoelig is, zonder toestemming van betrokkene of leidinggevende te gebruiken en/of naar buiten te brengen.

Gedragscode

In deze gedragscode voor verantwoord gebruik van bedrijfsmiddelen geeft Stichting Bravoo aan wat de afspraken zijn met betrekking tot verschillende onderwerpen rondom het gebruik van bedrijfsmiddelen en wat dit voor de medewerkers in de dagelijkse praktijk betekent.

Algemene normen

Iedere medewerker voldoet aan de volgende algemene normen voor 'zorgvuldigheid' (niet uitputtend):

- Ga zorgvuldig om met persoonsgegevens, waarbij de basisregels voor het omgaan met persoonsgegevens als bekend worden geacht.
- Voorkom het lekken van interne en vertrouwelijke informatie.
- Zorg voor een goede fysieke en technische bescherming van bedrijfsmiddelen. (beveiligingsmaatregelen).
- Voorkom dat beveiligingsmaatregelen moedwillig worden omzeild.
- Meld diefstal of verlies van bedrijfsmiddelen onmiddellijk na constatering door het sturen van een e-mail aan privacy@stichtingbravoo.nl en de direct leidinggevende of een telefonische melding bij de daarvoor aangewezen persoon (Zie hiervoor de procedure meldplicht datalekken van Stichting Bravoo).

Computergebruik

Voor het uitoefenen van de werkzaamheden stelt Stichting Bravoo aan de medewerker computer- en netwerkfaciliteiten (ict-bedrijfsmiddelen) ter beschikking. Het gebruik van deze ict-bedrijfsmiddelen is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:

- Zorg dat privacygevoelige gegevens niet toegankelijk zijn voor onbevoegden.
- Weet welke gegevens er mogen worden gebruikt (mag iedereen het zien?) en welke ict-voorzieningen kunnen worden ingezet (is het veilig genoeg?) bij het verrichten van de verschillende schoolwerkzaamheden.
- Sla (persoons)gegevens alleen op de daarvoor aangewezen systemen op. (Opslaan van gegevens in public Cloud omgevingen, zoals een persoonlijke dropbox of persoonlijke OneDrive, is niet toegestaan).
- Versleutel alle gegevens met betrekking tot Stichting Bravoo, indien deze gegevens, om welke reden dan ook, elders opgeslagen worden.
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.
- Sluit na gebruik de computer af of log uit.

- Meld storingen van beheerde werkplekken (computer of laptop) bij de ict-er van school en/of Skool.
- Wanneer er apparaten worden gebruikt die niet beheerd worden door Bravoo, wordt nooit de synchronisatiefunctie binnen 0365 aangezet. Er wordt alleen rechtstreeks in de cloud gewerkt en uitgelogd aan het einde van elke sessie.

Werkplek

Voorkom dat anderen (onbedoeld) toegang kunnen krijgen tot bedrijfsmiddelen waartoe zij geen rechten hebben en/of laat gegevens niet (onbedoeld) lekken. Als aanvullende regels op computergebruik gelden voor de werkplek de volgende clean desk en clear screen regels:

- Vergrendel bij het tijdelijk verlaten van de werkplek de pc (windowstoets+L).
- Verwijder interne en vertrouwelijke documenten van het bureau bij het voor langere tijd verlaten van de werkplek (denk hieraan bij het bijwonen van een vergadering).
- Voorkom dat gevoelige en vertrouwelijke informatie zichtbaar is wanneer iemand anders op het beeldscherm (of via een beamer) mee kan kijken. Sluit het e-mail programma af en zorg voor een opgeruimd digitaal bureaublad.
- Medewerkers printen via een beveiligingscode.
- Leerlingen printen via de leerkracht.
- Haal overbodig geworden papieren documenten met persoonsgegevens erop altijd door de papierversnipperaar.
- Berg de klassenmap altijd goed op bij het verlaten van het lokaal en de klassenmap bevat geen onnodige persoonsinformatie.

LET OP: Als persoonsgegevens toegankelijk/inzichtelijk zijn voor personen, die geen toegang behoren te hebben tot die gegevens is er sprake van een beveiligingsincident, waaruit mogelijk een datalek kan voortkomen. Weet dat beveiligingsincidenten en mogelijke datalekken gemeld moeten worden volgens de procedure meldplicht datalekken van Stichting Bravoo. Datalekken worden gemeld via privacy@stichtingbravoo.nl en de direct leidinggevende.

Gebruik eigen devices (BYOD)

Beveiligingsmaatregelen hebben betrekking op alle devices waarmee werkzaamheden voor Stichting Bravoo worden uitgevoerd. Stichting Bravoo is verantwoordelijk voor het implementeren van de juiste beveiligingsmaatregelen als het gaat om de bedrijfsmiddelen van de school.

Voor 'Own Devices' ligt de verantwoordelijkheid voor adequate beveiligingsmaatregelen bij de medewerker zelf. Van de medewerker wordt verwacht dat minimaal de volgende beveiligingsmaatregelen worden genomen:

- Beveilig het device bij voorkeur met een wachtzin, of in het geval van een smartphone of tablet, met een pincode die langer is dan 4 tekens.
- Vergrendel het device bij het verlaten van de werkplek (windowstoets+L).
- Sla persoonsgegevens van Stichting Bravoo niet op het eigen device op; dit is niet toegestaan.
- Versleutel alle gegevens, anders dan persoonsgegevens, met betrekking tot Stichting Bravoo als deze, om welke reden dan ook, niet op het schoolnetwerk opgeslagen worden (denk hierbij aan het eigen device).
- Scheid (versleutelde)gegevens, anders dan persoonsgegevens, van Stichting Bravoo en privégegevens van elkaar. Deze scheiding moet duidelijk herkenbaar zijn op het eigen device.

- Houd software up-to-date door het uitvoeren van periodieke updates (minimaal maandelijks).
- Neem adequate maatregelen tegen virussen of malware door het up-to-date houden van de virusscanner en door het periodiek (minimaal maandelijks) scannen van het device.

Stichting Bravoo mag controles uitvoeren op bovenstaande maatregelen. Op verzoek van Stichting Bravoo moet de medewerker zelf aantonen dat de bovenstaande maatregelen worden toegepast.

Software en digitaal lesmateriaal

Het gebruik van digitaal lesmateriaal is niet meer weg te denken bij Stichting Bravoo. Dit lesmateriaal staat steeds meer online waarbij steeds vaker persoonsgegevens worden uitgewisseld. De privacywetgeving eist dat elke organisatie vooraf aan het gebruik van dergelijk materiaal bekijkt wat de invloed ervan is op de privacy, dit kan specifieke maatregelen tot gevolg hebben.
De onderstaande regels gelden voor installatie en gebruik van software en (online)digitaal lesmateriaal:

- Installeren van software wordt bij Stichting Bravoo alleen toegestaan met de juiste licenties en na het nemen van eventuele aanvullende maatregelen.
- Bij het gebruik van online software, app's en digitaal lesmateriaal, wordt gekeken of er persoonsgegevens bij verwerkt worden.
- Een verwerkersovereenkomst wordt op bestuursniveau afgesloten met elke leverancier van (online)software, die in opdracht van Stichting Bravoo persoonsgegevens verwerkt. Regel dit vooraf aan het gebruik.
- Aanvragen van digitaal lesmateriaal en/of andere software loopt altijd via de schooldirecteur.

Gebruik van e-mail en chatfunctie

Stichting Bravoo stelt een e-mailsysteem en een bijbehorende mailbox aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik van e-mailfaciliteiten is verbonden aan deze werkzaamheden en gaan uit van de volgende afspraken:

- Gebruik het school e-mail adres alléén voor school gerelateerde zaken.
- Gebruik voor privé e-mail een eigen privé e-mailadres via een externe webmaildienst. (bijvoorbeeld webmail van Gmail, Hotmail of een eigen provider).
- Ontvangen van privémail op het school e-mailadres is incidenteel toegestaan.
- Het versturen van e-mail moet voldoen aan de normale gedragsregels die gelden voor schriftelijke correspondentie.
- Het is niet toegestaan e-mail te gebruiken voor berichten met pornografische, racistische, discriminerende, beledigende, (seksueel) intimiderende of aanstootgevende inhoud of voor berichten die kunnen aanzetten tot haat en geweld.
- Synchroniseert een medewerker de school e-mail met een eigen devices (tablet, telefoon) dan kan Stichting Bravoo, bij verlies of diefstal van het device, gebruik maken van de mogelijkheid om de e-mail op afstand te wissen, ook als daarmee alle (privé)gegevens van het device gewist worden.
- Bij langdurige afwezigheid kan de bestuurder besluiten de mailbox te laten openen om lopende zaken voortgang te geven.
- Bij het vermoeden van misbruik van een van bovenstaande punten, kan de bestuurder ook besluiten de mailbox te openen. Hier ligt een gemotiveerd besluit onder.

Gebruik van internet

Stichting Bravoo stelt het gebruik van internet en de bijbehorende faciliteiten aan de medewerker ter beschikking voor het uitoefenen van de werkzaamheden. Gebruik hiervan is verbonden aan deze werkzaamheden en gaat uit van de volgende afspraken:

- Beperkt persoonlijk gebruik is toegestaan, mits dit
  - niet storend is voor de dagelijkse werkzaamheden
  - niet voor commerciële doeleinden is en
  - geen verboden gebruik oplevert.
- Het is niet toegestaan om
  - op internet sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten
  - films, muziek, software en overig auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron
  - onder lestijd internettoegang te gebruiken voor privédoeleinden
  - deel te nemen aan kansspelen.
- Het is verboden op dreigende, beledigende, seksueel getinte, racistische dan wel discriminerende toon te communiceren via online fora, sociale netwerken en andere vergelijkbare communicatienetwerken over alle aan school verbonden betrokkenen en activiteiten. Dit geldt in het bijzonder ook voor internetgebruik buiten het schoolnetwerk met betrekking tot aan de school verbonden betrokkenen en activiteiten.

Veilig online

We brengen met z'n allen steeds meer tijd online door. Hierbij worden steeds meer mobiele devices gebruikt. Menselijk (online)handelen staat veelal aan de basis van een datalek.
Stichting Bravoo verwacht van medewerkers dat zij:

- het onderscheid kennen tussen veilige en onveilige netwerken (openbare wifinetwerken) en websites
- bij het verwerken van persoonsgegevens alléén gebruik maken van bekende én beveiligde draadloze netwerken
- weten wat malware is, het kunnen herkennen en weten hoe te handelen
- terughoudend zijn met het online achterlaten van gegevens met betrekking tot Stichting Bravoo
- controleren of er daadwerkelijk van een bekend én beveiligd netwerk gebruik gemaakt wordt bij het bezoek aan openbare ruimtes. (Een netwerk kan bekend zijn omdat het een Stichting Bravoo netwerk is, of het eigen draadloze netwerk thuis is).

Sociale media

Sociale media is een verzamelnaam voor alle internettoepassingen die het mogelijk maken om informatie met elkaar te delen op een eenvoudige en vaak leuke manier. Het gaat hierbij niet alleen om informatie in de vorm van tekst (nieuws, artikelen). Ook geluid (podcasts, muziek) en beeld (fotografie, video) worden gedeeld via social media (Instagram, YouTube, Facebook, Twitter enz). De essentie van sociale media is dat iemand er informatie deelt over zichzelf, over anderen of over een bepaald onderwerp.
Voor gebruik van sociale media geldt als uitgangspunt dat het digitale gedrag op sociale media niet afwijkt van het real life gedrag binnen de school. Medewerkers zijn altijd de vertegenwoordiger van Stichting Bravoo ook als zij online een privémening verkondigen. Van belang is te beseffen dat je met berichten op sociale media (onbewust) de goede naam van de school en betrokkenen ook kunt schaden. Om deze reden vragen wij om bewust om te gaan met de sociale media.
Bij Stichting Bravoo gelden de volgende afspraken voor het gebruik van sociale media:

- Deel op verantwoorde wijze kennis via sociale media rekening houdend met de goede naam van Stichting Bravoo en iedereen die hierbij betrokken is.
- Maak bij onderwijs gerelateerde onderwerpen duidelijk of publicatie op persoonlijke titel of namens Stichting Bravoo gedaan wordt.
- Publiceer geen vertrouwelijke informatie en/of persoonsgegevens op sociale media.
- Publiceer geen beeldmateriaal van leerlingen en medewerkers zonder de uitdrukkelijke voorafgaande aantoonbare toestemming van ouders als de leerling jonger is dan 16 jaar of de leerling zelf als deze ouder is dan 16 jaar.
- Weet dat publicaties op sociale media altijd vindbaar (openbaar) en moeilijk vernietigbaar zijn. Medewerkers zijn persoonlijk verantwoordelijk voor wat zij publiceren.
- Neem contact op met een leidinggevende als er twijfel bestaat over een publicatie of over de raakvlakken met Stichting Bravoo.
- Het is medewerkers niet toegestaan om met een privé account 'vrienden' te worden met leerlingen en ouders op sociale media.
- Inzetten van sociale media in het lesprogramma is gebonden aan de toestemming van ouders als leerlingen jonger zijn dan 16 jaar.

Gebruik beeld- en geluidsmateriaal

Het gebruiken van beeld- en geluidsmateriaal, het delen van foto's, video's en geluidsfragmenten van leerlingen door medewerkers vallend onder Stichting Bravoo mag alleen als daar vooraf toestemming voor gegeven is door ouders als de leerling jonger is dan 16 jaar of de leerling zelf als deze ouder dan 16 jaar is. Zonder deze toestemming mogen geen foto's, video's en geluidsfragmenten van leerlingen gebruikt worden.

- Stichting Bravoo verwijst hierbij naar de richtlijn die is opgesteld voor het gebruik en toestemming van beeldmateriaal.
- Voor de afspraken rondom het delen van beeld- en geluidsmateriaal via sociale media gelden de richtlijnen die genoemd worden bij het gebruik van sociale media.

Wachtwoorden en pincodes

Het beveiligen van toegang tot het netwerk, diverse (online) applicaties en devices (pc, laptop, telefoon) begint met een goed wachtwoord. Een lang wachtwoord of een 'wachtzin' is beter dan een kort, complex wachtwoord. Voor het gebruik van wachtwoorden gelden onderstaande afspraken:

- Wachtwoorden moeten minimaal 9 tekens bevatten, met minstens drie van de volgende vier elementen : kleine letter, hoofdletter, cijfer of speciaal teken (!@#$%^&*()
- Pincodes (op telefoon of tablet) moeten langer zijn dan 4 tekens.
- Wachtwoorden moeten volgens de afspraken binnen Stichting Bravoo jaarlijks worden vervangen.
- Gebruik niet voor elke systeem hetzelfde wachtwoord.
- Deel wachtwoorden nooit, ook niet incidenteel. Wachtwoorden zijn persoonlijk.

Meldplicht Datalekken

Van alle medewerkers wordt verwacht dat zij beveiligingsincidenten en mogelijke datalekken melden volgens de procedure meldplicht datalekken van Stichting Bravoo.
Datalekken worden gemeld via privacy@stichtingbravoo.nl bij de direct leidinggevende.

Controle gebruik bedrijfsmiddelen

Stichting Bravoo handelt bij de controle op het gebruik van bedrijfsmiddelen binnen de geldende wet- en regelgeving, te weten:

- De Grondwet,
- Algemene Verordening Gegevensbescherming
- Wet Medezeggenschap Onderwijs (WMO)
- Burgerlijk Wetboek (BW)
- Wetboek van Strafrecht
- Cao PO

Het Stichting Bravoo zal bij controle rondom het gebruik van bedrijfsmiddelen op basis van deze gedragscode uitgaan van de juiste balans tussen verantwoord gebruik van bedrijfsmiddelen en de bescherming van de privacy van medewerkers.

Voorwaarden voor controle

- Controle van persoonsgegevens met betrekking tot gebruik van bedrijfsmiddelen vindt slechts plaats in het kader van handhaving van de doelen van deze gedragscode.
- Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen.
- Indien een medewerker of een groep medewerkers wordt verdacht van het overtreden van regels, kan gedurende een vastgestelde (korte) periode, in opdracht van Stichting Bravoo gerichte controle plaatsvinden.
- Controle beperkt zich in beginsel tot verkeersgegevens van het e-mail- en internetgebruik. Slechts bij zwaarwegende redenen vindt, in opdracht van Stichting Bravoo, controle op de inhoud plaats.
- Verboden e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt.
- Bij constatering van ongeoorloofd gebruik wordt dit onmiddellijk met de betrokken medewerker besproken. Stichting Bravoo zal de medewerker op verzoek inzage verschaffen in de gegevens over het eigen gebruik. De medewerker wordt gewezen op de consequenties wanneer niet wordt gestopt met het ongeoorloofd gebruik.
- E-mailberichten van leden van de GMR onderling, van vertrouwenspersonen, bedrijfsartsen en van een ieder die zich op grond van zijn functie op enige vertrouwelijkheid moet kunnen beroepen, worden in principe niet gecontroleerd. Dit geldt niet voor veiligheid van berichten. Ook hier kan bij zwaarwegende redenen van afgeweken worden.

Uitvoering van de controle

- De controle ter voorkoming van negatieve publiciteit en seksuele intimidatie en de controle in het kader van systeem- en netwerkbeveiliging vindt plaats op basis van content-filtering.
- De controle op het uitlekken van interne en vertrouwelijke gegevens vindt plaats op basis van steekproefsgewijze content-filtering. Verdachte berichten worden apart gezet voor nader onderzoek.
- De controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeers- en opslaggegevens.
- Controle op het gebruik van beeldmateriaal vindt plaats op basis van klachten of meldingen van derden, of steekproefsgewijs bij beeldmateriaal dat openbaar beschikbaar is.
- De afdeling ict, de systeembeheerder(s) zijn aan geheimhouding gebonden als men om technische redenen kennis moet nemen van persoonsgebonden informatie, behalve als enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

- Door Stichting Bravoo worden de nodige maatregelen getroffen, opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn.
- Door Stichting Bravoo worden passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies en/of tegen enige vorm van onrechtmatige verwerking.

Disciplinaire maatregelen

Bij het handelen in strijd met deze gedragscode of de algemeen geldende wettelijke regels, kan het bestuur van Stichting Bravoo, afhankelijk van de aard en de ernst van de overtreding, disciplinaire maatregelen treffen. Hieronder vallen o.a. een waarschuwing/berisping, schadevergoeding, aangifte bij de politie, overplaatsing, schorsing en/of beëindiging van de arbeidsovereenkomst.
Medewerkers die zich niet aan deze gedragscode houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken. Zij krijgen daarbij inzage in de over hen vastgelegde gegevens en hebben de gelegenheid te reageren op het geconstateerde. Medewerker en leidinggevende maken dan afspraken voor de toekomst en bepalen de mogelijke maatregelen bij overtreding daarvan. Deze afspraken kunnen strenger zijn dan het in deze gedragscode bepaalde. Ook kan de toegang tot e-mail of internet worden beperkt of geheel worden afgesloten. Disciplinaire maatregelen (behalve een waarschuwing) kunnen niet enkel op basis van een langs geautomatiseerde uitgevoerde verwerking van persoonsgegevens worden getroffen, zoals een constatering van een automatisch filter of blokkade. Er worden geen disciplinaire maatregelen getroffen zonder dat de medewerker gelegenheid heeft gekregen zijn zienswijze naar voren te brengen.

Bezwaar en beroep

Als de medewerker het niet eens is met de (voorgenomen) disciplinaire maatregel, dan kan daar in een aantal gevallen bezwaar en/of beroep tegen worden ingesteld. Dit is meestal geregeld in de arbeidsovereenkomst, regels rondom personeelszaken en/of de van toepassing zijnde CAO.

(G)MR

Dit document heeft betrekking op verwerking van persoonsgegevens en/of controle van het gedrag of de prestaties van medewerkers. Het medezeggenschapsorgaan (de (G)MR) is om deze reden instemmingsplichtig. Dit orgaan heeft op 11 juni 2019 ingestemd met de inhoud van deze gedragscode.

De organisatie kan deze gedragscode met instemming van de (G)MR wijzigen als de omstandigheden daar aanleiding toe geven. Voorgenomen wijzigingen worden voorafgaand aan de invoering ervan aan de medewerkers bekend gemaakt.

Slotbepaling

Deze regeling wordt elke twee jaar geëvalueerd door Stichting Bravoo en de (G)MR.
De eerstkomende evaluatie vindt plaats gelijktijdig met de evaluatie IBP.