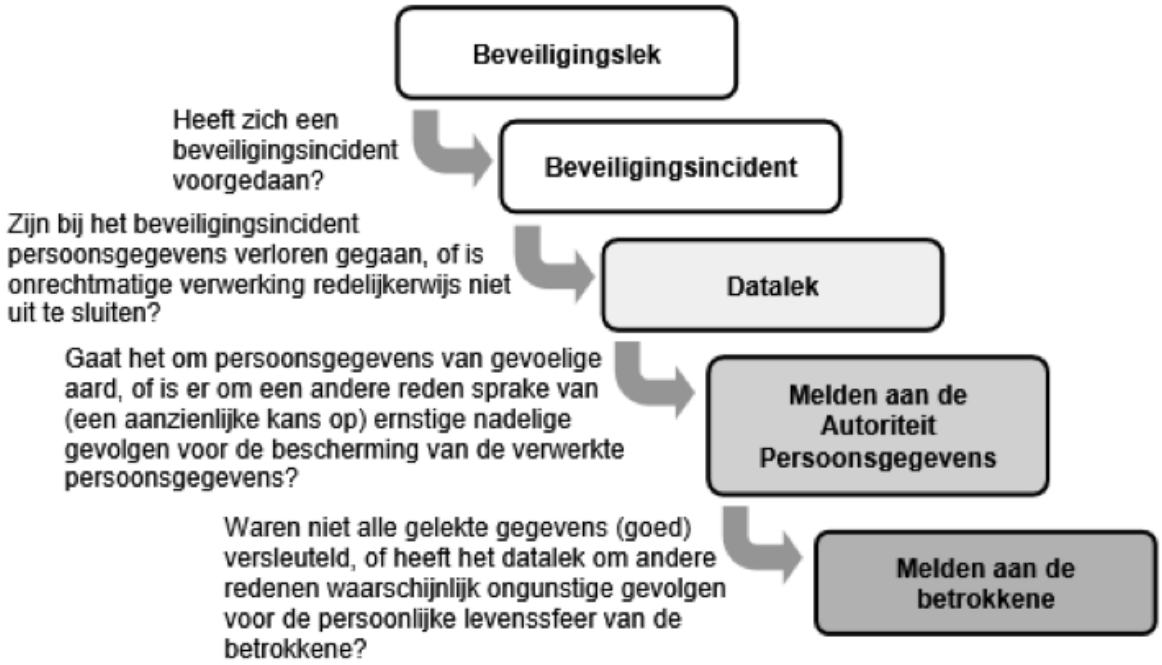
Addendum n.a.v. privacywetgeving

Per 25 mei 2018 wordt de Wet bescherming persoonsgegevens vervangen door de Europese Algemene Verordening Gegevensbescherming (AVG). Deze nieuwe wetgeving stelt hogere en aanvullende eisen aan gegevensverwerking en privacy. Binnen TriVia gelden daarom onderstaande afspraken die uiterlijk 25 mei 2018 geregeld moeten zijn binnen de scholen. Deze eisen worden als addendum toegevoegd aan zowel het EIC-beleid als aan het privacyreglement. Dit i.v.m. de overlap die er bij de verschillende beleidsterreinen is. Op het moment dat de genoemde beleidsstukken aan herziening toe zijn zal het addendum hierin verwerkt worden.

1. Aan alle ouders van nieuwe leerlingen wordt bij de inschrijving van hun kind gevraagd om schriftelijk toestemming te geven voor publicatie van foto's en video's (zie bijlage 1). Ieder jaar, aan het begin van het schooljaar, wordt aan de ouders expliciet gemeld dat zij deze toestemming kunnen wijzigen of intrekken.
2. Aan alle ouders van de huidig leerlingen wordt eenmalig gevraagd om schriftelijk toestemming te geven voor publicatie van foto's en video's (zie bijlage 1). Deze toestemming moet voor 25 mei 2018 verleend zijn. Ieder jaar, aan het begin van het schooljaar, wordt aan de ouders expliciet gemeld dat zij deze toestemming kunnen wijzigen of intrekken.
3. Adresgegevens (bv. klassenlijsten) worden alleen verstrekt wanneer ouders daar toestemming voor hebben gegeven.
4. Papieren dossiers die persoonsgegevens bevatten worden op een afgesloten plaats bewaard.
5. In alle schoolgidsen en op de websites van de scholen wordt de tekst uit bijlage 2 opgenomen. Hierin wordt o.a. verwezen naar het privacyreglement van TriVia. Dit reglement moet ook via een link op de website bereikbaar zijn.
6. Op iedere website wordt het privacy statement geplaatst. We maken hierbij gebruik van de tekst uit bijlage 3.
7. Bij TriVia wordt per 1-1-2018 een functionaris voor de gegevensbescherming (FG) aangesteld. De FG heeft jaarlijks met de directeuren van de scholen contact om te inventariseren of er voldaan wordt aan de eisen die gelden voor gegevensbescherming. Indien hier afwijkingen geconstateerd worden, leidt dit tot het opstellen van een verbeterplan. Bij twijfel kan de FG een steekproef afnemen.
   Deze functionaris moet aan de volgende eisen voldoen:
   - De FG moet goed bereikbaar zijn.
   - De FG moet kennis hebben van de privacywetgeving en van de praktijk van gegevensbescherming.
   - De FG moet voldoende middelen hebben om zijn/haar taak uit te voeren.
   - De FG moet onafhankelijk kunnen werken en mag daarom geen functie hebben waarin hij/zij het doel van een gegevensbewerking bepaalt.

   De FG maakt twee keer per jaar een analyse van de meldingen van beveiligingsincidenten en datalekken.
   De FG rapporteert aan het College van Bestuur.
8. Datalekken die kunnen leiden tot ernstige nadelige gevolgen voor de bescherming van persoonsgegevens worden direct gemeld bij de directeur van de school en binnen 48 uur door de directeur gemeld via het meldloket datalekken.
   https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0.
   De melder vult het formulier van uit bijlage 4 in. Van deze meldingen wordt een registratie bijgehouden (bijlage 5). Indien noodzakelijk worden datalekken ook gemeld aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). Indien datalekken plaatsvinden op bovenschools niveau wordt de melding door het CvB gedaan.
   Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

Onderstaand schema wordt gehanteerd bij het vermoeden van een datalek



Hierbij is het van belang om onderscheid te maken tussen een beveiligingsincident en een datalek.
Een beveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatie verwerkende systemen in gevaar is of kan komen.
Een datalek is een beveiligingsincident, waarbij persoonsgegevens verloren raken of onrechtmatig worden verwerkt (opgeslagen, aangepast, verzonden enz.).
Alle datalekken zijn dus beveiligingsincidenten, maar niet alle beveiligingsincidenten zijn datalekken!

9. Medewerkers van TriVia gaan zorgvuldig om met toegangscodes en wachtwoorden. Hiervoor gelden in ieder geval de volgende afspraken:
   - Een wachtwoord is persoonlijk en mag dus niet aan iemand anders bekend gemaakt worden.
   - Toegangscodes en wachtwoorden mogen alleen bewaard worden op een plaats die alleen toegankelijk is voor de medewerker (dus niet op een papiertje achter in de agenda). Hiervoor kan bv. een app gebruikt worden of een beveiligd bestand.
   - Toegangscodes en wachtwoorden worden niet automatisch opgeslagen op de computer. Een uitzondering hierop geldt wanneer er gewerkt wordt met een eigen account dat alleen via een eigen inlogcode en wachtwoord te bereiken is. De gegevens van dit account worden dan natuurlijk niet automatisch opgeslagen.
   - Bij het verlaten van de werkplek wordt de computer altijd vergrendeld achtergelaten.
   - Van medewerkers van TriVia wordt verwacht dat zij, wanneer zij thuis werken, ervoor zorgen dat de persoonsgegevens op een veilige manier afgeschermd zijn.
   - De directeur bespreekt ieder jaar met de leerkrachten of er nog steeds volgens deze regels gewerkt wordt.
10. Prints waarop persoonsgegevens of andere privacy gevoelige informatie staat worden alleen afgedrukt wanneer de medewerker bij de printer aanwezig is. Hiervoor kan gebruik gemaakt worden van een extra toegangscode op de printer.
11. TriVia maakt voor het beheer van ICT gebruik van de diensten van een bedrijf dat in ieder geval op het gebied van de verwerking van persoonsgegevens ISO gecertificeerd is.

12. Bij het gebruik van digitale leermiddelen, administratiesystemen, etc. wordt altijd een bewerkersovereenkomst gesloten met de leverancier. De directeur van de school is hier verantwoordelijk voor.
13. De directeur van de school zorgt ervoor dat medewerkers, ouders en leerlingen actief geïnformeerd worden over de privacy wetgeving en de maatregelen die de school in dat kader heeft getroffen en gewezen op hun rechten.
14. Door TriVia wordt uiterlijk 1-1-2018 een risico-analyse opgesteld.

Concept vastgesteld in het BDO	07-12-2017
Instemming PGMR	11-01-2018
Ter informatie aan de RvT	20-03-2018
Vastgesteld door het CvB	12-01-2018
Te herzien op	Januari 2022

Bijlage 1: Toestemming publicatie foto's en video's

[Plaats], [maand] [jaar]

Beste ouder/verzorger,

Op onze school laten wij u met foto's en video's zien waar we mee bezig zijn. Opnames worden gemaakt tijdens verschillende gelegenheden. Bijvoorbeeld tijdens activiteiten, schoolreisjes en lessen. Ook uw zoon/dochter kan op deze foto's (en soms in video's) te zien zijn.

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

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

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

Als we foto's en video's willen laten maken voor onderzoeksdoeleinden, bijvoorbeeld om een les van de stagiair op te nemen, zullen we u daar apart over informeren en zo nodig om toestemming vragen. Ook als we beeldmateriaal voor een ander doel willen gebruiken, nemen we contact met u op.

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

Alvast bedankt voor uw medewerking!

Met vriendelijke groet,

[naam ondertekenaar]

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

dat foto's en video's door [SCHOOL] gebruikt mogen worden*:

☐ in de schoolgids, schoolbrochure en/of schoolkalender
☐ op de website van de school
☐ in de (digitale) nieuwsbrief
☐ op sociale-media accounts van de school (Twitter, Facebook)
☐ op ouderportaal
☐ in de door de school aangeleverde persberichten

* aankruisen waarvoor u toestemming geeft

Datum: .....

Naam ouder/verzorger: .....

Handtekening ouder/verzorger: .....

Bijlage 2: Tekst schoolgids en website

Op [naam school] wordt zorgvuldig omgegaan met de privacy van de leerlingen. De school heeft leerlinggegevens nodig om leerlingen goed onderwijs te kunnen geven en te begeleiden. Ook worden de gegevens opgeslagen voor de goede administratieve organisatie van de school. De meeste leerlinggegevens komen van ouders (zoals bij de inschrijving op school), maar ook leraren en ondersteunend personeel leggen gegevens vast over de leerlingen (bijvoorbeeld cijfers en vorderingen). Soms worden er bijzondere persoonsgegevens, zoals medische informatie (dyslexie of ADHD), geregistreerd als dat nodig voor de juiste begeleiding van een leerling.

Tijdens de lessen wordt gebruik gemaakt van een aantal digitale leermaterialen. Hiervoor is een beperkte set met persoonsgegevens nodig om bijvoorbeeld een leerling te identificeren. Met de leveranciers van deze leermiddelen zijn duidelijke afspraken gemaakt over het gebruik van de gegevens die ze van de school krijgen. Een leverancier mag de leerlinggegevens alleen gebruiken als de school daar toestemming voor geeft.

De leerlinggegevens worden op school opgeslagen in het digitale administratiesysteem [naam pakket] en leerlingvolgsysteem [naam pakket]. Het programma is beveiligd en de toegang tot de persoonsgegevens is beperkt tot medewerkers van onze school. [Omdat [naam school] onderdeel uit maakt van [schoolbestuur/bevoegd gezag], worden daar ook (een beperkt aantal) persoonsgegevens mee gedeeld in het kader van de gemeenschappelijke administratie en het plaatsingsbeleid.]

Ouders hebben het recht om de gegevens van en over hun kind(eren) in te zien, te laten corrigeren of te verwijderen (als die gegevens niet langer nodig zijn). Voor vragen of het uitoefenen van deze rechten, kan contact worden opgenomen met de leraar/lerares van de leerling, of met de schooldirecteur.

Op deze school is een privacyreglement van toepassing dat hier te vinden is: [link]. Hierin is beschreven hoe op school wordt omgegaan met leerlinggegevens, en wat de rechten zijn van ouders en leerlingen.

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

Als u wilt weten hoe de digitale leermiddelen omgaan met leerlinggegevens, dan kunt u dat nalezen in de privacybijsluiters die horen bij de leermiddelen die de school gebruikt. U kunt daarvoor terecht bij: [link]*

Bijlage 3: Privacy statement

Wij zijn er van bewust dat u vertrouwen stelt in ons. Wij zien het dan ook als onze verantwoordelijkheid om uw privacy te beschermen. Op deze pagina laten we u weten welke gegevens we verzamelen als u onze website gebruikt, waarom we deze gegevens verzamelen en hoe we hiermee uw gebruikservaring verbeteren. Zo snapt u precies hoe wij werken.

Dit privacy statement is van toepassing op de diensten van PCPO TriVia. U dient zich ervan bewust te zijn dat PCPO TriVia niet verantwoordelijk is voor het privacy beleid van andere sites en bronnen. Door gebruik te maken van deze website geeft u aan het privacy beleid te accepteren.

PCPO TriVia respecteert de privacy van alle gebruikers van haar site en draagt er zorg voor dat de persoonlijke informatie die u ons verschaft vertrouwelijk wordt behandeld.

Ons gebruik van verzamelde gegevens

Gebruik van onze diensten
Wanneer u via onze website middels een online formulier reageert, vragen we u om persoonsgegevens te verstrekken. Deze gegevens worden gebruikt om de gevraagde actie uit te kunnen voeren. De gegevens worden opgeslagen op de beveiligde servers van BasisOnline. Wij zullen deze gegevens niet combineren met andere persoonlijke gegevens waarover wij beschikken.

Communicatie
Wanneer u e-mail of andere berichten naar ons verzendt, is het mogelijk dat we die berichten bewaren. Soms vragen wij u naar uw persoonlijke gegevens die voor de desbetreffende situatie relevant zijn. Dit maakt het mogelijk uw vragen te verwerken en uw verzoeken te beantwoorden. De gegevens worden opgeslagen op de beveiligde servers van onze e-mail provider. Wij zullen deze gegevens niet combineren met andere persoonlijke gegevens waarover wij beschikken.

Cookies
Voor een correcte werking maakt deze website gebruik van “functionele cookies” (tekstbestandjes die op uw computer worden geplaatst door uw internet browser). Deze cookies zijn geheel veilig, bevatten alleen niet-persoonlijke informatie en beïnvloeden de bezoeken aan de website niet.

Eventueel op deze website ingesloten functionaliteiten van externe aanbieders, zoals bijvoorbeeld Youtube video’s, Google Analytics, Google Agenda, Google Maps kaartje, Facebook tijdlijn of een Twitter blok plaatsen daarnaast hun eigen cookies voor de correctie werking van hun diensten.

Cookies uitzetten
De meeste browsers zijn standaard ingesteld om cookies te accepteren, maar u kunt uw browser opnieuw instellen om alle cookies te weigeren of om aan te geven wanneer een cookie wordt verzonden. Het is echter mogelijk dat sommige functies en services, op onze en andere websites, niet correct functioneren als cookies zijn uitgeschakeld in uw browser. U kunt deze cookies verwijderen dan wel uitzetten via uw browser, zie voor uitleg de uitgebreide handleiding door BasisOnline.

Doeleinden
We verzamelen of gebruiken geen informatie voor andere doeleinden dan de doeleinden die worden beschreven in dit privacy statement tenzij we van tevoren uw toestemming hiervoor hebben verkregen.

Derden
De informatie wordt niet met derden gedeeld. In enkele gevallen kan de informatie intern gedeeld worden. Onze werknemers zijn verplicht om de vertrouwelijkheid van uw gegevens te respecteren.

Veranderingen
Deze privacyverklaring is afgestemd op het gebruik van en de mogelijkheden op deze site. Eventuele aanpassingen en/of veranderingen van deze site, kunnen leiden tot wijzigingen in deze privacyverklaring. Het is daarom raadzaam om regelmatig deze privacyverklaring te raadplegen.

Keuzes voor persoonsgegevens
Wij bieden alle bezoekers de mogelijkheid tot het inzien, veranderen, of verwijderen van alle persoonlijke informatie die op enig moment aan ons is verstrekt.

Aanpassen/uitschrijven communicatie
Als u uw gegevens aan wilt passen of uzelf uit onze bestanden wilt laten halen, kunt u contact met ons op nemen. Zie onderstaande contactgegevens.

Vragen en feedback
We controleren regelmatig of we aan dit privacy statement voldoen. Als u vragen heeft over dit privacy statement, kunt u contact met ons opnemen.

Bijlage 4: Meldingsformulier beveiligingsincident en/of datalek

Datum/periode van het beveiligingsincident / datalek
Gegevens van de melder (naam, functie, hoe te bereiken)
Heeft het incident binnen de school plaatsgevonden, zo niet waar dan wel
Toedracht van het incident
Korte beschrijving van het incident (verlies, diefstal)
Wat voor soort gegevens zijn er bij het incident betrokken (wel of geen persoonsgegevens)
Wie is er verantwoordelijk voor het datalek (welke persoon of organisatie)
Welke actie is al ondernomen.

Bijlage 5: Incident registratie

Datum	
Melder/ontdekker	
Plaats incident	
Toedracht	
Gevolg/schade	
Gevolgen voor privacy	
Datalek	Ja/nee (indien ja, vul dan ook onderstaande gegevens in)
Datum melden bij Autoriteit persoonsgegevens	
Nummer incident rapport	
Wie zijn de betrokkenen?	
Zijn betrokkenen geïnformeerd?	
Type persoonsgegevens	
Aanvullende opmerkingen	