TrEf onderwijs
Leonard Springerlaan 39,
7941 GX Meppel

Tel.: 0521-342086
hbremer@TrEfonderwijs.nl
www.TrEfonderwijs.nl

Schoolprotocol: informatiebeveiliging en privacy

Datum vastgesteld	**DB 16 16 april 2019**
Instemming	**GMR 16 april 2019 (oudergeleding)**
Periode	**2019-2023**
Proceseigenaar	**Stafmedewerker TrEf: Riëtte Smit**
Evaluatiemoment	**Jaarlijks**

Voorwoord

In 2019 is het ‘schoolprotocol informatiebeveiliging en privacy’ van TrEf onderwijs herschreven conform de wet Algemene Verordening Gegevensbescherming (AVG). Het is een aanvulling op het ‘beleidsplan informatiebeveiliging en privacy’.

De belangrijkste onderwerpen voor de dagelijkse praktijk zijn in dit protocol uitgewerkt. Daarin zijn ook het wachtwoordenbeleid, het protocol datalek, een autorisatiemix en de gedragscode ICT en internetgebruik verwerkt.

Daarnaast is er bij Tref (digitaal) aanwezig:

- Dataregister leerlingen
- Dataregister medewerkers
- Bewerkersovereenkomsten
- Overzicht bewerkersovereenkomsten
- Registratieformulier beveiligingsincidenten en datalekken
- Overzicht registraties
- Privacyverklaring

Het schoolprotocol informatiebeveiliging en privacy is zodanig opgesteld dat het van toepassing is voor alle scholen van TrEf onderwijs. Elke school neemt in zijn schoolgids en/of website een tekst op over het IBP beleid. In die tekst wordt verwezen naar het beleidsplan op de website van TrEf. Zie bijlage 1 Voorbeeldtekst schoolgids/website.

Het beleidsplan informatiebeveiliging en privacy is vastgesteld voor een periode van vier jaar. Jaarlijks wordt het beleidsplan geëvalueerd.

Henk Bremer

College van Bestuur TrEf onderwijs

Inhoudsopgave

1. Inleiding

1.1 Algemeen

Uitgangspunt is ‘dataminimalisatie’: je mag niet meer gegevens vragen dan strikt noodzakelijk. Dit is ook het uitgangspunt wat betreft de inschrijfformulieren die op schoolniveau worden gemaakt. De inschrijfformulieren worden op schoolniveau gemaakt. Er wordt kritisch gekeken welke gegevens daadwerkelijk nodig zijn, zoals bijvoorbeeld geloofsovertuiging of kerkelijke gezindte. Als deze gegevens niet direct een doel hebben, mag het niet worden gevraagd.

1.2 Informatieplicht

Ouders hebben rechten als het gaat om privacy van hun kind. Denk aan recht op inzage, correctie of verwijdering van de persoonsgegevens. Ouders moeten helder geïnformeerd worden over het doel van de gegevensverwerking.

Volgens de Algemene Verordening Gegevensbescherming (AVG) moet de school (schooldirecteur, bestuur en/of bevoegd gezag) degene over wie de persoonsgegevens gaan (de betrokkene) op de hoogte stellen voor welk doel(en) de persoonsgegevens worden verzameld. Als de betrokkene jonger dan 16 jaar is, dan mogen volgens de AVG alleen de wettelijke vertegenwoordigers (ouders) beslissen over de privacy van de betrokkene. Gemakshalve gebruiken we hierna ‘ouders’.

De AVG eist dat de stichting en haar scholen de ouders extra informeert als:

- de verwachting van de ouders anders is: als de school persoonsgegevens gebruikt op een manier die ouders redelijkerwijs niet verwachten, is dit een reden om ouders extra informatie te geven;
- de omstandigheden waaronder de school persoonsgegevens krijgt: ouders zijn er niet altijd van op de hoogte dat de school via een andere organisatie nieuwe persoonsgegevens heeft gekregen, het is dan noodzakelijk ouders daarvan (en indien mogelijk: persoonlijk) op de hoogte te stellen;
- het gebruik dat gemaakt wordt van de gegevens: als de gevolgen van het gebruik van de persoonsgegevens voor de leerling (of diens ouders) groter zijn dan anders, is extra informatieverstrekking noodzakelijk;
- de aard van de gegevens: hoe gevoeliger de aard van de gegevens is die van de leerling gebruikt gaat worden, hoe meer reden er is om de ouders hierover gedetailleerd te informeren, denk hierbij aan het gebruik van medische gegevens.

De informatie wordt vooraf aan ouders bekend gemaakt. Dat hoeft niet persoonlijk en kan dus via de website, nieuwsbrief of schoolgids. Ouders dienen te zijn geïnformeerd op het moment dat de school de gegevens gaat gebruiken.

De informatieplicht geldt niet als:

- de school weet dat alle ouders volledig zijn geïnformeerd (vermoeden is niet genoeg);
- het onevenredig veel inspanning kost om iedereen (persoonlijk) te informeren, is een alternatief voldoende (dus geen persoonlijke brief of gesprek maar bijvoorbeeld via de nieuwsbrief of website).

Het is belangrijk om ouders actief te informeren over de privacy op school.

1.3 Toestemming

Voor het gebruik van leerlinggegevens heb je soms toestemming nodig van leerlingen en ouders; bijvoorbeeld bij het gebruik van foto’s. Je mag niet meer uitgaan van die toestemming. Er moet jaarlijks actief toestemming worden gevraagd. Tot 16 jaar moeten ouders toestemming geven. Toestemming van één ouder is voldoende, maar in geval van gescheiden ouders kan het verstandig

zijn om beide ouders te laten tekenen (als beide ouders gezag hebben). Toestemming kan ook weer ingetrokken worden. Als één van de ouders het intrekt, moet dat gedaan worden. Zie bijlage 8.2 voorbeeldbrief. De directeuren maken op school een overzicht waar ouders wel/niet toestemming voor hebben gegeven.

De (G)MR dient door de school betrokken te worden bij alle regelingen voor de verwerking van de persoonsgegevens en het gebruik van leerlingvolgsystemen. De (G)MR heeft hierbij een instemmingsrecht: zonder instemming van de (G)MR kan de regeling of het reglement niet in werking treden. Het IBP beleid is op alle scholen van Tref onderwijs gelijk, waardoor instemming van de GMR voldoende is.

Voor het gebruik van foto's en video-opnames van leerlingen op social media, op websites van de stichting en de scholen of in de nieuwsbrief, wordt jaarlijks aan het begin van het cursusjaar aan ouders vooraf toestemming gevraagd. Ouders mogen altijd besluiten om die toestemming niet te geven, of om eerder gegeven instemming in te trekken. Wanneer ouders toestemming hebben gegeven, wordt er zorgvuldig met de foto's omgegaan en wordt afgewogen of een foto geplaatst kan worden.

2. Leerlingdossier

In het leerlingendossier staan alle persoonlijke gegevens van elke leerling. Allereerst mag informatie worden bijgehouden wanneer de wet dit toelaat. Als er geen wettelijke basis is, mag de school enkel gegevens bijhouden indien ze hiervoor toestemming heeft gekregen. Aangezien de leerling meestal minderjarig is, zal deze toestemming moeten worden gegeven door de ouders. Als de ouders geen toestemming geven, mag die informatie niet worden opgeslagen. Verder moet de informatie ook steeds een doel hebben.

De leerlinggegevens worden opgeslagen in ons (digitale) administratiesysteem Parnassys. De vorderingen van de leerlingen worden vastgelegd in ons leerlingvolgsysteem Parnassys. Deze programma's zijn beveiligd en toegang tot die gegevens is beperkt tot medewerkers van onze scholen. Omdat de scholen onderdeel uitmaken van TrEf onderwijs worden daar ook (een beperkt aantal) persoonsgegevens mee gedeeld.

De controle van de gegevens in het leerlingendossier gebeurt via het zogenoemde 'inzagerecht'. Dit recht wordt uitgeoefend op vraag van de ouder, die de minderjarige leerling vertegenwoordigt. De school hoeft echter niet zomaar het hele dossier (of een kopie ervan) af te geven, ze mag ook gewoon vertellen wat er in staat.

2.1 Digitale leermaterialen

Tijdens de lessen maken wij gebruik van een aantal digitale leermaterialen. Hiervoor is een beperkte set met persoonsgegevens nodig om bijvoorbeeld een leerling te kunnen identificeren als die inlogt. Wij hebben met deze leveranciers duidelijke afspraken gemaakt over de gegevens die ze van ons krijgen. De leverancier mag de leerlinggegevens alleen gebruiken als wij daar toestemming voor geven, zodat misbruik van die informatie door de leverancier wordt voorkomen. Zie hoofdstuk 5 Bewerkersovereenkomsten.

2.2 Doorgeven en publiceren gegevens

Allereerst mag de school het dossier gebruiken om de leerling te ondersteunen. Dit zijn de zogenaamde onderwijs- en opvoedingsopdrachten van de school. In het kader daarvan mag de school het dossier ook doorgeven binnen de school, bijvoorbeeld als een leerling van studierichting verandert. Het doorgeven van gegevens naar een andere school is dan weer minder evident. Sommige administratieve gegevens mogen wel worden doorgegeven, maar dit is niet altijd het volledige leerlingendossier. Zo mogen bepaalde (negatieve) gegevens niet zomaar worden doorgegeven, aangezien een leerling anders misschien geen eerlijke kans zal krijgen op de nieuwe school. Zo kan er wel worden vermeld dat er ooit een tuchtmaatregel is genomen, zonder dat dit in

detail wordt toegelicht. Als de school meer wil doorgeven dan hetgeen wettelijk is bepaald, dan zal de leerling (of zijn ouders) toestemming moeten geven. In de praktijk blijkt dat alle voortgezet onderwijs scholen middels het inschrijfformulier de ouders vragen toestemming te geven voor het overdragen van de gegevens van een leerling van de basisschool naar de voortgezet onderwijsschool. Daarmee is het ingedekt voor alle gegevens.

In geval van uitwisseling van leerlinggegevens met andere organisaties, wordt daar vooraf toestemming gevraagd aan de ouders, tenzij die uitwisseling verplicht is op grond van de wet.

Het publiceren van gegevens (bv. het uithangen van resultaten in de school) is niet toegelaten zonder toestemming.

2.3 Bewaartermijn

Voor veel documenten is het wettelijk bepaald hoe lang deze mogen worden bijgehouden. Voor alle andere documenten vallen we terug op de privacywet, die stelt dat de info “niet langer dan noodzakelijk” mag worden bewaard. Dit betekent dat de gegevens dus beter worden verwijderd zodra hun doel is bereikt. Dit wil uiteraard niet zeggen dat gegevens moeten worden verwijderd zodra de leerling de school verlaat. Vaak is het nuttig om in een bufferperiode te voorzien.

3. Wachtwoordenbeleid

Wachtwoorden vormen een belangrijk aspect van de informatiebeveiliging. Wachtwoorden en wachtwoordzinnen helpen te voorkomen dat onbevoegde personen toegang krijgen tot bestanden, programma's en andere bronnen. Een wachtwoord behoort altijd te zijn toegewezen aan een gebruikersnaam, die een fysieke gebruiker uniek identificeert. Alle handelingen van een gebruiker moeten uniek kunnen worden toegewezen aan die gebruiker.

3.1 Gedragsregels wachtwoorden

- Gebruik verschillende wachtwoorden voor verschillende systemen/doelen, gebruik geen privéwachtwoorden op het werk.
- Gebruik verschillende wachtwoorden voor verschillende applicaties op het werk, minimaal voor de essentiële systemen die meer gevoelige informatie bevatten.
- Gebruik voor essentiële systemen een sterk wachtwoord en wissel dit regelmatig.
- Geef wachtwoorden aan niemand.
- Wachtwoorden mogen niet worden opgeschreven.
- Geef geen wachtwoorden door via e-mail, chat of andere elektronische communicatie en als dat toch moet, dan gescheiden (via een andere weg) van de gebruikersnaam.
- Geef geen al te gemakkelijke hints of controlevraag over het wachtwoord, bijvoorbeeld je naam of de meisjesnaam van je moeder.
- Geef nooit een wachtwoord op voor onderzoeken, vragen van anderen of om iemand te helpen, het vragen om een wachtwoord moet worden aangemerkt als een veiligheidsincident.
- Maak geen gebruik van de ‘wachtwoord onthoud’ functie van sommige webbrowsers.
- Maak geen gebruik van de functie om ingelogd te blijven.
- Maak altijd gebruik van sterke wachtwoorden.
- Wijzig een wachtwoord direct bij vermoeden van misbruik.

- Wachtwoorden moeten niet worden gebruikt in automatische inlogprocedures (bijvoorbeeld opgeslagen onder een functietoets of in een macro).
- Bij een grote hoeveelheid logins en wachtwoorden is het aan te bevelen om deze op te slaan in een daarvoor bedoelde veilige applicatie of app (wachtwoordmanager).

3.2 Twee-factorauthenticatie

Bij applicaties die veel gevoelige informatie bevatten, wordt er gebruikt gemaakt van een twee-factorauthenticatie (indien technisch mogelijk). Alle medewerkers zijn verplicht dit in te stellen voor het programma Parnassys. Ook het Cito portal maakt gebruikt van een twee-factorauthenticatie.

3.3 Autorisatiematrix

Ieder jaar wordt gecontroleerd of gebruikers nog toegang moeten hebben tot bepaalde informatie. Er wordt kritisch gekeken wat iedere medewerker wel (en juist niet) nodig heeft. Zie bijlage 3 voor een dataclassificatie en de autorisatiematrixen van de belangrijkste programma's die we gebruiken.

4. Gedragscode ICT en gebruik leerlinggegevens

Een leerkracht komt elke dag in aanraking met persoonsgegevens. Het is belangrijk om binnen de school te communiceren over IBP, zodat er veilig en verantwoord mee wordt omgegaan.

- Sluit je computer aan het eind van de dag af. Sluit programma's niet alleen af, maar log ook uit. Verlaat je het lokaal, gebruik dan de Windows toets + de letter L. Je computer sluit dan niet af, maar het scherm wordt zwart. Meld je daarna weer aan met Control+Alt+Delete.
- Klik niet klakkeloos iets aan: zorg dat je bewust 'klikt' op het netwerk van de school, voor je het weet haal je allerlei virussen en malware binnen. Malware is een verzamelnaam voor schadelijke en ongewenste software.
- Hang geen gegevens van kinderen op in de klas. Denk aan inlogcodes van computerprogramma's, klassenlijsten bij ontruimingsplan etc.
- Ga zorgvuldig om met de mail:
    - Niet mailen maar delen: verstuur niet alle dossiers per mail, maar deel bestanden met elkaar via office 365. En als je toch moet mailen, zorg dan in ieder geval dat het bestand beveiligd is.
    - Mailen naar meerdere personen: gebruik daarvoor de BCC (Blank Carbon Copy). Hiermee voorkom je dat andere personen alle mailadressen zien.
    - Mail via de beveiligde omgeving van Parnassys of via schoolmail. Geen mail van/naar het huisadres.
    - Verstuur mail van de klassenouder via Parnassys en niet via privéadres van de klassenouder. Individuele reacties kunnen rechtstreeks naar de klassenouder worden gestuurd. Optie: Vraag toestemming voor het delen van de mailadressen aan de klassenouder. Dit is opgenomen in voorbeeldbrief in bijlage 2. Meld aan het begin van het jaar bij de klassenouder dat er voorzichtig moet worden omgegaan met de mailadressen van de andere ouders.
- Surf veilig: zorg dat je weet dat je op een betrouwbaar netwerk zit. Controleer of de website die je bezoekt een groen slotje heeft.
- Sla veilig op: gebruik geen usb-sticks voor vertrouwelijke gegevens.
- De klassenmap en agenda's met gegevens van leerlingen niet open op de tafel laten liggen en opruimen als de leerkracht niet in het lokaal is. Altijd in een afgesloten kast

of lade bewaren evenals verslagen van oudergesprekken. Externe medewerkers mogen op geen enkele wijze zicht hebben of krijgen op gegevens van leerlingen, ouders en personeel.

- Gebruik nooit je privé-telefoon voor het opslaan en/of verzenden van schoolgegevens in de breedste zin van het woord.

- Gebruik geen usb-stick van leerlingen. Laat leerlingen documenten via of in de cloud aanleveren, zoals spreekbeurten en werkstukken.

- Wat betreft het gebruik van office 365 hebben we het volgende afgesproken:
  - alle scholen stappen in 2019 over op office 365;
  - documenten die meerdere personen nodig hebben worden opgeslagen in sharepoint;
  - persoonlijke documenten kunnen opgeslagen worden in onedrive;
  - documenten vanuit sharepoint worden gedeeld en zo min mogelijk gedownload en als bijlage verzonden;
  - bij het delen van documenten (met name met personen buiten TrEf onderwijs) wordt ingesteld of het document wel/niet gedownload mag worden en of het wel/niet bewerkt mag worden.

4.1 Aanvulling schoolleiding/zorgcoördinator

- Vraag jaarlijks actief toestemming aan ouders voor gebruik foto's en andere gegevens.
  - Plaats geen foto's/video's van kinderen waarvan ouders geen toestemming hebben gegeven.
  - Houd bij het plaatsen van foto's/video's rekenen met 'toeschouwers', zodat andere mensen niet zichtbaar in beeld zijn.
  - Plaats geen close-up foto's van kinderen.
  - Vermeld geen namen bij foto's.

- Vermeld geen namen van kinderen op de website of in andere externe nieuwsberichten zonder toestemming van ouders. Bijvoorbeeld: Nieuwe leerlingen verwelkomen in nieuwsbrief mag, maar de namen moeten weggehaald worden als de nieuwsbrief wordt opgeslagen op de website.

- Vraag niet meer gegevens dan noodzakelijk. Kritisch kijken naar bestaande lijsten.

- Ga zorgvuldig om met leerlingdossiers en verzend het niet zonder toestemming van ouders.

  - Voor de uitwisseling van gegevens tussen de basisschool en de nieuwe school is geen toestemming van ouders nodig. Ze kunnen dus ook geen bezwaar maken tegen de uitwisseling van die informatie: de school moet de informatie hoe dan ook uitwisselen. Wel moeten de ouders inzage krijgen in het overstapdossier, voordat deze wordt uitgewisseld.

- Bewaar gegevens niet langer dan noodzakelijk. Een standaard bewaartermijn is twee jaar. Een overstapdossier van een leerling die is doorverwezen naar een school voor speciaal onderwijs mag drie jaar bewaard blijven. In de Archiefwet zijn meer uitzonderingen opgenomen, zoals het verplicht bewaren van diploma's.

- Maak een schoolveiligheidsplan met een pestprotocol, aangevuld met een media- of

gedragscode, waarin aandacht is voor ‘sociale veiligheid op internet’ en ‘mediawijsheid’.

In bijlage 4 is een checklist privacy opgenomen.

5. Melding datalekken

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

5.1 Meldplicht

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

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

De meldplicht geldt voor de verantwoordelijke voor de persoonsgegevens, dat is dus het College van Bestuur. Een leverancier is een bewerker voor de school. Er kan worden afgesproken dat een bewerker namens de verantwoordelijke de melding doet, maar dat gebeurt dan na overleg met het College van Bestuur.

Als er een datalek is, moet daar binnen 72 uur na ontdekking van het lek melding van worden gedaan bij de Autoriteit Persoonsgegevens. Uit de praktijk blijkt dat er vaak wel datalekken zijn, maar dat hier (te) lichtvoetig mee omgegaan wordt. Denk er aan: een niet gemeld datalek is doorgaans ernstiger dan een gemeld datalek.

5.2 Procedure

1. **Ontdekken**
   De Ontdekker merkt een beveiligingsincident op. Via eigen waarneming of via waarneming van een derde. De Ontdekker verzamelt zoveel mogelijk informatie over het beveiligingsincident en meldt het bij de manager IBP, Riëtte Smit of bij afwezigheid bij het College van Bestuur, Henk Bremer.

2. **Inventariseren**
   Het Meldpunt bepaalt dan 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 daarna vastgelegd:
   - Samenvatting van het beveiligingsincident, wat is er met de gegevens gebeurd, wat voor gegevens zijn het (bijzondere gegevens of van gevoelige aard)
   - Datum/periode van het beveiligingsincident
   - Aard van het beveiligingsincident
   - Wanneer van toepassing (bij een datalek):
     - Omschrijving van de groep betrokkenen
     - Aantal betrokkenen

- Type persoonsgegevens in kwestie
- Worden de gegevens binnen een keten gedeeld

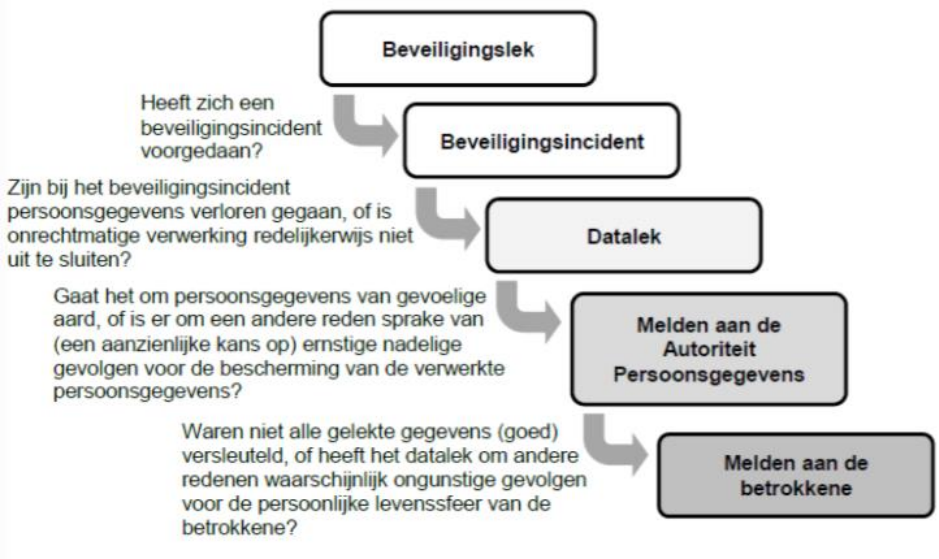
3. Beoordelen

Het Meldpunt meldt het incident bij de Functionaris voor Gegevensbescherming, Agnes Bennen van Akorda onderwijsdienstverlening. De FG bepaalt of het incident gemeld moet worden bij de Autoriteit persoonsgegevens.

Bij de beoordeling of er sprake is van een 'meldingsplichtig datalek', wordt er rekening gehouden met het type gegevens en met 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 (denk aan het lekken van een leerling die vaak kinderen pest en daarmee gezien kan worden als notoire pester).

De onderstaande beslisboom kan gebruikt worden:



4. Repareren

De Technicus (intern of extern) wordt gevraagd te achterhalen wat de oorzaak van het beveiligingsincident is en moet de oorzaak (laten) verhelpen. De technicus van de school of de vereniging 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)?

5. **Melden**
   Indien de conclusie bij stap 3 is dat er melding gedaan moet worden bij de Autoriteit Persoonsgegevens (en eventueel betrokkenen), dan zal de Melder dit binnen twee werkdagen 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.

   De FG bepaalt of het datalek daadwerkelijk wordt gemeld.

6. **Vastleggen**
   Alle informatie, die in de voorafgaande stappen is ingewonnen of ontstaan, wordt gearchiveerd door de manager IBP, Riëtte Smit (meldpunt). Het Meldpunt verstuurt een samenvatting van de genomen maatregelen aan de Ontdekker.

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

6. Bewerkersovereenkomst

De stichting moet als verantwoordelijke voor de persoonsgegevens afspraken maken met leveranciers als die persoonsgegevens ontvangen. Afspraken over datalekken vallen daar ook onder. Er worden schriftelijke afspraken met alle bewerkers gemaakt. Hiervoor wordt gebruik gemaakt van het model bewerkersovereenkomst die hoort bij het convenant ‘Digitale onderwijsmiddelen en privacy 2.0’ (www.privacyconvenant.nl). Dit wordt centraal geregeld door de manager IBP Riëtte Smit. Zodra er op schoolniveau een nieuwe leverancier bijkomt, moet dit worden doorgegeven aan Riëtte Smit, zodat de bewerkersovereenkomst in orde kan worden gemaakt.

7. Evaluaties

	Datum	Medewerker	Evaluatie
Tussenevaluatie 2020			
Tussenevaluatie 2021			
Tussenevaluatie 2022			
Eindevaluatie 2023			

8. Bijlagen

8.1 Voorbeeldtekst schoolgids/website

Wij gaan zorgvuldig om met de privacy van onze leerlingen. Dit is vastgelegd in het beleidsplan informatiebeveiliging en privacy (IBP) van onze school. De gegevens die over leerlingen gaan, noemen we persoonsgegevens. Wij maken alleen gebruik van persoonsgegevens als dat nodig is voor het leren en begeleiden van onze leerlingen, en voor de organisatie die daarvoor nodig is. In het privacyreglement kunt u precies lezen wat voor onze school de doelen zijn voor de registratie van persoonsgegevens. De meeste gegevens ontvangen wij van ouders (zoals bij de inschrijving op onze school). Daarnaast registreren leraren en ondersteunend personeel van onze school gegevens over onze leerlingen, bijvoorbeeld cijfers en vorderingen. Soms worden er bijzondere persoonsgegevens geregistreerd als dat nodig voor de juiste begeleiding van een leerling, zoals medische gegevens (denk aan dyslexie of ADHD).

De leerlinggegevens worden opgeslagen in ons (digitale) administratiesysteem Parnassys. De vorderingen van de leerlingen worden vastgelegd in ons leerlingvolgsysteem Parnassys. Deze programma's zijn beveiligd en toegang tot die gegevens is beperkt tot medewerkers van onze school. Omdat onze school onderdeel uitmaakt de stichting TrEf onderwijs worden daar ook (een beperkt aantal) persoonsgegevens mee gedeeld.

Tijdens de lessen maken wij gebruik van een aantal digitale leermaterialen. Hiervoor is een beperkte set met persoonsgegevens nodig om bijvoorbeeld een leerling te kunnen identificeren als die inlogt. Wij hebben met deze leveranciers duidelijke afspraken gemaakt over de gegevens die ze van ons krijgen. De leverancier mag de leerlinggegevens alleen gebruiken als wij daar toestemming voor geven, zodat misbruik van die informatie door de leverancier wordt voorkomen.

Ouders hebben het recht om de gegevens van en over hun kind(eren) in te zien. Als de gegevens niet kloppen, moet de informatie gecorrigeerd worden. Als de gegevens die zijn opgeslagen niet meer relevant zijn voor de school, mag u vragen die specifieke gegevens te laten verwijderen. Voor vragen of het uitoefenen van uw rechten, kunt u contact opnemen met de groepsleerkracht van uw kind of met de schooldirecteur.

In geval van uitwisseling van leerlinggegevens met andere organisaties, wordt daar vooraf toestemming gevraagd aan de ouders, tenzij die uitwisseling verplicht is op grond van de wet.

Voor het gebruik van foto's en video-opnames van leerlingen op bijvoorbeeld de website van de school of in de nieuwsbrief, vragen wij altijd vooraf uw toestemming. Ouders mogen altijd besluiten om die toestemming niet te geven, of om eerder gegeven instemming in te trekken. Als u toestemming heeft gegeven, blijven wij natuurlijk zorgvuldig met de foto's omgaan en wegen wij per keer af of het verstandig is een foto te plaatsen. Voor vragen over het gebruik van foto's en video's kunt u terecht bij de leerkracht van uw kind of bij de schooldirecteur.

Voor de privacyverklaring van TrEf en het beleidsplan IBP verwijzen wij naar de website van TrEf onderwijs: www.trefonderwijs.nl – tabblad info/privacy.

8.2 Voorbeeldbrief

Invoegen Logo School + Adres

Beste ouder/verzorger,

De stichting TrEf en haar scholen gaan zorgvuldig om met de privacy van de leerlingen. Dit is vastgelegd in het 'beleidsplan informatiebeveiliging en privacy' en de 'privacyverklaring' van de stichting die u kunt vinden op de website www.trefonderwijs.nl (tabblad info/privacy). In deze documenten staat beschreven hoe we omgaan met gegevens van leerlingen, digitaal leermateriaal en de informatieplicht die we hebben.

Voor het gebruik van foto's en video-opnames van leerlingen op social media, op websites van de stichting en de scholen of in de nieuwsbrief, vragen wij jaarlijks toestemming. U mag altijd besluiten om die toestemming niet te geven, of om eerder gegeven instemming in te trekken. Ook mag u op een later moment alsnog toestemming geven. Wanneer u toestemming hebt gegeven, gaan wij 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.

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 en toestemming vragen aan andere ouders als ze foto's plaatsen waar ook andere kinderen bij op staan.

Als we foto's en video's willen laten maken voor onderzoeksdoeleinden, bijvoorbeeld om een les van de stage-juf 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.

Alvast bedankt voor uw medewerking!

Met vriendelijke groet,

Team **<naam school invoegen>**

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

dat foto's en video's door **<naam school invoegen>** gebruikt mogen worden*:

☐ in de schoolgids en schoolbrochure

☐ in de schoolkalender

☐ op de website van de school

☐ in de (digitale) nieuwsbrief

☐ op sociale-media accounts van de school (Twitter, Facebook, Instagram)

☐ lokale tv, kabelkrant, krant

Voor het verspreiden van een klassenlijst in de groep van mijn kind, met naam/adres/telefoonnummer, geef ik*:

☐ wel toestemming

☐ geen toestemming

Iedere groep heeft een klassenouder die rechtstreeks communiceert met de andere ouders als er vervoer geregeld moet worden voor buitenschoolse activiteiten. Voor het doorgeven van mijn mailadres aan de klassenouder, geef ik*:

☐ wel toestemming

☐ geen toestemming

* aankruisen waarvoor u toestemming geeft

Datum: .....

Naam ouder/verzorger: .....

Handtekening ouder/verzorger: .....

S.o.s. Adres Schooljaar <jaartal invullen>.

Jaarlijks willen we graag controleren of de SOS-adressen nog wel kloppen. Het is meerdere malen gebleken dat het van groot belang is dat wij een SOS-adres achter de hand hebben. Aangezien het SOS-adres nog wel eens verandert, vragen we u dit formulier volledig in te vullen.

Naam kind:_____Groep:_____

s.o.s. – adres 1		s.o.s. – adres 2 (niet verplicht)	
Naam:		Naam:	
Adres:		Adres:	
Telefoon:		Telefoon:	

Emailadres:

Ook emailadressen zijn aan verandering onderhevig. Daarom ook het verzoek om het emailadres meteen door te geven aan school bij verandering. Als uw emailadres het laatste jaar is veranderd, wilt u dan hier uw emailadres invullen?

Emailadres:_____

8.3 Autorisatiematrix

Dataclassificatie:

Gevoelige informatie	**Standaard informatie**
Parnassys	Basispoort
Grippa	Oefensoftware methodes
Cito portal	
Kanvas	

Parnassys			Rollen					
			College van Bestuur	Directeuren	Intern begeleider	Leerkracht	Ondersteunend personeel	ICT-ers
Persoonsgegevens van leerlingen	a.	Contactgegevens leerling	V	V	V	V		V
	b.	Voor- en achternaam leerling	V	V	V	V		V
	c.	Nationaliteit en geboorteplaats	V	V	V	V		V
	d.	Contactgegevens ouders		V	V	V		V
	e.	Gezondheid of welzijn		V	V			V
	f.	Godsdienst of levensovertuiging		V	V			V
	g.	Aard en verloop onderwijs en behaalde resultaten		V	V	V		V
	h.	Organisatie onderwijs en verstrekken van leermiddelen		V	V			V
	i.	Berekenen, vastleggen en innen van gelden		V	V			V
	j.	Foto´s en videobeelden van activiteiten						
	k.	Gegevens van docenten en begeleiders		V	V	V		V
	l.	Andere gegevens voor toepassing van wet- en regelgeving						

Aandachtspunten Parnassys:

- Tweefactor authenticatie verplicht instellen.
- Tijdelijk toegang tot bepaalde groep/leerling is mogelijk, hier gebruik van maken in plaats van elkaar wachtwoorden doorgeven.
- Leerkrachten alleen rechten geven voor de eigen groep.

Grippa			Rollen					
			College van Bestuur	Directeuren	Intern begeleider	Leerkracht	Ondersteunend personeel	ICT-ers
Persoonsgegevens van leerlingen	a.	Contactgegevens leerling			V			
	b.	Voor- en achternaam leerling			V			
	c.	Nationaliteit en geboorteplaats			V			
	d.	Contactgegevens ouders			V			
	e.	Gezondheid of welzijn			V			
	f.	Godsdienst of levensovertuiging						
	g.	Aard en verloop onderwijs en behaalde resultaten			V			
	h.	Organisatie onderwijs en verstrekken van leermiddelen			V			
	i.	Berekenen, vastleggen en innen van gelden			V			
	j.	Foto´s en videobeelden van activiteiten						
	k.	Gegevens van docenten en begeleiders			V			
	l.	Andere gegevens voor toepassing van wet- en regelgeving						

Cito portal			Rollen					
			College van Bestuur	Directeuren	Intern begeleider	Leerkracht	Ondersteunend personeel	ICT-ers
Persoonsgegevens van leerlingen	a.	Contactgegevens leerling						
	b.	Voor- en achternaam leerling		V	V			
	c.	Nationaliteit en geboorteplaats						
	d.	Contactgegevens ouders						
	e.	Gezondheid of welzijn						
	f.	Godsdienst of levensovertuiging						
	g.	Aard en verloop onderwijs en behaalde resultaten		V	V			
	h.	Organisatie onderwijs en verstrekken van leermiddelen						
	i.	Berekenen, vastleggen en innen van gelden						
	j.	Foto´s en videobeelden van activiteiten						
	k.	Gegevens van docenten en begeleiders						
	l.	Andere gegevens voor toepassing van wet- en regelgeving						

Kanvas			Rollen					
			College van Bestuur	Directeuren	Intern begeleider	Leerkracht	Ondersteunend personeel	ICT-ers
Persoonsgegevens van leerlingen	a.	Contactgegevens leerling						
	b.	Voor- en achternaam leerling		V	V	V		V
	c.	Nationaliteit en geboorteplaats						
	d.	Contactgegevens ouders						
	e.	Gezondheid of welzijn		V	V	V		V
	f.	Godsdienst of levensovertuiging						
	g.	Aard en verloop onderwijs en behaalde resultaten						
	h.	Organisatie onderwijs en verstrekken van leermiddelen						
	i.	Berekenen, vastleggen en innen van gelden						
	j.	Foto´s en videobeelden van activiteiten						
	k.	Gegevens van docenten en begeleiders						
	l.	Andere gegevens voor toepassing van wet- en regelgeving						

Basispoort en overige oefensoftware lesmethoden			Rollen					
			College van Bestuur	Directeuren	Intern begeleider	Leerkracht	Ondersteunend personeel	ICT-ers
Persoonsgegevens van leerlingen	a.	Contactgegevens leerling		V	V	V	V	V
	b.	Voor- en achternaam leerling		V	V	V	V	V
	c.	Nationaliteit en geboorteplaats						
	d.	Contactgegevens ouders						
	e.	Gezondheid of welzijn						
	f.	Godsdienst of levensovertuiging						
	g.	Aard en verloop onderwijs en behaalde resultaten		V	V	V	V	V
	h.	Organisatie onderwijs en verstrekken van leermiddelen						
	i.	Berekenen, vastleggen en innen van gelden						
	j.	Foto´s en videobeelden van activiteiten						
	k.	Gegevens van docenten en begeleiders						
	l.	Andere gegevens voor toepassing van wet- en regelgeving						

8.4 Checklist privacy

Denk bij het registreren, verzamelen en verwerken van gegevens altijd aan de 5 vuistregels.	
☐	**Doel:** Heb ik vooraf een doel voor de verwerking van persoonsgegevens vastgesteld?
☐	**Doelbinding:** Worden de persoonsgegevens alleen gebruikt voor het doel dat ik vooraf heb vastgesteld.
☐	**Grondslag:** Is er minimaal een wettelijke grondslag voor de verwerking? ☐ Ik heb toestemming van leerling en ouders. ☐ De gegevens zijn nodig voor een uitvoering van een overeenkomst. ☐ Het verwerking van deze gegevens is wettelijk verplicht. ☐ De verwerking van de gegevens is nodig voor het uitvoeren van onze publiekrechtelijke taak. ☐ Er is een rechtvaardigd belang dat ik kan uitleggen aan (de ouders van) de leerlingen.
☐	**Data minimalisatie:** Gebruik ik alleen de gegevens die noodzakelijk zijn om het vastgestelde doel te verwezenlijken en bewaar ik ze niet langer dan noodzakelijk?
☐	**Transparantie:** Heb ik ouders (of de leerlingen) vooraf geïnformeerd over het doel van de gegevensverwerking en heb ik uitgelegd, welke gegevens worden gebruikt en met wie deze worden gedeeld?