Vlaanderen
is onderwijs & vorming

KENNISCENTRUM **DIGISPRONG**

TECHNISCHE HANDLEIDING GOOGLE WORKSPACE FOR EDUCATION

KENNISCENTRUM
DIGISPRONG

Gefinancierd door de Europese Unie
NextGenerationEU

DE VLAAMSE VEERKRACHT

INHOUD

UPDATE MEI 2023

1. COOKIES

Op 12 mei verscheen er bij Surf Sivon in Nederland (1) een update met betrekking het instellen en gebruik van de workspace omgeving van google. Deze updates zijn ook relevant voor de Vlaamse scholen.

1. Het uitlezen van de cookies in de browser door Google
2. De tracking door de cookies zelf door 3e partijen.

Dit is een generiek risico die ook aanwezig is bij andere systemen (anders dan Google).

Google geeft aan dat zij geen personen kunnen identificeren aan de hand van cookies en dat ze dus ook geen inzage kunnen verlenen in persoonlijke data die ze verzamelen. Lees het Google statement hierover. Dit is in strijd met de AVG.

De tracking door derden kan ondervangen worden door het whitelisten van vertrouwde websites en/of het gebruik van een add blocker om in ieder geval tracking cookies te blokkeren.

WELKE URL MOET JE WHITELISTEN?

Als je site A bekijkt en site A bevat content van site B. Dan moet je de URL van site B whitelisten. Voor een aantal scholen blijkt dit goed te werken en is de lijst met sites die moet worden 'gewhitelist' beperkt. Uitgangspunt is natuurlijk dat de cookies van site B te vertrouwen zijn.

Welke applicatie op de whitelist zouden moeten staan is vooral een trial en error proces. Hieronder een voorbeeld:
[*.]smartschool.be
[*.]google.com
[*.]google.be
[*.]klascement.be
[*.]leerid.be
[*.]vlaanderen.be

https://leerling-leerid.vlaanderen.be/p/aanmelden
https://schoolloket-leerid.vlaanderen.be/p/aanmelden
docs.google.com
play.google.com
ops.google.com
[*.]drive.google.com – het gebruiken van bv. video's in de eigen Google Drive in Google Presentation of Classroom.
[*.]googleusercontent.com – bestanden downloaden van Google Drive.
https://accounts.google.com – het doen/hebben van SSO met Google op gelieerde applicaties.

(1) https://sivon.nl/update-google-workspace-for-education/

2. PSEUDONIEM E-MAIL ADRES

Een anoniem adres is niet te herleiden tot een persoon. Een pseudoniem e-mail is wel te herleiden tot een persoon. Anoniem en pseudoniem is in de communicatie door elkaar gebruikt. We hanteren vanaf nu de term pseudoniem. Een pseudoniem is meestal door de eigen organisatie te herleiden tot een persoon, terwijl de 'buitenwereld' niet weet om wie het gaat.

Het advies is om alleen pseudonieme mailadressen te gebruiken voor leerlingen. Voor leraren/docenten is het niet noodzakelijk. Leerlingen zijn zich niet altijd bewust met wie of op welke websites ze hun e-mailadres delen, bij leraren/docenten mag je verwachten dat zij bewuster hun e-mailadres delen. Een email adres komt wordt in veel gevallen gevraagd voor toegang tot een online dienst.

Het gebruik van een pseudoniem is vooral van belang bij jongere leerlingen. Zij overzien minder de gevolgen van het digitale spoor dat ze achterlaten op internet. Het gaat hier dus echt om het email adres 1234@school.be. Bij display name (in Google mail bijvoorbeeld) kan wel de naam opgegeven worden. Het doel is om een e-mail adres niet direct tot de persoon herleidbaar te maken. Bij een datalek op het internet worden in het algemeen minimaal e-mailadressen gelekt en dan betreft leerlingen de grootste groep. Hierbij helpt het pseudonimiseren van e-mailadressen. We noemen dit dataminimalisatie, één van de vuistregels voor privacy.

Dit advies is ook breder toe te passen. Ook bij andere systemen dan Google is het goed dit advies te implementeren: gebruik niet meer gegevens dan nodig is.

Als het e-mailadres van leerlingen gebruikt voor single sign-on en identificatie bij andere systemen is het advies om een migratiepad te hanteren. Voor nieuwe leerlingen wordt dan een pseudoniem gebruikt. Bestaande accounts blijven zoals ze zijn en faseren geleidelijk uit. Huidige accounts omzetten heeft een grote impact, is technisch een complexe activiteit omdat in alle gekoppelde systemen dit op hetzelfde moment moet gebeuren en bij fouten is de kans op een datalek groot. Accounts worden bijvoorbeeld aan de verkeerde mailbox/bestanden gekoppeld of accounts worden onterecht opnieuw aangemaakt waardoor toegang tot de mailbox/bestanden niet meer mogelijk is. De consensus bij de werksessies is dat de risico's van verlies van data en toegang zwaarder wegen als leerlingen niet meer bij hun leermiddelen kunnen komen (of erger nog dat bij het toewijzen van account fouten optreden die tot een datalek leiden). De argumenten om dit migratiepad te volgen, wegen daarmee voldoende zwaar om deze afweging te maken in de lokale DPIA.

3. YOUTUBE

YouTube is een additionele dienst en dus geen onderdeel van de zogenaamde core-services van Workspace. YouTube moet uitstaan bij de additionele services: leerlingen hebben geen toegang tot de YouTube browser.
Additionele Google-diensten vallen niet onder de Google Workspace for education-overeenkomst. Het gebruik ervan levert een hoog risico op voor leerlingen en medewerkers, omdat de school geen controle heeft over persoonsgegevens die Google hierbij verzamelt of gebruikt. Google ziet zichzelf als verwerkingsverantwoordelijke (data controller) en verwerkt data met 33 brede commerciële doelen.

De privacy risico's van YouTube zijn systeem onafhankelijk. Dit speelt dus ook als YouTube gebruikt wordt in een Microsoft omgeving. YouTube wordt ook veel gebruikt in educatieve applicaties. In deze gevallen moet dit in embedded mode zijn met privacy enhanced enabled. YouTube films kunnen gekeken worden in embedded mode. Google heeft bevestigd dat gebruik van de embedded player wel voldoet aan de gemaakte privacy afspraken.

Voor YouTube zijn er 3 user cases te onderscheiden

1. Zelf video materiaal maken en uploaden.
   Ons advies is: doe dat niet in YouTube maar deel video's in drive.
2. Een specifieke YouTube video bekijken
   Plaats deze video in embedded mode (privacy modus aan) in classroom, presentaties of sites.
3. Vrij doorzoekbaar YouTube gebruiken en video's afspelen.

De embedded mode voldoet aan de AVG, maar beperkt de gewenste functionaliteit voor het onderwijs. Een aantal scholen beperkt de privacy impact voor scenario 3 met een of meerdere van de volgende maatregelen:

- Video's zoeken in duckduckgo en in embedded mode afspelen op de duckduckgo website. Om expliciete content in de zoek resultaten te voorkomen gebruik je de safe mode. Je kan safe search met duckduckgo instellen via admin.google.com.
- Een beperkte set leraren toegang geven tot YouTube om video's te beheren. De privacy van deze leraren is dan niet volledig beschermt, maar voorkomt dat iedereen video's upload. Deze groep leraren krijgt dan uitleg over de privacy-risico's. De vraag is of deze medewerkers volledig vrijwillig deze keuze kunnen maken. Toestemming is geen geldige grondslag. Een alternatief is om voor deze medewerkers een apart YouTube-account te maken (zodat de informatie over hun eigen werk-account niet gedeeld wordt met Google).
- Een andere optie is een YouTube account met meerdere gebruikers. Dit maakt volgen van een persoon onmogelijk, maar deze optie geeft een beveiligingsrisico omdat het account gedeeld wordt.
- YouTube video's zoeken en/of afspelen op gedeelde laptops in gastmodus is wel een optie.
- YouTube cookies blokkeren

De onderstaande opties beperken de risico niet:

- YouTube video's afspelen met een privé-account is geen optie. De school blijft verantwoordelijk voor gebruikte/voorgeschreven leermiddelen. Ook bij een privé-account zoeken leerlingen in opdracht van de school, en Google houdt informatie bij over deze leerlingen.

- De YouTube player uit de Google playstore is geen optie omdat Youtube via de browser te gebruiken is.

- YouTube video's afspelen in incognito modus in de browser. De meeste bescherming die incognito geeft is lokaal. De andere gebruikers kunnen niet zien wat jij op deze computer gedaan hebt. Tracking op het web van de website die je bezoekt, in dit geval Youtube, gaat nog wel door. Voor het anoniem surfen op internet is een private browsing modus niet geschikt.

4. SYNCHRONISATIE

Het gaat hier om de synchronisatie van gegevens uit de Chromebrowser met het Google Workspace account. Deze synchronisatie vindt plaats als inloggen bij Chromebrowser is toegestaan. In de update van de FAQ van oktober 2021 hadden we een andere mogelijkheid gegeven om synchronisatie uit te zetten. Dit menu is van 15 december 2021 terug te vinden in admin.google.com.

5. DATA LOCATIE

Uit overleg met Google blijkt dat Google niet fundamenteel anders omgaat met persoonsgegevens bij de gratis of betaalde editie. De gebruikersdata (bestanden etc.), ook wel customerdata genoemd, wordt zo veel mogelijk binnen Europa verwerkt (opgeslagen).

Ook bij de betaalde versie van Workspace staat niet alle data in de EER. Customerdata staat in de regio van de gebruiker. Voor Vlaamse scholen zal dit in EER datacenters zijn. Over data locatie van meta data (ook wel service data) hebben we nog geen duidelijkheid. Service data en diagnostic valt ook niet onder de data locatie (data region policy).

De optie om gegevens binnen de EU op te slaan, is alleen voor de betaalde versie beschikbaar. Om compliant te zijn, kan deze optie geselecteerd worden als het kan. Alleen in de betaalde versie (standard of plus) kan de datalocatie EER gekozen worden. Deze optie komt niet beschikbaar in fundamentals (gratis versie) of de teaching and learning upgrade. Deze optie biedt Google aan klanten aan, om te kunnen voldoen aan het eigen interne beleid. Zoals gezegd is er weinig verschil in opslag van data voor Vlaamse scholen.

1.

INLEIDING

1.1 WAAROM DEZE GIDS?

Vlaanderen wil via Digisprong de coronacrisis aangrijpen voor een duurzame digitale versnelling in ons onderwijs (zie ook Nota Digisprong, VR 22/12/2020). In totaal gaat het over een investering van 375 miljoen euro. Een van de belangrijkste acties is dat elke leerling vanaf het 5de jaar basisonderwijs een eigen laptop of gelijkwaardig ICT-toestel krijgt. Je school krijgt ook middelen voor ICT-materiaal voor gedeelde toestellen in de lagere jaren en voor leraren. We verwachten dat 600.000 digitale toestellen zullen worden aangekocht.

Naast het versterken van ICT binnen je schoolmuren is het uiteraard ook belangrijk dat je aandacht schenkt aan de privacy van leerlingen en leraren. Deze gids is een aanzet tot het beter afschermen van gevoelige gegevens en het veiliger maken van de Google-omgeving op school.

Belangrijk om vermelden is dat je voor het gebruik en implementeren van een (Google-)platform altijd een DPO-advies nodig hebt van je schoolbestuur of koepel.

Begin 2021 kwam na een onderzoek in Nederland aan het licht dat er privacyrisico's zijn verbonden aan het gebruik van Google G Suite for Education (Workspace for Education). De Nederlandse Autoriteit Persoonsgegevens adviseerde eind schooljaar 2020-2021 Nederlandse scholen om te stoppen met het gebruik van Google Workspace for Education en Education Fundamentals indien Google deze privacyrisico's niet zou verhelpen. Één van de grootste risico's die aan het licht waren gekomen was dat Google zichzelf ziet als verwerkingsverantwoordelijke in plaats van verwerker. Hierdoor kunnen zij zelf bepalen voor welk doel zij metadata verzamelen en op welke manier dit gebeurt. Google heeft aangegeven dat ze een oplossing zullen voorzien voor de Nederlandse onderwijsinstellingen.

De Vlaamse Toezichtcommissie (VTC) waarschuwt[1] dat het noodzakelijk is dat er voldoende garanties worden geboden bij de inzameling en gebruik van de gegevens van de onderwijsbevolking, inclusief ouders en leraren door o.a. softwareleveranciers.

1 https://overheid.vlaanderen.be/sites/default/files/media/VTC/VTC_O_2020_01_DPIA_lijsten_v1_voor_web.pdf?timestamp=1589396929

De VTC raadt in haar advies aan dat onderwijsinstellingen die in het verleden al investeringen hebben gedaan, zich best geleidelijk voorbereiden om een overstap te maken naar een product dat voldoet aan de AVG.

Voor Vlaanderen zijn er door het Departement Onderwijs en Vorming met Google gesprekken opgestart over deze problematiek voor het Vlaamse onderwijs.

Tot er meer duidelijkheid is over welke contractuele, technische en organisatorische maatregelen door Google zullen genomen worden voor het Vlaamse onderwijs, wachten onderwijsinstellingen best af om een Google-licentie af te sluiten voor Workspace for Education.

Onderwijsinstellingen die al geïnvesteerd hebben in Google Workspace for Education kunnen in afwachting van een fundamentele oplossing een aantal instellingen uitvoeren die de beveiliging een stukje verbeteren. Het invoeren van deze instellingen lost het probleem niet op, maar geeft je onderwijsinstelling de tijd om na te denken over de volgende stap.

Als jouw onderwijsinstelling besluit één of meerdere van de maatregelen niet te implementeren, dan heeft dit gevolgen voor de afweging van de privacyrisico's. Je onderwijsinstelling moet dan zelf onderbouwen dat het niet nemen van de technische maatregel geen gevolgen heeft voor de privacyrisico's en/of wat de compenserende maatregelen zijn die de onderwijsinstelling neemt om het privacyrisico van het gebruik van Workspace for Education niet te laten toenemen. Het niet opvolgen van de technische maatregelen is dus niet zonder gevolg en moet nadrukkelijk beschreven en getoetst worden door je verantwoordelijke voor gegevensbescherming.

Deze brochure geeft een overzicht van een aantal instellingen die, mits correct uitgevoerd op toestellen die eigendom zijn van de onderwijsinstellingen, de privacy-risico's op een aanvaardbaar niveau brengen. Privé-toestellen vallen niet onder deze scope en hiervoor moet je apart maatregelen nemen om een groot rest-risico te vermijden.

1.2 MET WIE IS DEZE GIDS TOT STAND GEKOMEN?

Deze gids werd geschreven en gepubliceerd door het Kenniscentrum Digisprong. Dit document is het resultaat van een samenwerking van het Kenniscentrum Digisprong met Kennisnet Nederland, Google, de pedagogische begeleidingsdiensten, de koepels, het Departement Onderwijs en Vorming, Vicli en andere experten uit het werkveld. Dankzij hun expertise, hulp en input hebben we getracht een gids te schrijven die niet enkel doordacht, maar ook vlot bruikbaar is voor de mensen in het werkveld.

1.3 IMPLEMENTATIEWIJZES

Er zijn drie manieren van implementatie voor de te nemen maatregelen:

- Centraal beheer van instellingen via Google Workspace Beheerdersconsole.
- Centraal beheer van instellingen via groepsbeleid (Group Policy) van het besturingssysteem.
- Individuele instellingen.

Maatregelen die de gebruiker en bijbehorende gebruikersaccounts betreffen, kunnen veelal alleen via de Google Workspace omgeving in de Admin console ingesteld worden. Ga naar deze beheerdersomgeving via admin.google.com.

Maatregelen die dataminimalisatie bij het gebruik van producten of functionaliteiten betreffen, kunnen ofwel via de Admin console, ofwel via het groepsbeleid van het besturingssysteem geïmplementeerd worden.

Slechts in een enkel geval zal je als individuele gebruiker maatregelen hoeven nemen. In deze handleiding wordt zo veel mogelijk uitgegaan van gecentraliseerd beheer van de te treffen maatregelen.

2.

CENTRALE BEHEEROPTIES MOGELIJK MAKEN

2.1 ONDER BEHEER PLAATSEN VAN CHROMEBOOKS EN CHROME-BROWSERS

Beheerders van Google Workspace hebben een type account waarmee veel controle kan worden uitgeoefend op de data die met Google gedeeld worden. De meeste maatregelen kunnen centraal vanuit de Google Workspace Admin console beheerd worden.

Om dit mogelijk te maken, moeten de Chromebooks en Chrome-browsers van een organisatie ook daadwerkelijk onder beheer geplaatst zijn. De Chromebooks en Chrome-browsers moeten hiervoor aangemeld zijn bij jouw organisatie en desbetreffende organisatie-eenheid binnen Google Workspace. Deze nemen vervolgens alle instellingen over die je in de Google Workspace Admin console aangeeft.

Bij Chromebooks moet je het gehele apparaat onder beheer plaatsen. Bij de besturingssystemen Windows, macOS en Linux moet je de Chrome-browser onder beheer plaatsen.

2.1.1 CHROMEBOOKS IN BEHEER BRENGEN

Chromebooks in beheer brengen gebeurt veelal via jouw leverancier. Let op, hier is een kost aan verbonden. Voor centraal beheer van Chromebooks heb je de Chrome Education Upgrade licentie nodig. Indien jouw leverancier de Chromebooks nog niet onder centraal beheer gebracht heeft, doe je het volgende:

Dit is een eenmalige licentie (dus geen terugkerende kost). Met het oog op een goede beveiliging van de toestellen is het zeker aangeraden om deze aan te schaffen.

Opgelet: Dit dient enkel uitgevoerd te worden indien het toestel ook eigendom is van je school.

Bij opstart van een nieuwe Chromebook of een Chromebook waar een powerwash (factory reset) op uitgevoerd is, klik je na het verbinden met wifi en het accepteren van de voorwaarden op "Aanmelden voor Enterprise". Indien deze optie niet beschikbaar is, kan je deze oproepen via de toetsencombinatie CTRL+ALT+E of via '*meer opties > Aanmelden voor Enterprise*' in de aanmeldzone. Hier voer je de inloggegevens in van de administrator van het Google Workspace voor Education domein van je school. De Chromebook wordt nu geregistreerd in de Google Workspace omgeving voor centraal beheer.

Vanuit de beheeromgeving van Google Workspace kan je deze Chromebook nu in je gewenste organisatie-eenheid – zoals de klas – plaatsen. Meer informatie hierover vind je terug op de pagina beleid toepassen op verschillende gebruikers[2] in de gids voor Google Workspace-beheerders.

2.1.2 CHROMEBOOK BEHEERDE GASTSESSIE

In een beheerde gastsessie start de gebruiker het Chromebook-besturingssysteem op als gast in plaats van als gebruiker. Er wordt meestal voor deze optie gekozen wanneer het gedeelde toestellen betreft. Zie ook hoofdstuk 6 Instellingen voor toestellen met gedeeld gebruik.

De instellingen voor o.a. netwerk- en printerbeheer van het apparaat worden wel centraal door jou als ICT-beheerder beheerd. De opslag van bestanden op het apparaat is van tijdelijke aard. Als je bijvoorbeeld een afbeelding downloadt, dan wordt deze automatisch verwijderd bij het afsluiten van de Chromebook. Daarnaast opent gedurende een beheerde gastsessie de Chrome-browser ook altijd in gastmodus. Alle browsergerelateerde data (formulieren, browsergeschiedenis, cookies en inlogsessies op websites en webapplicaties) zijn tijdelijk en worden bij afsluiten van het apparaat verwijderd.

Bij het onder beheer plaatsen van een Chromebook, kan je ervoor kiezen om een Chromebook zonder gebruikersaccounts te gebruiken. Dit doe je door de Chromebook automatisch te laten opstarten in een beheerde gastsessie. In de Google Workspace Admin Console doe je dit als volgt:

Apparaten > Chrome > Instellingen > Instellingen voor beheerde gastsessies > Beheerde gastsessie automatisch starten.

In deze handleiding staan veel instellingen die voor gebruikers en browsers gelden. Deze stel je in via:

Apparaten > Chrome > Instellingen > Instellingen voor gebruikers en browsers.

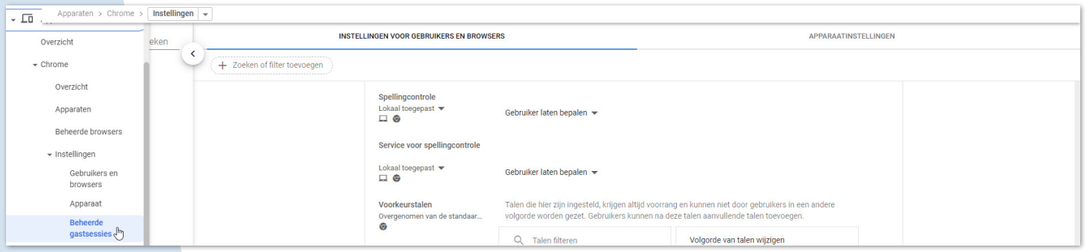
2 https://support.google.com/a/topic/1227584?hl=nl&ref_topic=4511280

Als je Chromebooks in een beheerde gastsessie binnen jouw organisatie gebruikt dan zal je al deze instellingen ook moeten uitvoeren voor de gastsessies via:

Apparaten > Chrome > Instellingen > Instellingen voor beheerde gastsessies.

Als voorbeeld vind je hieronder de instellingen voor spellingcontrole. Alle instellingen beschreven voor gebruikers en browsers zal je dus ook voor beheerde gastsessie moeten uitvoeren. Spellingcontrole uitzetten voor beheerde gastsessies doe je via:

Apparaten > Chrome > Instellingen > Instellingen voor beheerde gastsessies.



2.1.3 CHROMEBROWSERS BEHEREN

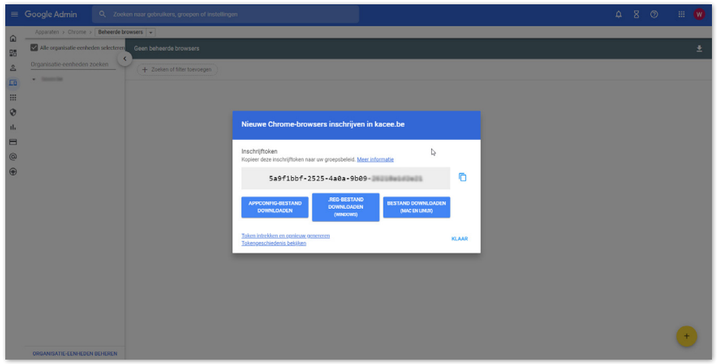
Je kan de Chrome-browserinstellingen alleen centraal beheren als deze in beheer staan. Dit controleer je in de Admin console onder *Apparaten > Chrome > Beheerde browsers*.

Als je een ander besturingssysteem gebruikt, zoals Windows of macOS, voer dan volgende stappen uit:

1. Token voor beheer genereren vanuit de Admin Console.
2. Beheerderspolicy met de beheerderstoken instellen op jouw besturingssysteem.

Je genereert de token onder:

Apparaten > Chrome > Beheerde browsers. Rechtsonder in beeld klik je op het gele plusteken ('+').



Hierna installeer je het groepsbeleid van jouw besturingssysteem via het beleid 'CloudManagementEnrollmentToken'.

2.2 INSTELLINGEN OP HET BESTURINGS-SYSTEEM VIA GROEPSBELEID

Sommige van de te nemen maatregelen kan je meteen op het besturings-systeem uitvoeren via een zogenaamde 'group policy', ofwel groepsbeleid. De instellingen van het besturingssysteem hebben voorrang op de instellingen die via de Admin Console zijn ingesteld. In de overzichtstabel van de maatregelen vind je terug welke policies je op welke manier kan instellen via het groepsbeleid.

Als beheerder zal jij of jouw leverancier voor het beheren van het groepsbeleid gebruik maken van een zogenaamde Group Policy beheertool. Het algemene beheer van de apparaten van jouw organisatie valt buiten het bestek van deze handleiding. Hiervoor kan je eventueel terecht bij jouw leverancier.

Meer informatie over de instellingen via het besturingssysteem vind je op de pagina Lijst met Chrome Enterprise-beleid[3].

3 https://chromeenterprise.google/policies/

3.

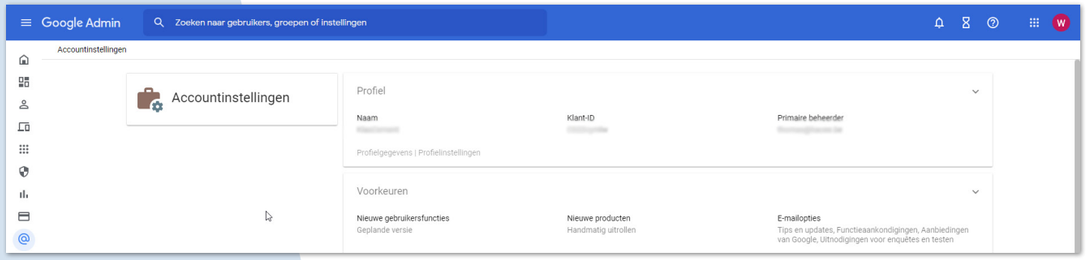
INSTELLINGEN IN DE ADMIN CONSOLE

3.1 GOOGLE WORKSPACE ALS BASISONDERWIJS/VOORTGEZET ONDERWIJS INSTELLEN

Wanneer je als beheerder Google Workspace for Education instelt in de Google Beheerdersconsole, moet je een organisatietype selecteren voor jouw school of onderwijsinstelling. Dit doe je bij de accountinstellingen.

Opmerking: Google gebruikt in de beheerdersconsole de (Nederlandse) term 'voortgezet onderwijs' in plaats van 'secundair onderwijs'.

Accountinstellingen > Profiel > Organisatietype.



Hier kan je kiezen tussen:

- **Basisonderwijs/Voortgezet onderwijs:** inclusief kleuterschool, basisschool, onderbouw middelbare school en bovenbouw middelbare school. Ook samenwerkingsverbanden met alleen dit soort scholen. Selecteer deze optie als jouw leerlingen voornamelijk jonger zijn dan 18 jaar.
- **Hoger onderwijs:** inclusief middelbaar beroepsonderwijs, hoger beroepsonderwijs en wetenschappelijk onderwijs. Selecteer deze optie als jouw leerlingen voornamelijk ouder zijn dan 18 jaar.

Voor gebruikers onder de 18 gelden beperkingen in bepaalde Google-services als ze zijn ingelogd op hun Google Workspace for Education-account. Sommige services zijn daarnaast niet beschikbaar voor gebruikers onder de 18.

- **YouTube** wordt in een beperkte modus uitgevoerd. Met de beperkte modus van YouTube worden mogelijk niet-gezinsvriendelijke video's weggefilterd, terwijl de meeste video's gewoon beschikbaar blijven.
- In **Google zoeken** wordt SafeSearch standaard ingeschakeld (verhinderen van expliciete resultaten zoals bijvoorbeeld adult content), in Google Play kunnen geen aankopen meer gedaan worden en alle beschikbare content bevat de classificatie Iedereen, Iedereen vanaf 10 jaar en ouder of tiener.
- Bij **Google Maps** en **Google Earth** kan geen locatiegeschiedenis geraadpleegd worden, geen betalende functies uitgevoerd worden en worden ze verhinderd om hun eigen locatie te delen.
- Bepaalde services worden uitgeschakeld zoals Blogger, Google Pay e.a.. De volledige lijst vind je hier[4].

3.1.1 MOET IK DE LEEFTIJD INSTELLEN VOOR MIJN HELE ORGANISATIE OF ZIJN ER ALTERNATIEVEN?

Als je kiest voor de optie **Basisonderwijs/Secundair onderwijs** worden verschillende instellingen automatisch doorgevoerd waarbij de privacy van gebruikers standaard (beter) is beschermd. Als de hele organisatie het kenmerk Basisonderwijs/Voortgezet onderwijs krijgt, staan veel functies uit die je wellicht wel wil toestaan voor leraren. Het is daarom niet nodig de hele organisatie op Basisonderwijs/Voortgezet onderwijs te zetten. Dit kan per organisatie-eenheid (bijvoorbeeld 1 organisatie-eenheid voor leerlingen en 1 voor leraren). Meer info daarover vind je hier[5].

3.2 HOE KAN IK EEN PRIVACYVRIENDELIJK E-MAILADRES MAKEN?

Het is aangeraden om zo weinig mogelijk gebruik te maken van de echte namen van medewerkers en leerlingen. Maak e-mailadressen daarom minder herleidbaar. Dat kan door bijvoorbeeld het unieke leerlingnummer of personeelsnummer in het e-mailadres te gebruiken in plaats van de naam, bv. leerling123@school.be in plaats van jan.jansen@school.be. Deze maatregel zorgt ervoor dat de privacy van de leerling beter is beschermd, omdat uit het e-mailadres zelf dan geen persoon is af te leiden. Deze maatregel beperkt ook de gevolgen voor de privacy van leerlingen in geval van een datalek.

Doordat het e-mailadres en leerlingnummer in de Google Workspace Directory zijn gekoppeld aan andere gegevens van de leerling of medewerker, blijven gebruikers voor de school (en voor Google) wel identificeerbaar. Als je een e-mail van leerling123@school.be ontvangt, toont Google Mail dus de naam van de leerling bij dit e-mailadres. De echte voornaam en achternaam kan wel gebruikt worden, intern, in de directory. Als het e-mailadres gelekt

4 https://support.google.com/a/answer/10651918#zippy=%2Cgoogle-zoeken%2Cgoogle-play%2Cgoogle-maps-en-google-earth%2Cgoogle-fotos%2Cservices-die-niet-beschikbaar-zijn-voor-gebruikers-onder-de
5 https://support.google.com/a/answer/175197?hl=nl

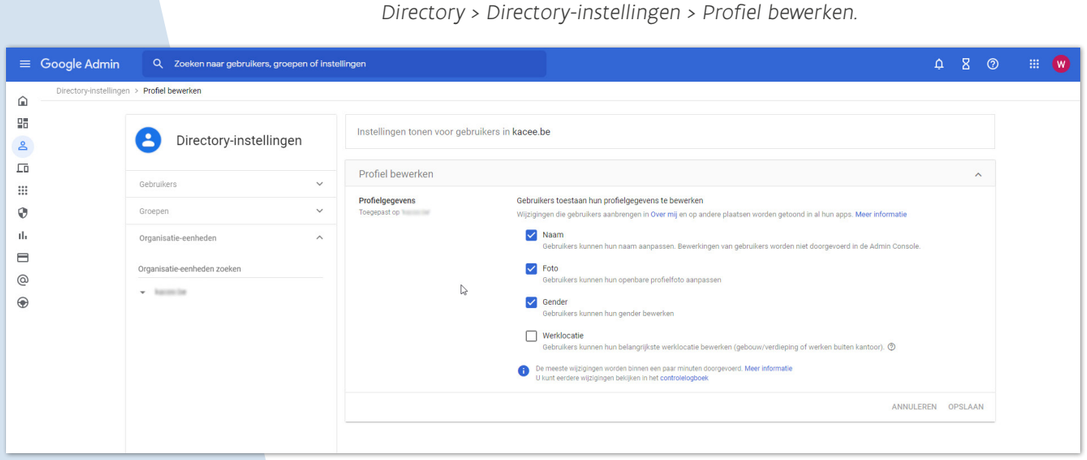
wordt (dus buiten de eigen Google-omgeving), dan wordt de naam van de leerling daar niet bekend (alleen 'leerling123'). Het is ten zeerste aanbevolen om 2FA authenticatie te activeren (indien mogelijk en haalbaar voor je gebruikers). Hoe je dit kan inschakelen en afdwingen, lees je hier[6].

Let op: Wanneer het e-mailadres als unieke identifier gebruikt wordt voor single-sign-on bij andere systemen, is de overstap naar een anoniem e-mailadres lastiger. Je kunt er dan voor kiezen om de bestaande accounts te behouden zoals ze zijn en de nieuwe accounts anoniem te maken.

3.3 GEBRUIKERSPROFIELEN

Beheerders kunnen instellen dat gebruikers hun profiel niet kunnen aanpassen. Hierdoor voorkom je dat leraren en leerlingen alsnog persoonlijke data toevoegen en hun profiel aanvullen met gevoelige gegevens. Dat doe je via:

Directory > Directory-instellingen > Profiel bewerken.



3.4 GEOGRAFISCHE LOCATIE DATAOPSLAG

Als beheerder kan je bepaalde gegevens opslaan in een specifieke geografische locatie door een beleid voor gegevensregio's te gebruiken. De opties voor geografische locaties zijn de Verenigde Staten en Europa.

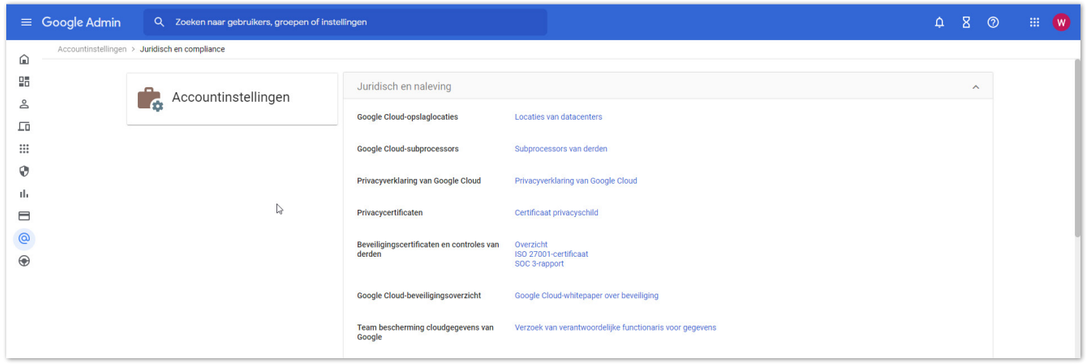
Dataopslag in Europa geeft je in dit geval de hoogste bescherming van persoonsgegevens. Om Europa als dataopslag te kunnen instellen heb je de versie Education Standard of Plus van Google Workspace for Education nodig.

6 https://support.google.com/a/answer/175197?hl=nl

Door deze instelling wordt het dataverkeer met de Verenigde Staten beperkt en blijven gegevens binnen Europa, één van de maatregelen om de risico's te beperken. Data die door deze instelling geografisch beheerd worden, vind je bij de Google Workspace Admin Help[7].

Instellen onder:

Admin console > Accountinstellingen > Juridisch en Compliance.



3.4.1 BIJ DE GRATIS VERSIE (GOOGLE WORKSPACE FOR EDUCATION FUNDAMENTALS) KAN IK NIET KIEZEN VOOR OPSLAG VAN GEGEVENS BINNEN EUROPA. IS DAT NOODZAKELIJK?

De optie om gegevens binnen Europa op te slaan is alleen opgenomen in de **betaalde** versies van Google Workspace for Education (vanaf Google Workspace for Education Standard en hoger). Het opslaan van gegevens binnen Europa is een van de maatregelen die je kan nemen om het privacyrisico van gegevensuitwisseling met de Verenigde Staten te beperken. Kies dus voor opslag binnen Europa als dat (technisch) mogelijk is.

3.5 AANVULLENDE GOOGLE-DIENSTEN (ADDITIONAL SERVICES)

Door het gebruik van deze Additional Services geven onderwijsinstellingen Google toegang tot informatie van hun leerlingen en studenten, zonder dat de onderwijsinstellingen de volledige controle houden over hun gegevens. Dat is in strijd met de AVG (Algemene verordening gegevensbescherming). Dit betekent dat toegang tot aanvullende services (standaard) uitgeschakeld moet zijn.

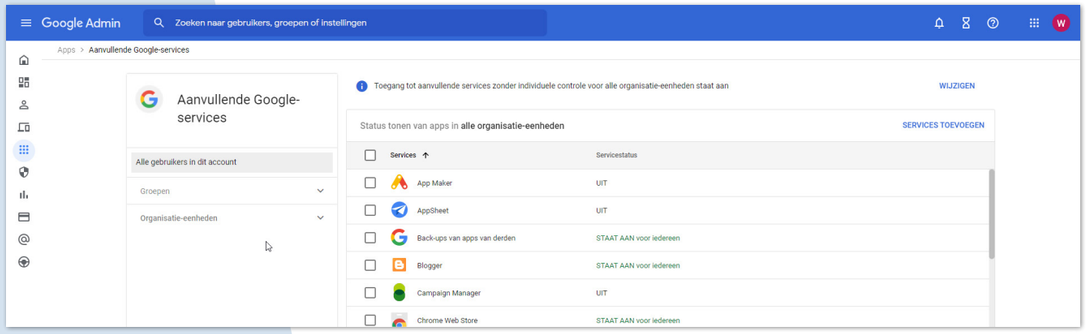
7 https://support.google.com/a/answer/9223653?hl=en

- Wanneer de toegang tot aanvullende diensten is geblokkeerd, kunnen leerlingen wel de zoekfuncties (Google Search) nog steeds gebruiken omdat automatisch uitloggen in SafeSearch-modus aanstaat. Hierdoor worden zij niet gevolgd door Google omdat zij 'onzichtbaar' worden uitgelogd zodat Google de gebruiker van Zoeken niet kent.
- Het gebruik van YouTube door leerlingen en studenten is niet mogelijk zolang zij ingelogd zijn in hun account van Google Workspace for Education. Leraren kunnen YouTube-video's enkel nog met de klas delen door deze te embedden, bijvoorbeeld door de (link naar de) video op te nemen in Classroom of Slides. Hierdoor kunnen video's nog wel bekeken worden.
- Leerlingen of studenten in het secundair onderwijs die er zelf voor willen kiezen om Google Scholar, YouTube of andere aanvullende services te gebruiken, moeten zich afzonderlijk bij Google aanmelden voor een consumentenaccount. Zij moeten uitloggen uit hun account van Google Workspace for Education bij de onderwijsinstelling. Google, en niet je school, is dan verantwoordelijk voor het verkrijgen van geldige toestemming van deze studenten (van 13 jaar en ouder) voor de gegevensverwerking in dergelijke privé-Google-accounts.

Aanvullende services kunnen individueel aan- of uitgezet worden.

Instellen onder:

Admin console > Apps > Aanvullende Google services > Uitschakelen voor iedereen.



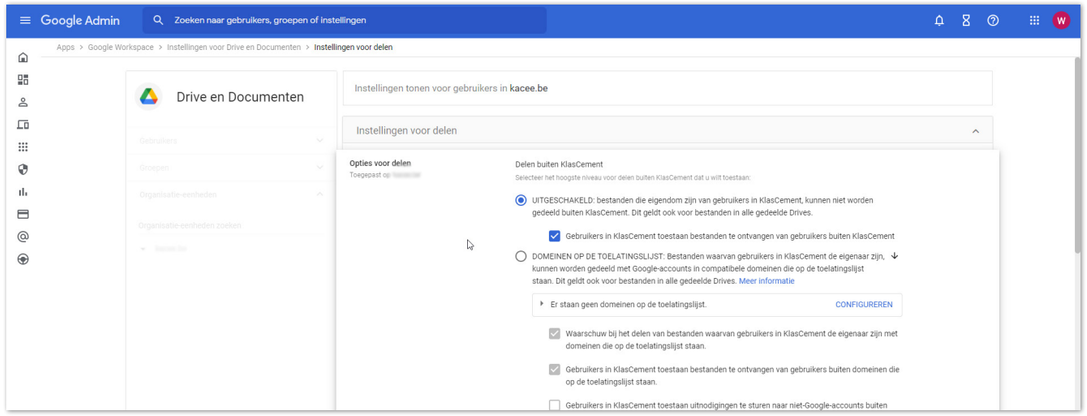
3.6 WELKE MAATREGELEN KAN IK NEMEN BIJ GEBRUIK VAN NAMEN IN FILES EN FOLDERS VAN GOOGLE CLASSROOM?

Als een leraar een opdracht aanmaakt in Google Classroom dan maakt Google automatisch files aan in Google Drive waarin de namen van leerlingen kunnen voorkomen. In de technische handleiding adviseren wij geen namen van personen te gebruiken in files en folders. Om toch Classroom te kunnen gebruiken, kan je de volgende maatregel nemen om de privacy van de betrokkene afdoende te beschermen.

Opgelet: indien u dit uitzet voor leraren kunnen zij niets meer extern delen met stagescholen, ouders of andere externen.

In de Admin Console van Google zet je "extern delen van files en folder" uit.

Apps > Google Workspace > Instellingen voor Drive en Documenten > Instellingen voor delen > Opties voor delen.



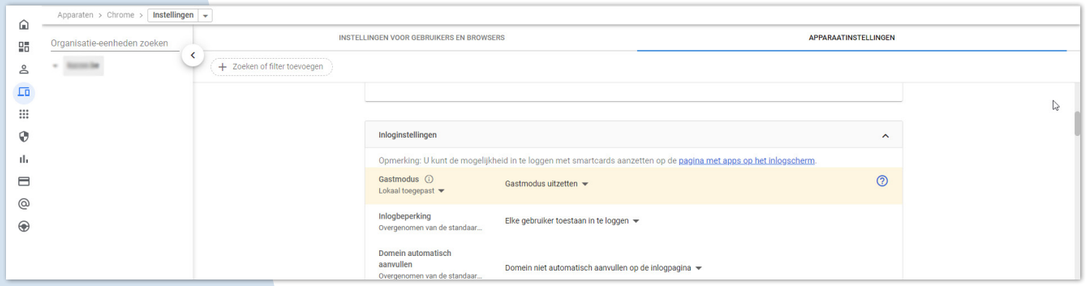
4.

CHROME-APPARAATBELEID INSTELLEN

4.1 GASTMODUS UITSCHAKELEN

Door de gastmodus uit te schakelen wordt verhinderd dat de Chromebooks anoniem gebruikt worden. Om het toestel te gebruiken moet je dus met een account van de school inloggen.

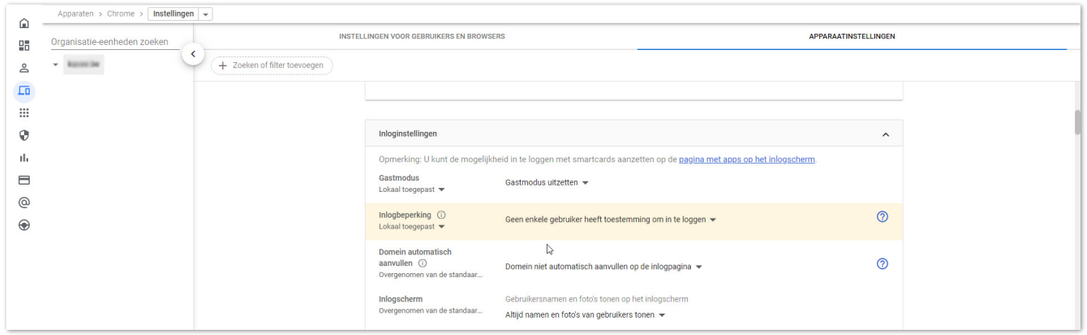
Apparaten > Chrome > Instellingen > Apparaat > inloginstellingen



4.2 INLOGBEPERKING

Door een inlogbeperking in te stellen kunnen gebruikers niet inloggen met een persoonlijke Google-account. De knop 'Persoon toevoegen' is niet beschikbaar.

Apparaten > Chrome > Instellingen > Apparaat > Inloginstellingen.

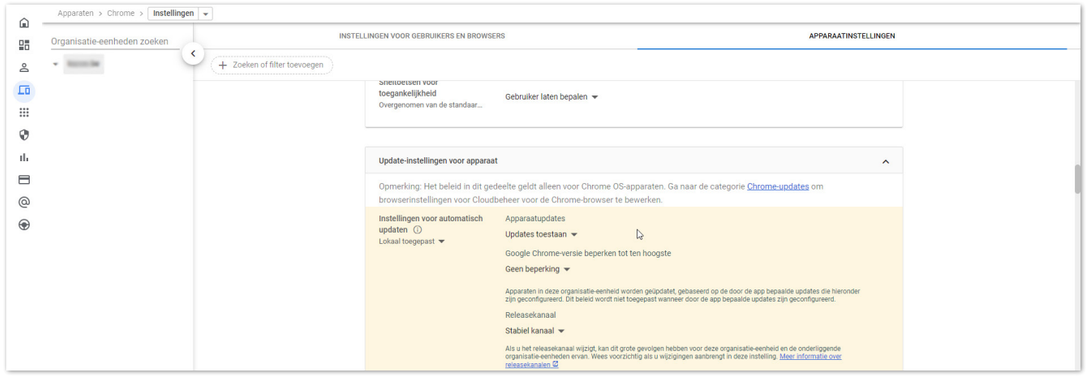


4.3 AUTOMATISCHE UPDATES

Het is afgeraden om de automatische updates uit te zetten voor iedere gebruiker. Het is ook afgeraden om de Google Chrome-versie te beperken. Softwareondersteuning is namelijk enkel beschikbaar voor de nieuwste versie van Chrome OS.

Opgelet: als auto-updates geconfigureerd zijn dan worden IP-adressen en hardware-ID's naar de Google-servers gestuurd. Indien toestellen mee naar huis genomen worden, kan er ook gewerkt worden via 'Updates implementeren volgens een specifiek schema' onder het item 'Implementatieplan'.

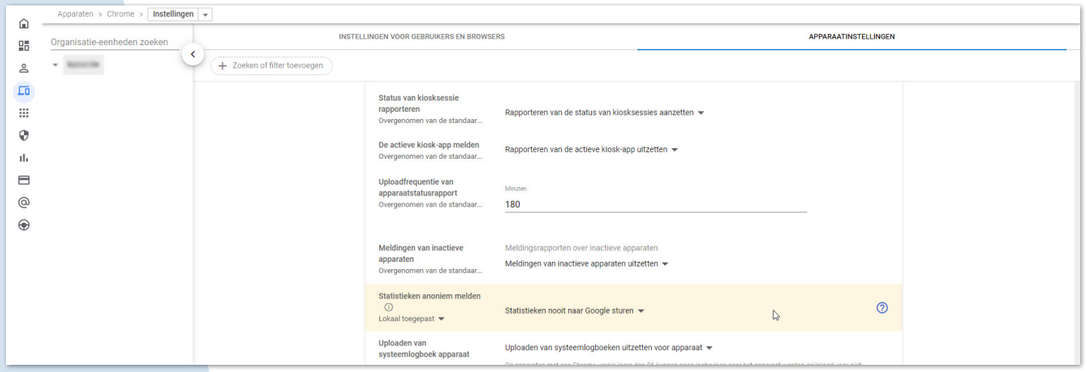
Apparaten > Chrome > Instellingen > Apparaat > Update-instellingen voor apparaat.



4.4 STATISTIEKEN ANONIEM MELDEN UITSCHAKELEN

Deze instelling geeft aan of het Chrome OS-apparaat gebruiksstatistieken en crashrapporten naar Google verzendt wanneer een systeem- of browserproces mislukt. Gebruiksstatistieken bevatten geaggregeerde informatie, zoals voorkeuren, klikken op knoppen en geheugengebruik. Schakel deze bij voorkeur uit.

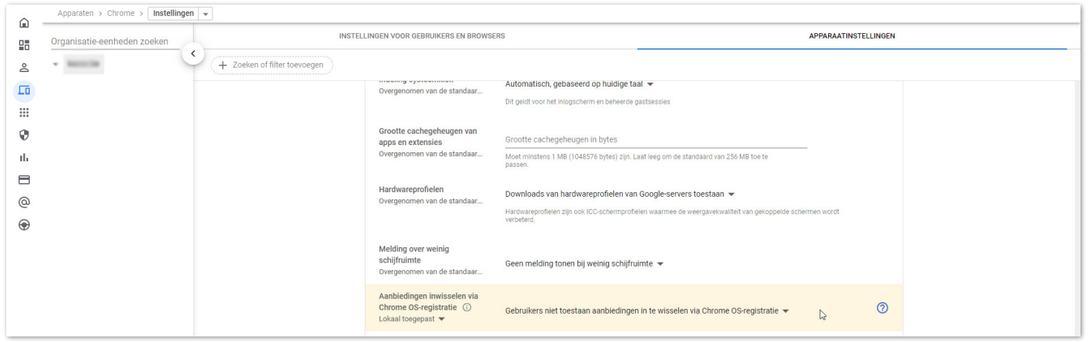
Apparaten > Chrome > Instellingen > Apparaat > Gebruikers- en apparaatrapporten.



4.5 AANBIEDINGEN INWISSELEN VIA CHROME OS-REGISTRATIE UITSCHAKELEN

Het is beter om gebruikers binnen de organisatie te verhinderen aanbiedingen in te wisselen via Chrome OS-registratie. Deze aanbiedingen zijn kosteloze proefversies en speciale aanbiedingen voor gebruikers van (nieuwe) Chromebooks. Denk aan YouTube Premium, Stadia ...

Apparaten > Chrome > Instellingen > Apparaat > Andere instellingen.



5.

CHROME-BELEID INSTELLEN VOOR BROWSERS

Als beheerder kan je de Chrome-browser implementeren voor gebruikers op Microsoft-, Apple- en Linux-computers. Vervolgens kan je meer dan 200 beleidsregels beheren voor het gebruik van Chrome, zoals met welke apps en extensies gebruikers kunnen werken, gegevensbeveiliging en privacy, en browserfuncties.

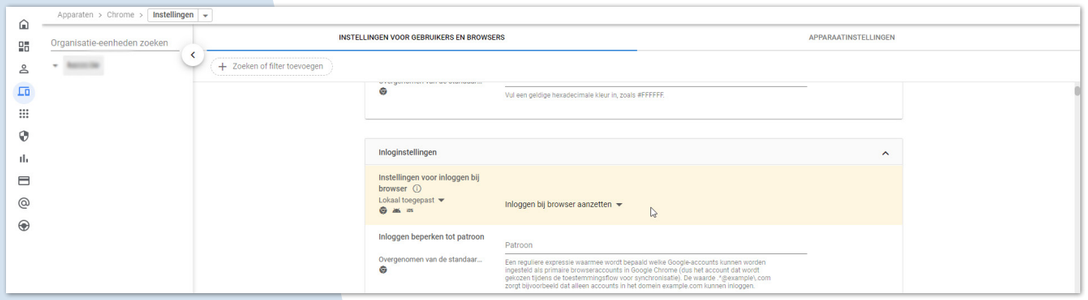
Meer over het beheren van browsers vind je hier[8].

5.1 INLOGGEN BIJ CHROME-BROWSER

Voor beheerde Chrome-browsers is het aangeraden om het inloggen op Chrome-browsers aan te zetten. Op deze manier worden de Google Workspace privacysettings afgedwongen.

"Inloggen bij browser" kan ingesteld worden via:

Apparaten > Chrome > Instellingen > Gebruikers en browsers > Inloginstellingen > Inloggen bij browser aan zetten.

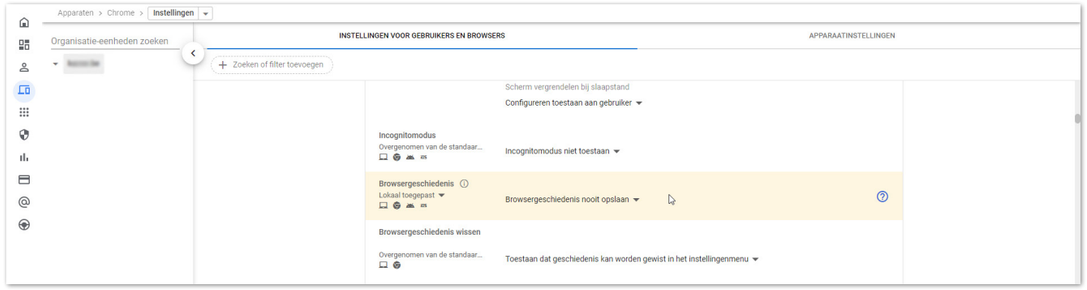


8 https://support.google.com/chrome/a/answer/188446?hl=nl&ref_topic=4386908

5.2 BROWSERGESCHIEDENIS

Hierdoor worden alle browsergerelateerde data (formulieren, browsergeschiedenis, cookies en inlogsessies op websites en webapplicaties) tijdelijk. Bij het afsluiten worden deze data van het apparaat verwijderd.

Apparaten > Chrome > Instellingen > Gebruikers en browsers > Beveiliging.

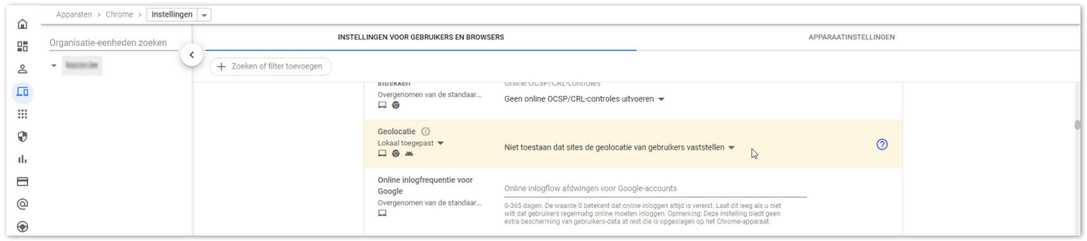


5.3 GEOLOCATIE

Hiermee kan je instellen of de fysieke locatie van een gebruiker door websites mag worden bijgehouden. In de Chrome-browser komt dit beleid overeen met de gebruikersopties in de instellingen van Chrome.

Opgelet: Android-apps hebben met deze instelling geen toegang meer tot locatie en krijgen hierdoor misschien een beperkte functionaliteit.

Apparaten > Chrome > Instellingen > Gebruikers en browsers > Beveiliging.

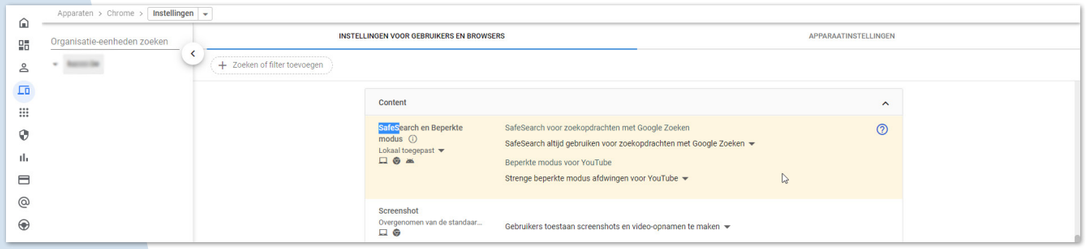


5.4 SAFESEARCH EN BEPERKTE MODUS

Met deze instelling zet je SafeSearch aan of uit. SafeSearch filtert expliciete content, zoals pornografie, uit de zoekresultaten van gebruikers. Voor domeinen in het basis- en secundair onderwijs moet "de standaardinstelling SafeSearch" altijd gebruikt worden voor zoekopdrachten met Google Zoeken.

Ook voor YouTube is het aangeraden om over te schakelen naar 'Strenge beperkte modus afdwingen voor YouTube'. Hiermee worden gebruikers gedwongen de 'Beperkte modus' te gebruiken. Met deze modus wordt via een algoritme bepaald welke video's kunnen worden bekeken, gebaseerd op de content ervan.

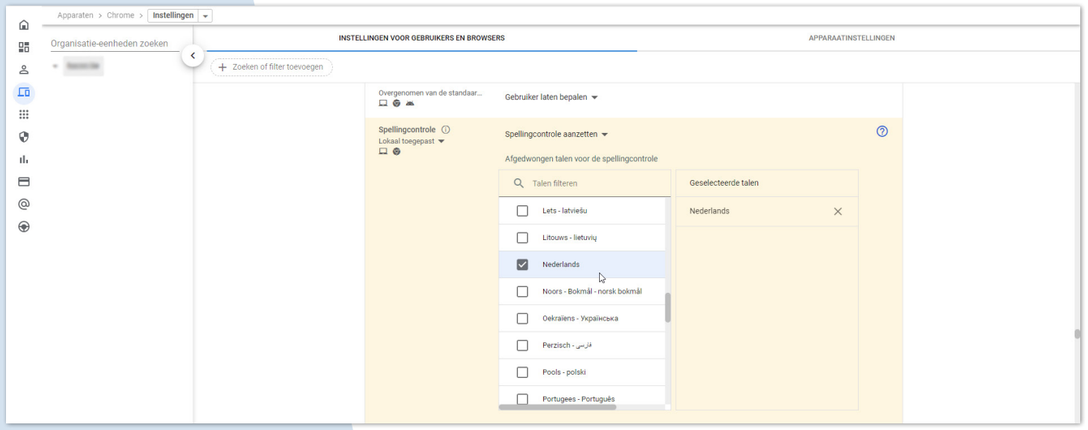
Apparaten > Chrome > Instellingen > Gebruikers en browsers > Content



5.5 SPELLINGCONTROLE LOKAAL INSTELLEN

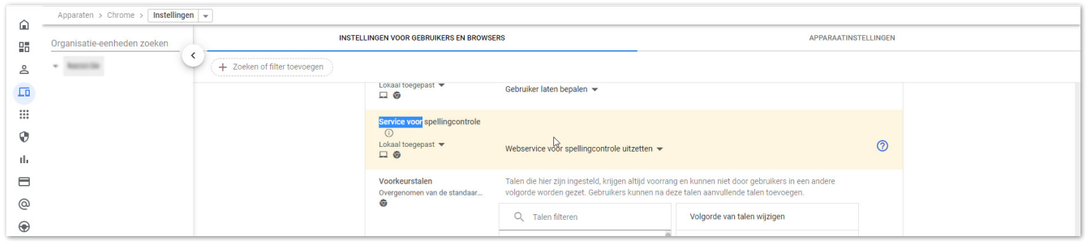
Door de spellingcontrole aan te zetten en de webservice uit te zetten, wordt er enkel lokaal op spelling gecontroleerd. Vink de talen aan waarop gecontroleerd mag worden. De functie spellingcontrole werkt uiteraard alleen als de data door Google op spelling gecontroleerd kunnen worden. Hierbij worden woorden, zinnen of zinsdelen uitgewisseld met Google. Omdat de verwerking van de spellingcontrole in de Verenigde Staten en niet lokaal op de computer van de gebruiker plaatsvindt, wordt dit als een risico beschouwd. Om deze reden moet de spellingcontrole uitstaan zodat data niet gedeeld wordt.

Apparaten > Chrome > Instellingen > Gebruikers en browsers > Gebruikerservaring.



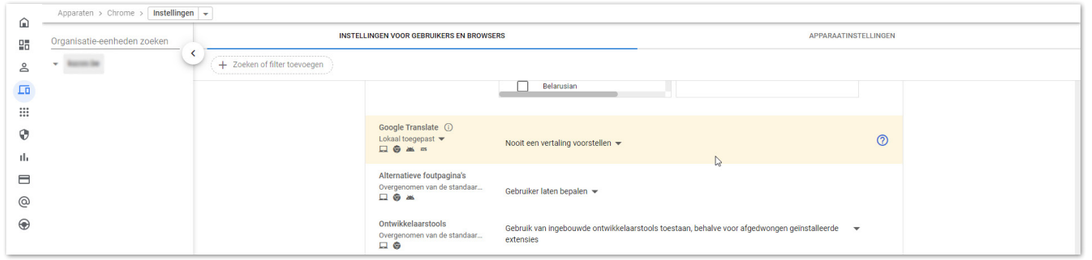
Zet hierna de webservice uit.

Apparaten > Chrome > Instellingen > Gebruikers en browsers > Gebruikerservaring



5.6 GOOGLE TRANSLATE BEPERKEN

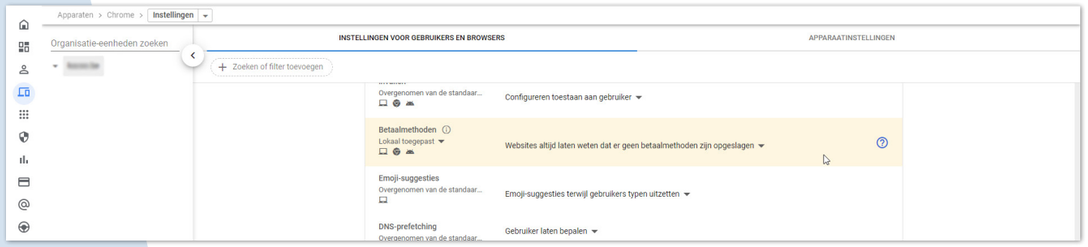
Wat geldt voor het uitzetten van de spellingcontrole, geldt ook voor de vertaalfunctie van Google voor websites die worden bezocht. Deze werkt uiteraard alleen als de data door Google verwerkt kunnen worden. Omdat de verwerking van de vertaalgegevens in de Verenigde Staten en niet lokaal op de computer van de gebruiker plaatsvindt, wordt dit als een risico beschouwd. Om deze reden kies je beter voor de optie "Nooit een vertaling voorstellen".



5.7 BETAALMETHODEN

Hierdoor geef je websites geen toestemming om te controleren of er betaalmethoden opgeslagen zijn op het toestel.

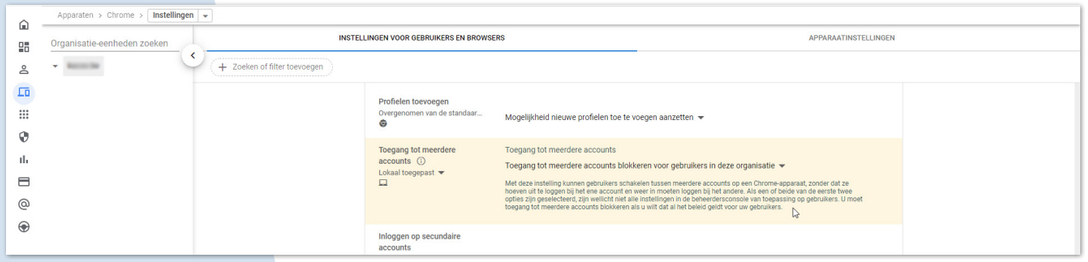
Apparaten > Chrome > Instellingen > Gebruikers en browsers > Gebruikerservaring.



5.8 TOEGANG TOT MEERDERE ACCOUNTS

Door de optie 'Toegang tot meerdere accounts blokkeren voor gebruikers in deze organisatie' te kiezen, kunnen gebruikers slechts met één (beheerd) account inloggen op het toestel.

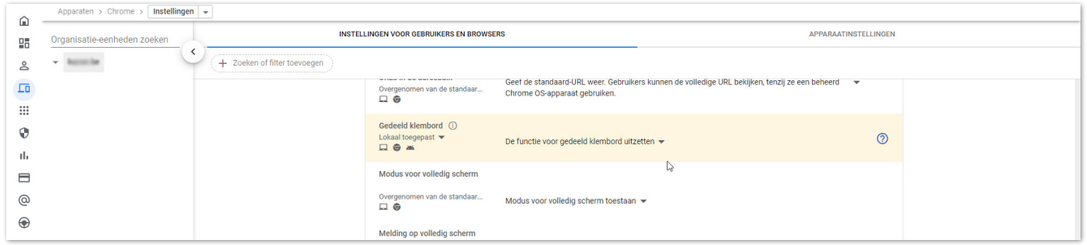
Apparaten > Chrome > Instellingen > Gebruikers en browsers > Gebruikerservaring.



5.9 GEDEELD KLEMBORD

Met een gedeeld klembord kunnen ingelogde gebruikers tekst kopiëren en plakken tussen Chrome-desktops en Android-apparaten als Chrome-synchronisatie aanstaat. Aangezien er geen controle is op waar deze tekst tussentijds opgeslagen wordt, schakel je dit beter uit.

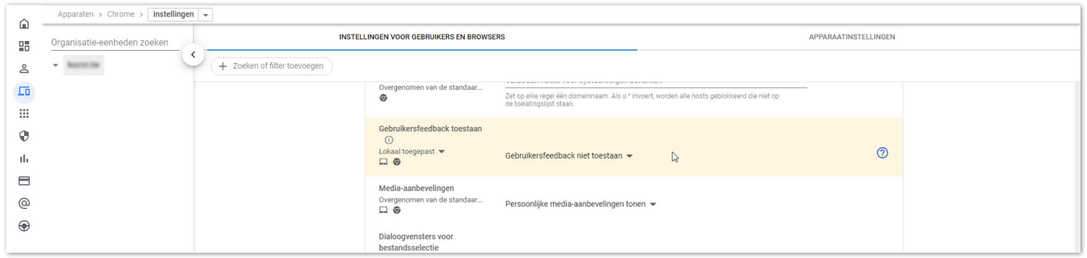
Apparaten > Chrome > Instellingen > Gebruikers en browsers > Gebruikerservaring.



5.10 GEBRUIKERSFEEDBACK TOESTAAN

Kies voor de optie 'Gebruikers niet toestaan dat ze feedback delen met Google'. Als je deze functie niet instelt, kunnen gebruikers feedback naar Google sturen. Hierbij kan veel persoonlijke of zelfs gevoelige informatie gedeeld worden, waar Google (en niet je onderwijsinstelling) verantwoordelijk voor is.

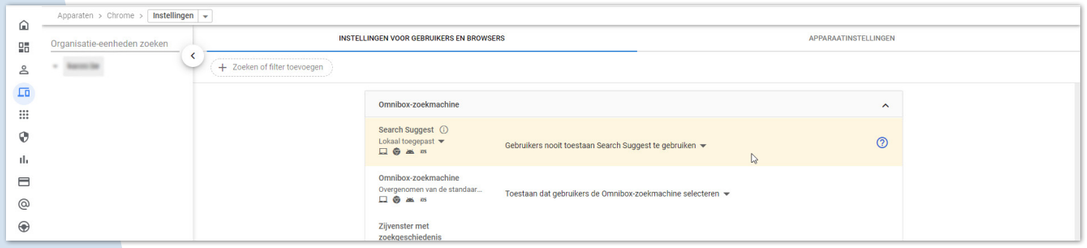
Apparaten > Chrome > Instellingen > Gebruikers en browsers > Gebruikerservaring.



5.11 SEARCH SUGGEST

De functie 'Download Search Suggesties' wordt getoond aan ingelogde gebruikers bij het openen van een nieuw tabblad. Voor deze suggesties moet Google de browsergeschiedenis bijhouden. Zet deze functie uit om het verzamelen en delen van deze persoonlijke data met Google te voorkomen.

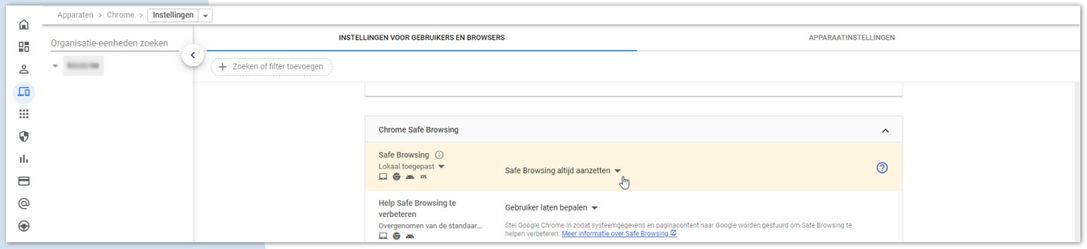
Apparaten > Chrome> Instellingen> Instellingen voor gebruikers en browsers > Omnibox-zoekmachine > Gebruikers nooit toestaan search suggest te gebruiken.



5.12 SAFE BROWSING

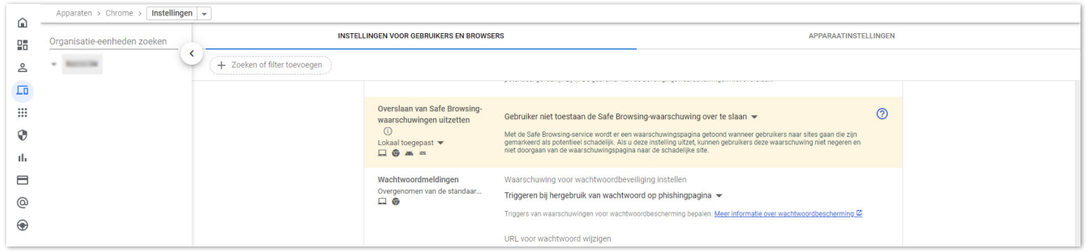
Met de functie 'Safe Browsing' stuurt de Chrome-browser regelmatig systeeminformatie en de inhoud van bezochte pagina's naar Google. De inhoud van dergelijke pagina's kan persoonsgegevens bevatten bij bijvoorbeeld het gebruik van leermiddelen. Het is niet nodig deze informatie bij te houden en te delen met Google. Zet deze systeemrapportages daarom uit.

Apparaten > Chrome > Instellingen voor gebruikers en browsers > andere instellingen > Help safe browsing te verbeteren > Het verzenden van aanvullende gegevens om safe browsing te helpen verbeteren uitschakelen.



Wijzig de instelling 'Overslaan van Safe Browsing-waarschuwingen uitschakelen' naar 'Gebruiker niet toestaan de Safe Browsing-waarschuwing over te slaan'.

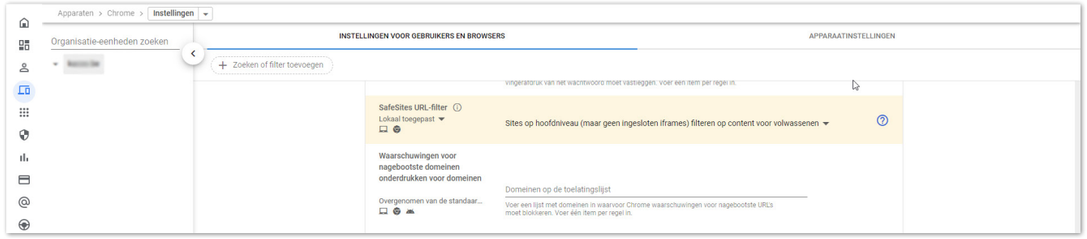
Apparaten > Chrome > Instellingen voor gebruikers en browsers > Chrome Safe Browsing.



5.13 SAFESITES URL-FILTER

Hiermee worden de sites op het hoofdniveau gefilterd op content voor volwassenen, pornografische sites worden niet weergegeven voor gebruikers. Ingesloten iframes worden niet gefilterd.

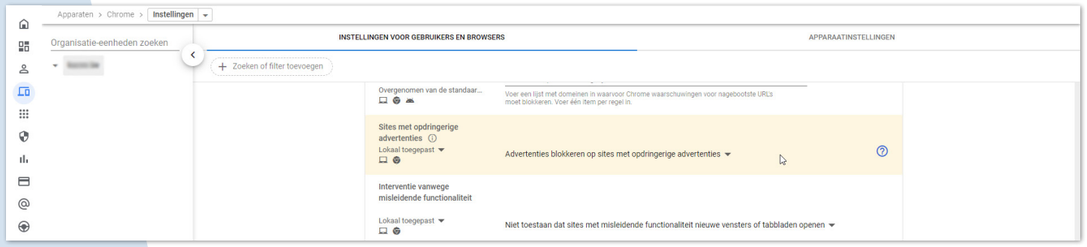
Apparaten > Chrome > Instellingen > Gebruikers en browsers > Chrome Safe Browsing.



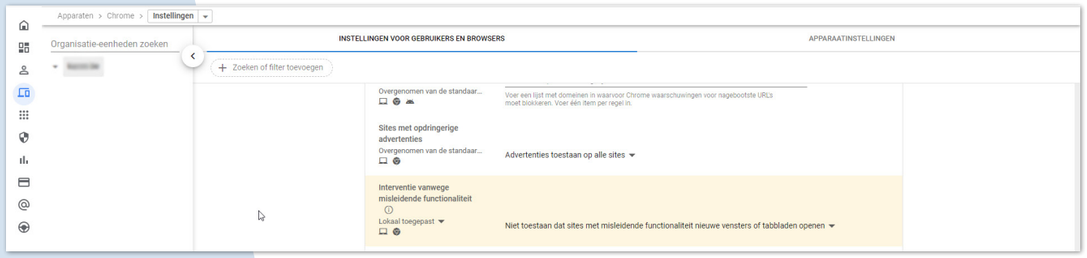
5.14 SITES MET OPDRINGERIGE ADVERTENTIES

Je kan voorkomen dat er advertenties worden weergegeven op sites met opdringerige advertenties.

Apparaten > Chrome > Instellingen > Gebruikers en browsers > Chrome Safe Browsing.



Kies daarna de volgende instelling in de rij, 'Interventie vanwege misleidende functionaliteit'. Op deze manier verhinder je dat een website nieuwe vensters of tabbladen opent.



6.

INSTELLINGEN VOOR TOESTELLEN MET GEDEELD GEBRUIK

6.1 BEHEERDE GASTSESSIES INSCHAKELEN

Met beheerde gastsessies kunnen meerdere gebruikers hetzelfde apparaat met Chrome OS delen zonder in te loggen op hun Google-account. Gebruik bijvoorbeeld beheerde gastsessies om Chrome-apparaten te configureren als leenapparaten, gedeelde computers, toestellen met een kioskfunctie ...

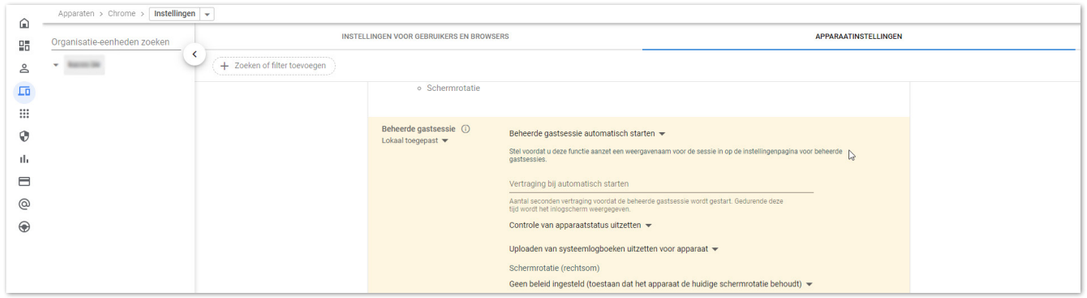
Met beheerde gastsessies krijgen jouw gebruikers een volledige browse-ervaring en toegang tot meerdere websites in venstermodus, niet op volledig scherm.

Plaats apparaten die gebruikers zullen gebruiken om beheerde gastsessies uit te voeren in een aparte organisatie-eenheid. Je kan een Chrome-apparaat slechts in één organisatie-eenheid tegelijk plaatsen. Je kan daarna instellingen voor beheerde gastsessies toepassen op apparaten in die organisatie-eenheid.

Opgelet: voer deze instelling niet door voor al jouw toestellen, maar enkel op de desbetreffende organisatie-eenheid!

Kies voor 'beheerde gastsessie automatisch starten' en vink de vakjes rond meldingen uit.

Apparaten > Chrome > Instellingen > Apparaat > Kiosk-instellingen.

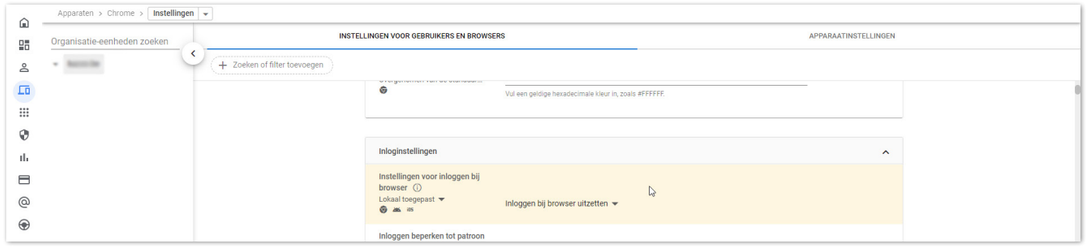


6.2 INLOGGEN OP CHROME BIJ BEHEERDE GASTSESSIES

Voor toestellen met gedeeld gebruik is het afgeraden om in te loggen op Chrome-browsers om evidente privacyredenen.

Stap 1: 'Inloggen bij Browser' uitzetten onder:

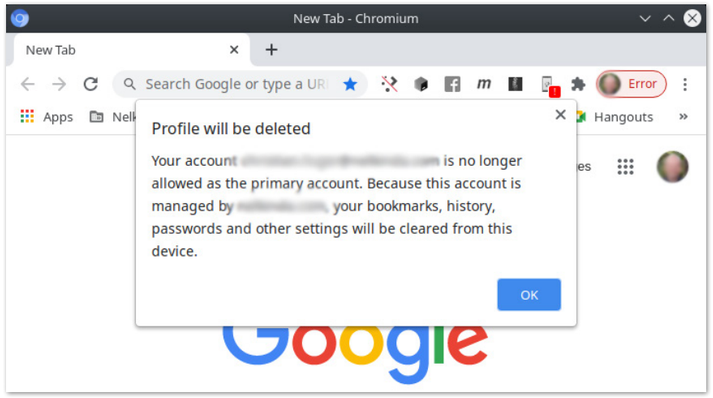
Apparaten > Chrome > Instellingen > Instellingen voor gebruikers en browsers > Inloginstellingen > Inloggen bij browser aanzetten.



6.2.1 WAAROM KRIJG IK EEN POP-UP TE ZIEN ALS "INLOGGEN BIJ DE CHROME-BROWSER" NIET IS TOEGESTAAN?

Als het Chrome-browseraccount is gekoppeld aan het Google Workspace-account, dan log je in Chrome in met je Google Workspace-account. Dan

worden persoonlijke settings gesynchroniseerd met het Google Workspace-account. Als de optie om in te loggen bij de Chrome-browser is uitgezet, krijgen gebruikers die favorieten in de browser hebben opgeslagen deze pop-up te zien: **Profile will be deleted**.



Het profiel dat wordt verwijderd, is het Chrome-browseraccount met favorieten, wachtwoorden en dergelijke. Het is niet het Google Workspace-account. Je bent dus alleen jouw persoonlijke instellingen kwijt.

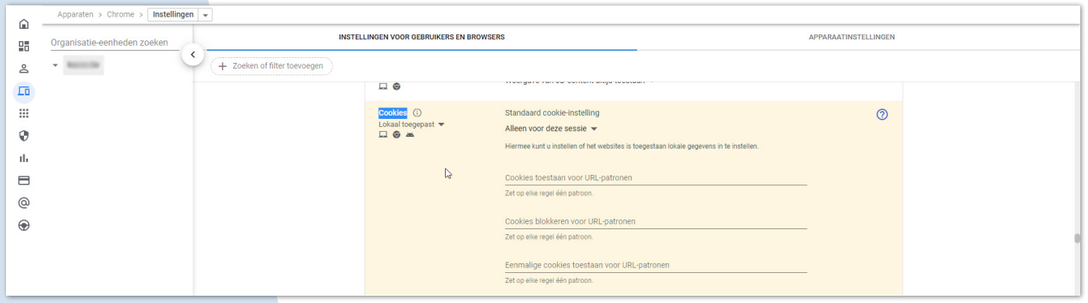
Volgens de instellingen van deze handleiding is inloggen bij de Chrome-browser niet toegestaan. Je kan dan alleen nog lokale browserprofielen aanmaken. Het browserprofiel 'verhuist' dan niet mee als er op een ander device wordt ingelogd. Zodra een nieuwe Chrome-browser beschikbaar komt waarbij Google dataverwerker is in plaats van verwerkingsverantwoordelijke, kan deze setting heroverwogen worden.

7.

YOUTUBE

7.1 WAAROM KAN IK NIET MEER INLOGGEN BIJ YOUTUBE MET MIJN GOOGLE WORKSPACE-ACCOUNT?

Doordat aanvullende Google-diensten niet onder de Google Workspace for Education-overeenkomst vallen, moeten deze diensten uit staan. YouTube is een van de aanvullende diensten. Het gebruik ervan is een hoog risico voor leerlingen en medewerkers, omdat je school geen controle heeft over hun persoonsgegevens die Google verzamelt of gebruikt.



Je kan door het uitzetten van de aanvullende diensten niet meer inloggen bij YouTube met jouw Google Workspace-account. Dit betekent dat je geen playlists meer kan aanmaken of video's uploaden. Je kan wel nog video's bekijken in de embedded mode, zoals beschreven in de technische handleiding. Als je de YouTube-player embedt in Google Workspace core services (zoals Sites of Classroom) worden er geen advertenties meer getoond. De YouTube-cookies van de embedded player voldoen aan de nieuwe privacyvoorwaarden.

7.2 WORKAROUNDS

Je kan in Google Workspace een organisatie-eenheid creëren waarin afgeweken wordt van de geldende privacyinstellingen. In deze organisatie-eenheid kan je enkele generieke, anonieme accounts aanmaken die wel toegang krijgen tot YouTube. Als deze accounts niet naar personen te herleiden zijn, bijvoorbeeld youtubebeheer1@school.be, heeft dit geen of weinig impact op je privacy. Vanaf deze accounts kan je dan toch video's uploaden.

Ook zijn er scholen die gebruikmaken van een laptop of computer waarop niet of anoniem is ingelogd. Leerlingen kunnen in de klas dan op die laptop of computer YouTube gebruiken voor huiswerkopdrachten. Op deze manier worden ook geen persoonsgegevens verzameld, waardoor er geen (hoog) privacyrisico is.

Let op: zorg er in alle gevallen voor dat er geen audiovisueel materiaal van herkenbare kinderen wordt geüpload. Google is daarvoor nog steeds verwerkingsverantwoordelijke.

8.

COOKIES

8.1 WAT ZIJN THIRD PARTY COOKIES?

Er zijn verschillende types cookies:

- **First party cookies** worden gemaakt door de website die je bezoekt. De site wordt weergegeven in je adresbalk.
- **Third party cookies** worden gemaakt door andere sites. Deze sites zijn eigenaar van een deel van de content (zoals advertenties of afbeeldingen) die je ziet (of niet ziet met bijvoorbeeld Facebook-pixels) op de webpagina die je bezoekt. Deze third party cookies kunnen functioneel, analytisch of tracking zijn. Een adverteerder kan met deze cookies een profiel opbouwen gebaseerd op jouw surfgedrag. Hierdoor weet de third party dus meer van jou dan de first party. Dit is een hoge vorm van inbreuk op de privacy.
- **Functionele cookies** zijn nodig om een website beter te laten functioneren. Dit zijn bijvoorbeeld cookies die bijhouden wat er in een winkelwagentje zit.
- **Analytische cookies** worden gebruikt om onder andere bezoekersstatistieken bij te houden.
- **Tracking cookies** volgen de bezoeker tijdens het bezoek aan een website en eventueel ook daarna. Dit wordt onder andere gebruikt voor retargeting. Een voorbeeld hiervan zijn advertenties die je steeds overal terugziet en je dus 'volgen'.

De wet maakt alleen onderscheid tussen cookies die zonder toestemming mogen worden geplaatst (functionele cookies) en cookies die mét toestemming mogen worden geplaatst (bijvoorbeeld tracking- en analytische cookies). Internetbrowsers kunnen dit onderscheid niet maken en herkennen alleen first en third party cookies. Dat betekent dat je aanvullende privacymaatregelen moet nemen.

8.2 WAAROM MOET IK THIRD PARTY COOKIES UITZETTEN?

Google is verwerkingsverantwoordelijke voor alle persoonsgegevens van gebruikers die Chrome gebruiken. Google staat zichzelf toe de persoonsgegevens die worden verwerkt en verzameld via de Chrome-browser over het surfgedrag van leerlingen en leraren te verwerken voor brede commerciële doeleinden (waaronder marketingdoeleinden, gedragsadvertenties, bedrijfsontwikkeling en onderzoek). Gebruikers kunnen geen inzage vragen in deze gegevens. Als school heb je op dit moment dus geen enkele vorm van controle over deze gegevens en daarmee kan de privacy van de gebruikers van Chrome niet worden gegarandeerd.

Je moet je als beheerder van de Google Workspace-omgeving wel bewust zijn van de gevolgen indien alle cookies uitgeschakeld zijn. Dit betekent dat een aantal services en websites niet meer gaan functioneren. In de volgende twee hoofdstukken wordt uitgelegd hoe je dit kan voorkomen. In hoofdstuk 8.3 werk je als school zeer beperkend en bepaal je zelf welke applicaties en websites nog third party cookies mogen gebruiken, in hoofdstuk 8.4 krijg je tips hoe je, als je de optie kiest om third party cookies niet uit te schakelen, de gebruiker toch beter kan beveiligen.

8.3 KAN IK BEPAALDE THIRD PARTY COOKIES OOK TOESTAAN?

In een leeromgeving worden verschillende applicaties gebruikt. Sommige applicaties hebben third party cookies nodig om goed te kunnen functioneren. Een voorbeeld is Google Drive. Als de third party cookies zijn geblokkeerd, kan je niets downloaden uit Google Drive.

Google Drive valt onder de Google Workspace for Education-voorwaarden. De Google Drive-cookies mag je dus accepteren. Het accepteren van third party cookies is echter een globale instelling. Wat betekent dat als je de Google Drive-cookies accepteert, je daarmee in een keer alle third party cookies accepteert. Een workaround is werken met whitelists. Je kan een

whitelist maken van websites waarvan je weet dat de third party cookies geen inbreuk op de privacy veroorzaken. In onderstaande screenshot zie je hoe je whitelists instelt via de Google Workspace admin console.

8.4 IS ER EEN ALTERNATIEF VOOR HET BLOKKEREN VAN COOKIES?

Het gebruik van (tracking- en analytische) cookies levert een hoog privacyrisico op. Het uitzetten van third party cookies is een maatregel om die risico's te beperken. Dit leidt soms tot problemen bij het gebruik van webtoepassingen, bijvoorbeeld bij het inloggen op digitaal lesmateriaal. Het alternatief is om sessiecookies wél toe te staan, in combinatie met het afgedwongen gebruik van een goede ad/tracker blocker. Dat is software voor je internetbrowser die gebruik maakt van lijsten met bekende trackingcookies. Zo wordt het plaatsen van trackingcookies beperkt of voorkomen. Ook zijn deze blockers in staat om bekende malware en schadelijke content te blokkeren. Voor je minderjarige leerlingen die (nog) minder bewust surfen op het internet, biedt het gebruik van deze ad/tracker blockers daarom ook extra bescherming.

Er zijn goede ervaringen met plug-ins die extra bescherming bieden maar als school moet je zelf nagaan of/en welke blocker voor ads/trackers het beste bij jou past en aan de voorwaarden van je eigen organisatie voldoet.

Dit alternatief voor het uitzetten van third party cookies combineer je met het verwijderen van de cookies aan het einde van de sessie of dag.

Dit alternatief voor het uitzetten van third party cookies bepaal je als school zelf, net als de afweging.

8.5 KAN IK COOKIES AUTOMATISCH VERWIJDEREN?

Ja. Stel de Chrome-browser zo in dat de cookies automatisch verwijderd worden als je de sessie sluit. Dit beperkt de impact van de trackingcookies. Zo doe je dit:

1. Klik op de 3 puntjes rechtsboven > 'Instellingen'
2. Kies 'Privacy en beveiliging' > 'Site-instellingen' > 'Cookies en andere sitegegevens'
3. Kies voor de optie 'Cookies en sitegegevens wissen als je alle vensters sluit'

Wil je dit ook in Google Workspace? Kies daar dan voor de cookiesinstelling 'Alleen voor deze sessie'. Dit heeft hetzelfde effect.

Deze werkwijze heeft ook effect op gebruik van SSO-oplossingen. Je blijft dan alleen deze sessie (of werkdag) ingelogd, zodat je sneller weer bij je werk kan in een digitale leer- of kalenderomgeving. Bij het afsluiten van het venster moet je dus opnieuw inloggen.

Bij deze maatregel staat het gebruik van (third party) cookies aan, maar worden deze cookies niet langer dan nodig opgeslagen. Dit beperkt de privacyrisico's slechts gedeeltelijk, want er worden nog steeds third party cookies gebruikt. Maak daarom altijd gebruik van aanvullende maatregelen.

9.

GOOGLE WORKSPACE FOR EDUCATION UP-TO-DATE HOUDEN

9.1 WELKE HULPMIDDELEN ZIJN BESCHIKBAAR OM WIJZIGINGEN TE MONITOREN?

Nadat je alle Google Workspace-settings hebt uitgevoerd, is het belangrijk om wijzigingen te monitoren. Hiervoor zijn de volgende hulpmiddelen beschikbaar:

9.1.1 MAJOR SERVICE ANNOUNCEMENTS

Google stuurt major service announcements (MSA) uit naar het e-mailadres van de primary admin user.

9.1.2 WORKSPACE-UPDATES

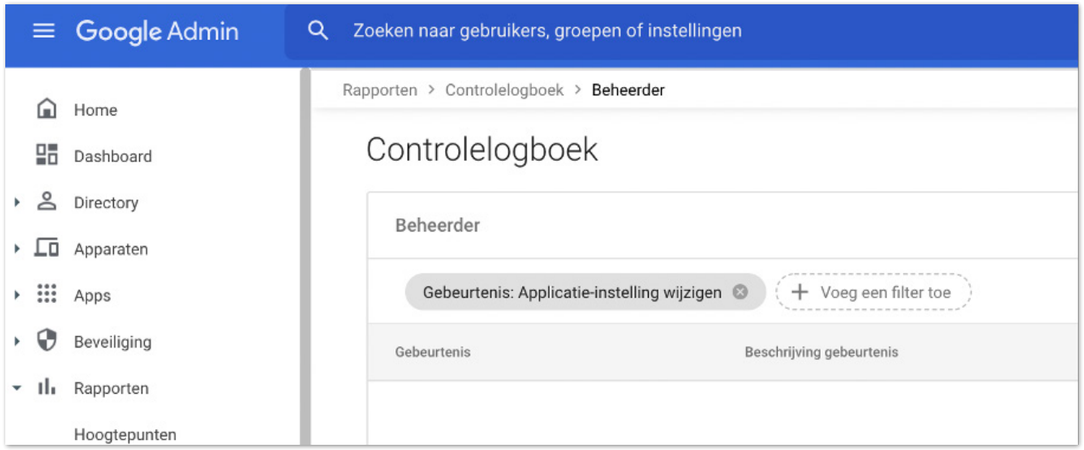
Google schrijft een blog over Workspace-updates. Je aanmelden voor deze updates doe je op deze website[9].

9.1.3 CHROME-UPDATES

Chrome release notes worden hier[10] gepubliceerd.

9.1.4 MELDINGENCENTER

Gebruik meldingencenter om op de hoogte te blijven van belangrijke wijzigingen. Stel een e-mailmelding in voor 'Applicatie-instelling wijzigen' en andere gebeurtenissen die je wil monitoren.



9.1.5 KANALEN KENNISCENTRUM DIGISPRONG

Deze gids zal geregeld een aanpassing krijgen. Kritieke updates zullen ook vermeld worden via de ICT-nieuwsbrief van KlasCement en onze andere kanalen.

9 https://workspaceupdates.googleblog.com/
10 https://support.google.com/chrome/a/answer/7679408#92&zippy=%2Cchrome

10.

CHECKLIST

Alle in deze handleiding genoemde handelingen zijn privacybevorderende maatregelen die meegewogen zijn bij het beperken van de risico's van het gebruik van Google Workspace for Education (Plus) in het onderwijs. Indien je als onderwijsinstelling besluit één of meerdere van de maatregelen niet te implementeren, dan heeft dit gevolgen voor de afweging van de privacyrisico's. De onderwijsinstelling moet dan zelf onderbouwen dat het niet nemen van de technische maatregel geen gevolgen heeft voor de privacyrisico's en/of wat de compenserende maatregelen zijn die de onderwijsinstelling neemt om het privacyrisico van het gebruik van Google Workspace for Education niet te laten toenemen. Het niet opvolgen van de technische maatregelen is dus niet zonder gevolg en moet nadrukkelijk beschreven en getoetst worden door de DPO in overleg met je aanspreekpunt informatieveiligheid.

10.1 BASISINSTELLINGEN		
4.1	Google Workspace als Basisonderwijs/Voortgezet onderwijs instellen	☐ uitgevoerd
4.2	Privacyvriendelijk e-mailadressen aanmaken	☐ uitgevoerd
4.3	Gebruikersprofielen beveiligen	☐ uitgevoerd
4.4	Geografische locatie dataopslag instellen op Europa	☐ uitgevoerd
4.5	Aanvullende Google-diensten (Additional Services) blokkeren	☐ uitgevoerd
4.6	Bestanden delen uitschakelen buiten de Workspace-omgeving	☐ uitgevoerd
10.2 CHROMEBOOKS		
5.1	Gastmodus uitschakelen	☐ uitgevoerd
5.2	Inlogbeperking	☐ uitgevoerd
5.3	Automatische updates	☐ uitgevoerd
5.4	Statistieken anoniem melden uitschakelen	☐ uitgevoerd
5.5	Aanbiedingen inwisselen via Chrome OS-registratie uitschakelen	☐ uitgevoerd
10.3 CHROME-BROWSER		
6.1	Inloggen bij Chrome-browser aanzetten	☐ uitgevoerd
6.2	Browsergeschiedenis	☐ uitgevoerd
6.3	Geolocatie uitzetten	☐ uitgevoerd
6.4	SafeSearch en beperkte modus aanzetten	☐ uitgevoerd
6.5	Spellingcontrole lokaal instellen	☐ uitgevoerd
6.6	Google Translate beperken	☐ uitgevoerd
6.7	Betaalmethoden opslaan tegengaan	☐ uitgevoerd
6.8	Toegang tot meerdere accounts blokkeren	☐ uitgevoerd
6.9	Gedeeld klembord uitschakelen	☐ uitgevoerd
6.10	Gebruikersfeedback niet toestaan	☐ uitgevoerd
6.11	Search Suggest uitschakelen	☐ uitgevoerd
6.12	Safe Browsing-rapportage uitschakelen	☐ uitgevoerd
6.13	SafeSites URL-filter inschakelen	☐ uitgevoerd
6.14	Sites met opdringerige advertenties tegengaan	☐ uitgevoerd
10.4 TOESTELLEN MET GEDEELD GEBRUIK		
7.1	Beheerde gastsessies automatisch starten	☐ uitgevoerd
7.2	Inloggen op Chrome uitschakelen (enkel bij beheerde gastsessies)	☐ uitgevoerd
10.5 COOKIES		
9.3	Third party cookies blokkeren	☐ uitgevoerd

Indien bepaalde instellingen niet overgenomen zijn, kan je hier het nummer van het hoofdstuk noteren en motiveren voor het niet uitvoeren van de actie en/of vermelden welke alternatieve acties je ondernomen hebt.

11.

BRONNEN

Google. (2022). Flanders Technical Guide - Google Workspace for Education.

Kennisnet. (2021, augustus 2). *kennisnet.nl*. Opgehaald van Kennisnet: https://www.kennisnet.nl/app/uploads/kennisnet/publicatie/Kennisnet-Technische-handleiding-Google-Workspace-for-Education.pdf

Sivon. (2021, oktober 29). *Veelgestelde vragen* over het gebruik van Google Workspace en de DPIA Google. Opgehaald van sivon.nl: https://www.sivon.nl/actueel/veelgestelde-vragen-dpia-google-en-het-ap-advies-over-google-workspace/

https://sivon.nl/update-google-workspace-for-education/

Opmerkingen, verouderde screenshots, fouten?
Meld deze via kenniscentrumdigisprong@ond.vlaanderen.be.

COLOFON

Deze gids werd geschreven en gepubliceerd door het Kenniscentrum Digisprong. Dit document is het resultaat van een samenwerking van het Kenniscentrum Digisprong met Kennisnet Nederland, Google, de pedagogische begeleidingsdiensten, de koepels, het Departement Onderwijs en Vorming, Vicli en andere experten uit het werkveld. Digisprong werd gefinancierd door de Europese en de Vlaamse overheid.

Datum van uitgave
Maart 2022
Update mei 2023

Auteurs
Wim Nijst
Davy Van Hemelen
Toon Beens

Met dank aan (in willekeurige volgorde)
Koen Vandenhoudt – Vicli
Lieve Tack – UCLL
Sophie Duhayon – OVSG
Koen Braspenninckx – Koba
Vik Pauwels – SCOOP
Bert Mertens – VZW Spijker
Achim Rosier – GO! SG20
Peter van Antwerpen – OLV Lyceum Genk
Gino de Meester – Katholiek Onderwijs Vlaanderen
Erik Moncarey – Onderwijs Vlaanderen

Eindredactie
Thomas Corthals
Jasper Van Biesen

Ook dank aan alle collega's van het Kenniscentrum Digisprong die van grote waarde waren bij het tot stand komen van dit document.

In samenwerking met Google for Education Benelux.

Grafische vormgeving
Wim Nijst

Departement Onderwijs en Vorming
Kenniscentrum Digisprong
Hendrik Consciencegebouw
Koning Albert II Laan 15 (bus 5A)
1210 Sint-Joost-ten-Node
digisprong.be