



Handleiding Google ChromeOS en Chrome browser

Versie 2.0 februari 2024



Inhoudsopgave

1	Introductie	3
2	Verwerkersovereenkomst ChromeOS	3
3	Chrome Education Upgrade.....	3
4	Privacy instellingen voor ChromeOS en Chrome browser	4
	<i>Zet 'optional services' uit</i>	<i>5</i>
	<i>Gebruik altijd K-12 settings.....</i>	<i>5</i>
	<i>Zet de Chrome Web Store uit.....</i>	<i>6</i>
	<i>Zet de Google Play uit.....</i>	<i>6</i>
	<i>Zet ad personalisatie uit. Voor K-12 is dit de default waarde</i>	<i>7</i>
	<i>Verstuur geen "crash report" naar Google.....</i>	<i>7</i>
	<i>Overweeg "Safe Sites" uit te zetten en een andere filter functie te implementeren.....</i>	<i>7</i>
5	Eindgebruikers instellingen	8
	<i>Switch off Privacy Sandbox</i>	<i>8</i>
	<i>Zet advertentieonderwerpen uit.....</i>	<i>8</i>
	<i>Zet door sites voorgestelde advertenties uit</i>	<i>9</i>
	<i>Zet advertentiemeting uit.....</i>	<i>9</i>
	<i>Gebruik Chrome Sync encryptie.....</i>	<i>10</i>
6	Gebruik privacy vriendelijke browsers settings.....	11
	<i>'Niet bijhouden' uitschakelen (do not track) en website preloading disables</i>	<i>11</i>

Versie beheer

3 juli 2023 (versie 1.0)	Eerste versie van de handleiding
27 februari 2024 (versie 2.0)	Aanpassing in de lay-out Update n.a.v. verificatie op de Google opgeleverde product aanpassingen. Google heeft de product - wijzigingen adequaat doorgevoerd. Verificatie heeft geen invloed op de door scholen in te voeren maatregelen. Scholen moeten nog steeds de maatregelen volgen in deze handleiding.

1 Introductie

In mei 2023 hebben SURF en SIVON met Google overeenstemming bereikt over de nieuwe Terms of Service (ToS) voor het gebruik van Chrome OS en Chrome-browser voor Chromebooks. Nadat je als schoolbestuur deze overeenkomst hebt geaccepteerd en de Chromebooks in beheer hebt genomen, is Google verwerker en ben jij als schoolbestuur verwerkersverantwoordelijke voor de verwerking van persoonsgegevens op Chromebooks (die draaien op ChromeOS) en in Chrome-browsers (die draaien op Chromebooks). Door deze overeenkomst te accepteren en bijbehorende maatregelen door te voeren, beperk je de privacyrisico's voor scholieren en medewerkers bij het gebruik van Chromebooks met ChromeOS en de Chrome-browser.

De zogenaamde processor versie van Chrome (DP Chrome OS) is beschikbaar sinds 12 augustus 2023.

De nieuwe privacy voorwaarden gelden alleen voor de zogenaamde essential services.

2 Verwerkersovereenkomst ChromeOS

Accepteer de nieuwe verwerkersovereenkomst 'ChromeOS Agreement for the Dutch Education Sector'. Nederlandse educatie-instelling zijn hierover geïnformeerd door Google. De overeenkomst is te vinden in de admin console (zie afbeelding);

The image shows two side-by-side screenshots. The left screenshot is from the Google Admin console, specifically the 'Data processor mode for ChromeOS' page. A red circle highlights a button labeled 'SWITCH TO DATA PROCESSOR MODE FOR CHROMEOS'. An arrow points from the text 'Klik hier' to this button. The right screenshot shows the 'Terms of Service' page for the 'ChromeOS Agreement for the Dutch Education Sector'. It contains text about the agreement and sections for '1. Services' and '1.2 Admin Console'. At the bottom right of the Terms of Service page, there are 'CANCEL' and 'ACCEPT' buttons.

3 Chrome Education Upgrade

Scholen kunnen alleen verwerkersverantwoordelijk zijn en Google verwerker als de door de scholen gebruikte apparaten in beheer zijn genomen. Je kunt je Chrome-apparaten in beheer nemen met de zogenaamde Chrome Education Upgrade. Dit is feitelijk een Enterprise editie van Chrome OS.

Chromebooks kennen een zogenaamde Update Expiration Date (AUE)

<https://support.google.com/chrome/a/answer/6220366?hl=en>. Deze datum kun je zien als het einde van de levensduur van het apparaat. Als er geen updates meer beschikbaar zijn voor het apparaat, dien je het dus te vervangen. Schoolbesturen hebben een overweging te maken of een



apparaat dat nog niet in beheer is maar wel dicht tegen de houdbaarheidsdatum zit, alsnog in beheer te nemen of direct te vervangen. Apparaten waarvan de AUE-datum al is gepasseerd, dienen sowieso te worden vervangen.

De standaardinstelling is dat Chrome OS automatisch software-updates uitvoert. Handhaaf deze instelling.

N.B. Het in beheer nemen van apparaten is ook één van de te nemen maatregelen voor mobiele apparaten zoals in norm 11.3 van het normenkader: *'mobile device management of mobile application management (MDM/MAM) wordt gebruikt voor het beveiligen van mobiele apparaten of telewerkfaciliteiten. Dit wordt opgenomen in het IBP-beleid (norm 1.2). Het MDM of MAM moet dusdanig zijn ingesteld dat invulling wordt gegeven aan de elementen van het toetsingskader.'*

4 Privacy instellingen voor ChromeOS en Chrome browser

Dit zijn maatregelen die scholen centraal moeten instellen.

Voor de verwerker versie (data processor) van Chrome heeft Google een nieuwe compliance pagina ingericht. Deze pagina is te vinden onder Chrome -> Compliance -> Data processor

<https://admin.google.com/u/1/ac/chrome/compliance/productoverview>

The screenshot shows the Google Admin console interface. On the left is a navigation menu with 'Admin' at the top, followed by 'Devices', 'Overview', 'Chrome', 'Guides', 'Managed browsers', 'Settings', 'Users and browsers', 'Device', 'Managed guest sessions', 'Apps and extensions', 'Connectors', 'Printers', 'Reports', and 'Compliance'. The 'Data processor' option under 'Compliance' is highlighted. The main content area has a search bar and a breadcrumb trail: 'Devices > Chrome > Compliance > Data processor ChromeOS'. Below this is a header for 'Data processor ChromeOS' with a sub-header 'You are in control of your own personal data.' The main content is titled 'Product overview' and contains a paragraph explaining the data processor mode Terms of Service. Below this is a table with two columns: 'Features/capabilities' and 'Description'. The table lists three services: 'Download service data', 'Takeout customer data', and 'Delete user data', each with a brief description of what it allows administrators to do.

Op deze pagina staan de essential services die onder de nieuwe overeenkomst met Google vallen en waar Google verwerker is.

De optional services vallen niet onder de nieuwe overeenkomst. Google is voor deze diensten nog verantwoordelijke. Google heeft zogenaamde switches ontwikkeld zodat admins de optional services uit kunnen zetten.



Zet 'optional services' uit

Voor nieuwe Google tenants is de default waarde 'uit'. Voor bestaande tenants moeten admins de optional services uit zetten. Het gaat hierbij alleen om optional services waarbij persoonlijke data worden verwerkt.

Vanuit het menu optional services zoals hierboven weergegeven kan je doorklikken naar de diverse settings en daar de service uit zetten. Hieronder staan een drietal voorbeelden. Elke dienst kan individueel uitgezet worden.

The image shows three screenshots of the Google Admin console interface, each representing a different optional service that can be disabled. Each screenshot has a light yellow background and contains the following information:

- Nearby Share:** Shows the service name with an information icon, the status 'Locally applied' with a dropdown arrow, a laptop icon, and the action 'Prevent users from enabling Nearby Share' with a dropdown arrow.
- Google Calendar integration:** Shows the service name with an information icon, the status 'Locally applied' with a dropdown arrow, a laptop icon, and the action 'Disable Google Calendar integration' with a dropdown arrow.
- Spell check service:** Shows the service name, the status 'Locally applied' with a dropdown arrow, a laptop icon, a speech bubble icon, and the action 'Disable the spell checking web service' with a dropdown arrow.

Er is ook een "uber-switch". Deze is alleen beschikbaar voor nieuwe tenants. Met deze switch kunnen alle optional services in een keer uit gezet kunnen worden. **Let op!** Als optional service nu gebruikt worden kan het gebruik van de uber switch tot verlies van functionaliteit of data leiden.

Gebruik altijd K-12 settings

Met een K-12 setting zorg je als school voor de best mogelijke privacy-instellingen. Hanteer voor alle leerlingen en bij voorkeur ook voor alle medewerkers deze setting. Een uitzondering zijn de administrator accounts.

Met de K-12 setting bescherm je je organisatie tegen experimenten met een nieuwe technologie die Privacy Sandbox heet. Privacy Sandbox is een manier om persoonlijke advertenties te kunnen tonen zonder 3rd party cookies te gebruiken. Google zegt géén trials te doen met Privacy Sandbox onder gebruikers die vallen onder de K-12 instellingen. Voor gebruikers die in Workspace gemarkeerd zijn als ouder dan 18 jaar, kun je Privacy Sandbox lokaal uitzetten.

In de admin console -> Account settings -> Age based settings

Age-based access settings ^

Age label
Applied at 'Kennisnet EDU Demo'

Choose an appropriate age label
Your [organization type](#) determines the default setting selected here for groups and org units. Specify a different age label if the default setting does not apply for a group or org unit. [Learn about age-based access settings](#)

Some or all users in this group or org unit are under 18
Access to some Google services or features may be restricted and data in those services or features may be deleted for users in the group or org unit

All users in this group or org unit are 18 or older
Don't select if this group or org unit has any users under 18

i Most changes take effect within a few minutes. [Learn more](#)
You can view prior changes in the [audit log](#)

CANCEL SAVE

Zet de Chrome Web Store uit

De Chrome web store valt niet onder de verwerkersovereenkomst. Default staat de Chrome web store uit.

The screenshot shows the Google Admin console interface. On the left is a navigation menu with 'Admin' at the top, followed by 'Apps' and 'Additional Google services'. The main content area shows 'Settings for Chrome Web Store'. A warning box states: 'Terms of Service This service is not covered by the Google Workspace Agreement. If you do not have the requisite authority to bind the customer or End User to these terms, please disable the service'. Below this, the 'Service status' is set to 'OFF for everyone'.

Zet de Google Play uit

De Google Play valt niet onder de verwerkersovereenkomst. Google Managed Play is een processor service. Tijdens het Chrome onderzoek hebben we niet kunnen vaststellen of de dienst zonder hoge risico's te gebruiken is.

The screenshot shows the Google Admin console interface for 'Settings for Google Play > Service status'. It indicates 'Showing settings for users in all organisational units'. The 'Service status' is set to 'OFF for everyone'. A warning box at the bottom states: 'Most changes take effect within a few minutes. Learn more'.



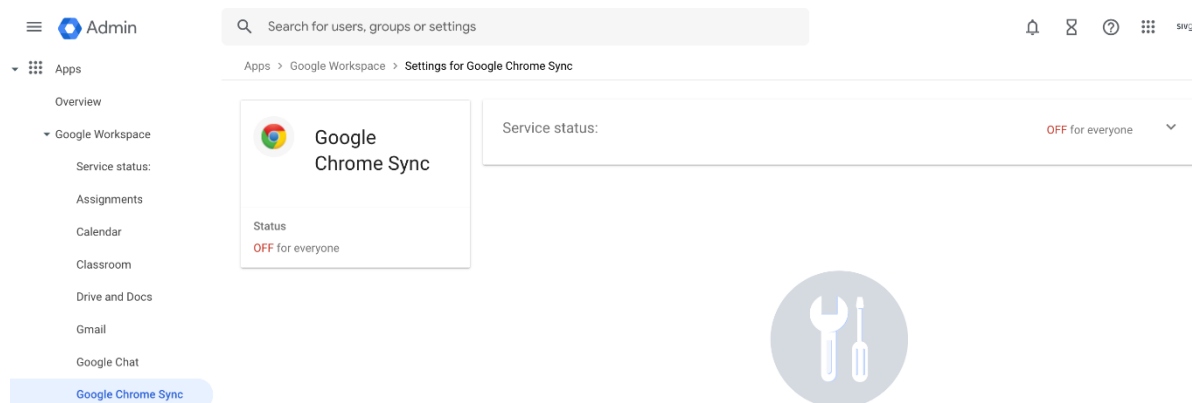
Zet ad personalisatie uit. Voor K-12 is dit de default waarde

K-12 instellingen moet voor alle po- en vo-scholen gelden. Voor niet K-12 scholen volg de instructie zoals hier beschreven <https://support.google.com/a/answer/6304811?hl=en>

Zet Chrome Sync uit

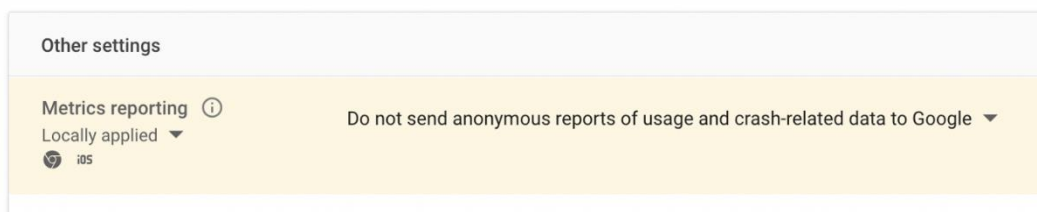
Met Chrome Sync kan gevoelige data verwerkt worden. Er zijn drie opties om de privacyrisico's te mitigeren:

- 1) Zet Chrome Sync uit
- 2) Gebruikt Chrome Sync encryptie (gebruiker moet dit zelf instellen)
- 3) Wacht op de release van client side encryptie van Chrome Sync



Verstuur geen "crash report" naar Google

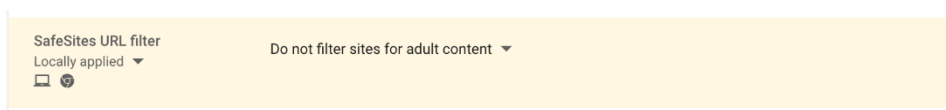
Onder devices -> chrome -> settings -> users and browser gebruik de instelling "stuur geen crash reports" naar Google.



Overweeg "Safe Sites" uit te zetten en een andere filter functie te implementeren

Safe Sites is een essential service en valt daarmee onder de verwerkersovereenkomst. Volgens Google wordt er geen data opgeslagen als url gecontroleerd worden door Safe sites. "Google stated it did not collect any personal identifiers with the URLs and did not store the URLs." We hebben dit niet kunnen verifiëren. Hier zit een mogelijk risico.

Onder devices -> chrome -> settings -> users and browser kan je de SafeSites URL filter uitzetten. Implementeer dan een andere filterfunctie om toegang tot adult content te blokkeren.



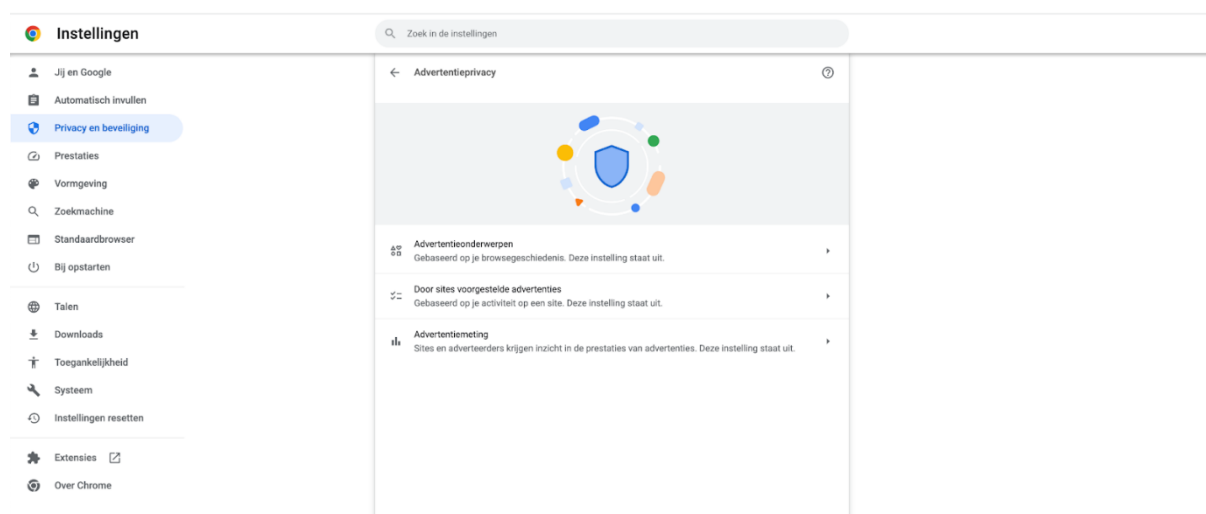
5 Eindgebruikers instellingen

Dit zijn instellingen die de eindgebruikers zelf moet doorvoeren.

Switch off Privacy Sandbox.

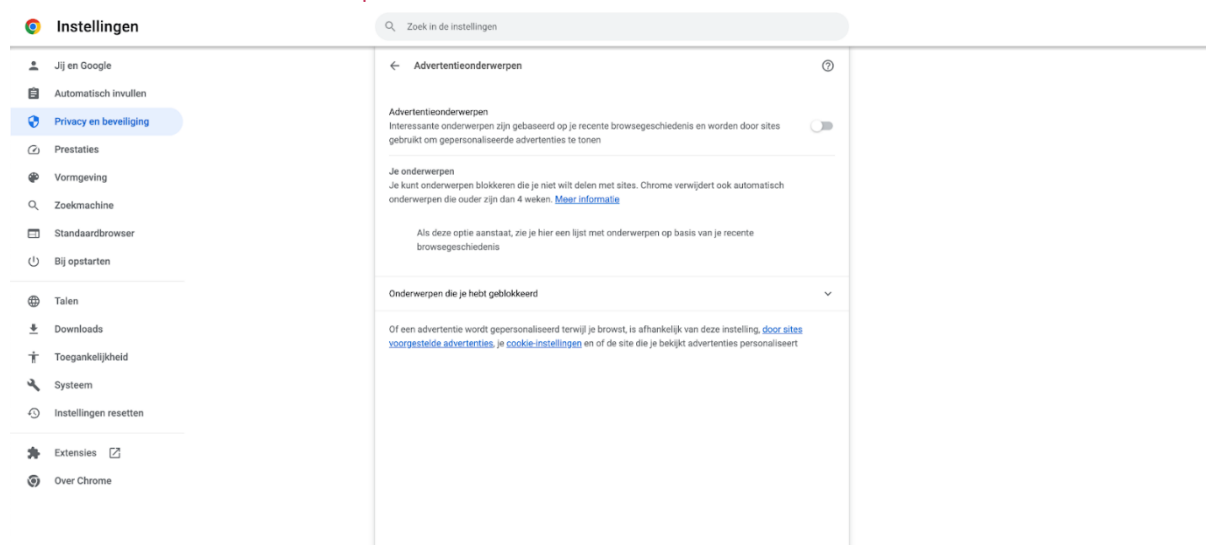
Privacy Sandbox is een nieuwe ontwikkeling voor het presenteren van persoonlijke advertenties zonder het plaatsen van 3rd party cookies. Google zal geen trials doen met de Privacy Sandbox voor gebruikers die van onder de K-12 instellingen vallen. Voor gebruikers die in Workspace gemarkeerd zijn als ouder dan 18 kan de Privacy Sandbox lokaal uitgezet worden zoals hieronder beschreven.

Ga in de browser naar instellingen -> Privacy en beveiliging -> Advertentieprivacy (voorheen Privacy sandbox).



Elke functie kan afzonderlijk aan en uitgezet worden.

Zet advertentieonderwerpen uit





Zet door sites voorgestelde advertenties uit

The screenshot shows the Chrome settings page with 'Instellingen' selected. The left sidebar lists various settings categories, with 'Privacy en beveiliging' highlighted. The main content area is titled 'Door sites voorgestelde advertenties' and features a toggle switch that is turned off. Below the toggle, there is a section for 'Sites die je hebt geblokkeerd' with a dropdown arrow. The text explains that sites visited for more than 4 weeks are automatically blocked and that users can manage this list.

Zet advertentiemeting uit

The screenshot shows the Chrome settings page with 'Instellingen' selected. The left sidebar lists various settings categories, with 'Privacy en beveiliging' highlighted. The main content area is titled 'Advertentiemeting' and features a toggle switch that is turned off. Below the toggle, there are two columns of information: 'Als dit aanstaat' and 'Overwegingen'. The 'Als dit aanstaat' section explains that limited data is shared to improve ad performance and that ad metrics are removed from the device. The 'Overwegingen' section explains that Chrome limits the amount of data shared with sites and that Android devices can have comparable settings for privacy.

Privacy Sandbox



Proeven

Met een Privacy Sandbox-proef kunnen sites dezelfde browsefunctionaliteit leveren terwijl er minder van je gegevens worden gebruikt. Dit betekent meer privacy voor jou en minder tracking op meerdere sites. Als andere proeven klaar zijn om te worden getest, voegen we deze toe. [Over browsergebaseerde advertentiepersonalisatie](#)

Browsergebaseerde advertentiepersonalisatie
Je browsegeschiedenis heeft invloed op de advertenties die je ziet

Advertentiemeting
Adverteerders kunnen inzicht krijgen in hoe advertenties presteren

Spam- en fraudebeperking
Help sites fraude te bestrijden en bots te onderscheiden van mensen

Gebruik Chrome Sync encryptie

Instellingen Zoek in de instellingen

Jij en Google

- Automatisch invullen
- Privacy en beveiliging
- Prestaties
- Vormgeving
- Zoekmachine
- Standaardbrowser
- Bij opstarten
- Talen
- Downloads
- Toegankelijkheid
- Systeem
- Instellingen resetten

Synchronisatie en Google-services

Synchroniseren met [Uitzetten](#)

Synchronisatie

Beheren wat je synchroniseert

Beheren hoe je browsegeschiedenis wordt gebruikt om Google Zoeken en meer te personaliseren

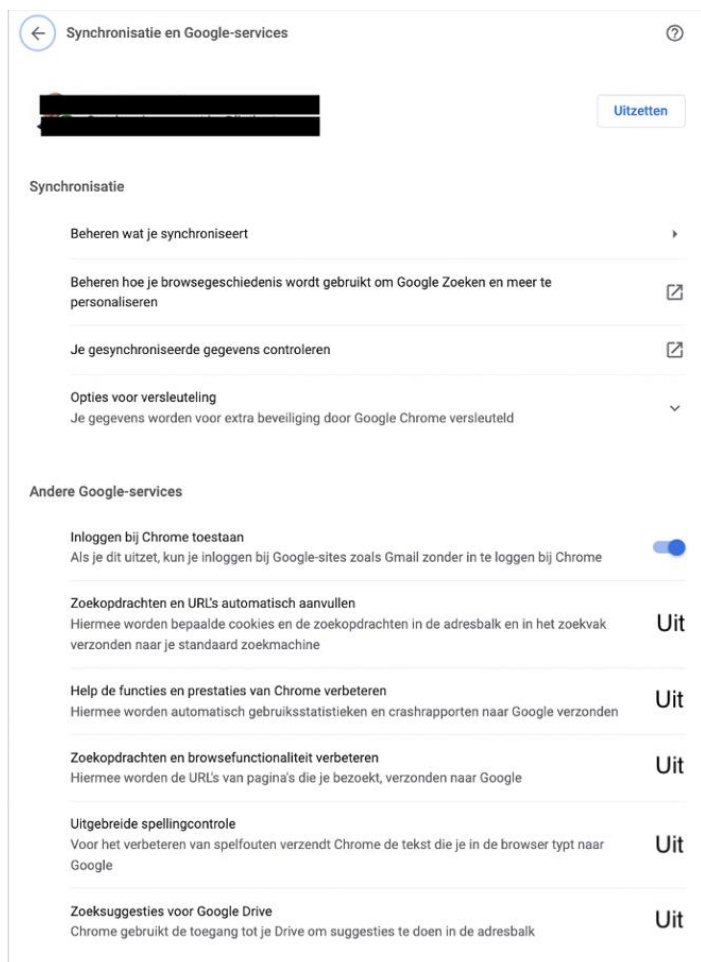
Je gesynchroniseerde gegevens controleren

Opties voor versleuteling
Je gegevens worden voor extra beveiliging door Google Chrome versleuteld

- Gesynchroniseerde wachtwoorden versleutelen met je Google-account
- Gesynchroniseerde gegevens versleutelen met je eigen [wachtwoordzin voor synchronisatie](#). Hieronder vallen geen betaalmethoden en adressen van Google Pay.

6 Gebruik privacy vriendelijke browsers settings

Verder adviseren we de volgende privacyvriendelijke browser settings te gebruiken.



'Niet bijhouden' uitschakelen (do not track) en website preloading disables

Wanneer je op internet browsst op computers of Android-apparaten, kun je een verzoek naar websites verzenden om jouw browsegegevens niet te verzamelen of bij te houden. De functie is standaard uitgeschakeld.

- 1) Open Chrome op je computer.
- 2) Klik rechtsboven op Meer  > **Instellingen**.
- 3) Klik op **Privacy en beveiliging** > **Cookies en andere sitegegevens**.
- 4) Zet **Een verzoek voor niet bijhouden met je browseverkeer verzenden** aan of uit.



Instellingen

Zoek in de instellingen

- Jij en Google
- Automatisch invullen
- Privacy en beveiliging**
- Prestaties
- Vormgeving
- Zoekmachine
- Standaardbrowser
- Bij opstarten
- Talen
- Downloads
- Toegankelijkheid
- Systeem
- Instellingen resetten

Alle cookies toestaan

Cookies van derden blokkeren in incognitomodus

Cookies van derden blokkeren

- Sites mogen cookies gebruiken om de browsefunctionaliteit te verbeteren, bijvoorbeeld door je ingelogd te houden of door artikelen in je winkelwagen te onthouden
- Sites kunnen je cookies niet gebruiken om je browse-activiteit op verschillende sites te bekijken, bijvoorbeeld om advertenties te personaliseren. Functies op bepaalde sites werken misschien niet.

Alle cookies blokkeren (niet aanbevolen)

Cookies en sitegegevens wissen als je alle vensters sluit
Als de schakelaar aanstaat, word je ook uitgelogd van Chrome

Een verzoek voor 'Do Not Track' met je browseverkeer verzenden

Pagina's vooraf laden voor sneller browsen en zoeken
Hiermee worden de pagina's die je volgens Chrome misschien wilt bezoeken, vooraf geladen. Chrome kan hiervoor gebruikmaken van cookies, als je cookies toestaat, en de pagina's versleutelen en versturen via Google, zodat je identiteit verborgen blijft voor sites.



Colofon

Handleiding Google ChromeOS en Chromebrowser

Datum van uitgave

3 juli 2023 (versie 1.0)

27 februari 2024 (versie 2.0)

Auteurs

Versie 1.0: Hans-Peter Ligthart (SIVON), Job Vos (SIVON)

Versie 2.0: Hans-Peter Ligthart (SIVON)

Sommige rechten voorbehouden

Hoewel aan de totstandkoming van deze uitgave de uiterste zorg is besteed, aanvaarden de auteur(s), redacteur(s) en uitgever van SIVON geen aansprakelijkheid voor eventuele fouten of onvolkomenheden. Deze handleiding helpt schoolbesturen als verwerkingsverantwoordelijke de nodige Privacy instellingen door te voeren in Google Chrome. Consulteer bij twijfel een in privacy gespecialiseerde specialist, jurist of advocaat voor advies over de toepassing in uw eigen organisatie.

Deze publicatie is tot stand gekomen in samenwerking met SURF.

SIVON helpt scholen bij het realiseren en doorontwikkelen van veilig en toekomstbestendig digitaal onderwijs, nu en in de toekomst; zij adviseert, ontzorgt en behartigt de belangen van scholen, zodat die zich kunnen richten op hun primaire taak: het verzorgen van het allerbeste onderwijs.

Licentie en auteursrechten

Creative Commons Naamsvermelding – NietCommercieel – Gelijk Delen 4.0 Internationaal (CC BY-NC-SA 4.0)



sivon.nl