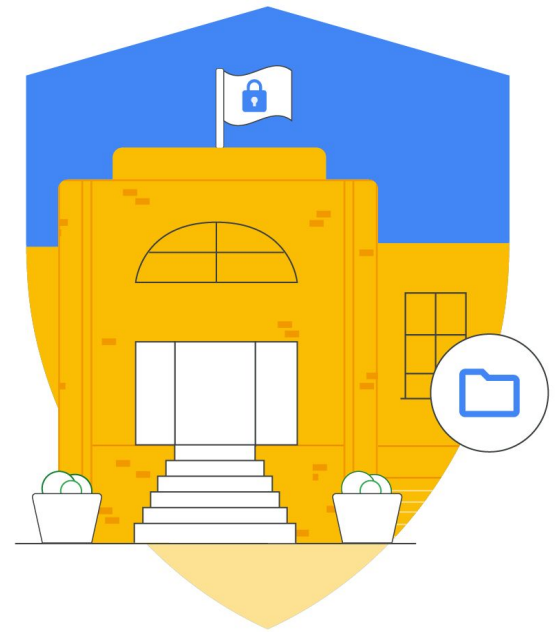


Säkrare undervisning med Google for Education

Låt eleverna lära sig i en säkrare digital miljö, fri från annonser, spam och cyberhot. Erbjud den säkerhet på företagsnivå som skyddar datan hos flera miljarder Google-användare – samtidigt som du slipper krånglig administration.

Google Workspace for Education och Chromebook är säkra som standard, privata genom design och låter skolorna bestämma.



Hur skyddas skolors data av Google for Education?

Använder Google data från skolor?

Alla Googles produkter är säkra som standard och skyddas kontinuerligt av heltäckande processer som automatiskt upptäcker och förhindrar hot på internet. Verktyg som liknar de som [blockerar 99,9 % av all skräppost i Gmail – över 100 miljoner e-postmeddelanden varje dag](#) – skyddar känsliga uppgifter och gör det enklare att efterleva viktiga internationella säkerhets- och integritetsstandarder.

Google krypterar data och skyddar den med flera säkerhetslager. Googles [datacenter](#) använder maskinvara som har utformats av Google och system som har optimerats för säkerhet och prestanda. Resultatet? Data skyddas vid varje punkt, vilket gör det möjligt att identifiera, bemöta och åtgärda hot. Faktum är att Google Workspace är [världens säkraste](#) molnbaserade kommunikations- och samarbetsvit, och inga [attacker med utpressningsvirus](#) har någonsin rapporterats på en företags-, utbildnings- eller konsumentenhet med ChromeOS.

Skolor äger sin data

Skolan behåller fullständiga rättigheter till den immateriella egendom användarna skapar i Google Workspace for Education och kan ställa in regler och behörigheter för hur och när någon i skolan kan komma åt och hämta data och dokument. Google äger, använder eller säljer inte kunddata som lagras i [Google Workspace for Educations tjänster](#). Vi skyddar denna data med strikta säkerhetsprotokoll, ger fullständig insyn och tillhandahåller omfattande integritetspolicyer med strikta säkerhetsprotokoll.

Insyn som skolor kan lita på

Google strävar efter att erbjuda insyn gällande policyer och metoder för datainsamling. I [integritetsmeddelandet för Google Workspace for Education](#) och [användarvillkoren för Google Workspace](#) finns information om hur vi strävar efter att skydda data.

Inga annonser i Google Workspace for Educations tjänster

Vi använder eller säljer inte kunddata från Google Workspace for Education till tredje part, och vi delar inte data som lagras i våra system med tredje part, såvida detta inte uttryckligen begärs av datans ägare i enlighet med de omständigheter som anges i [integritetsmeddelandet för Google Workspace for Education](#) eller om så krävs enligt lag.

Kan jag använda Google Workspace for Education i enlighet med juridiska standarder?

Google stödjer efterlevnad av strikta säkerhets- och integritetsstandarder, bland annat FERPA, COPPA och GDPR, och har granskats av oberoende [tredjepartsorganisationer](#). Det finns en fullständig lista över globala efterlevnadsstandarder i [centret för molnefterlevnad och föreskriftsresurser](#).

Kan administratörer hantera och skydda skolans domäner?

Vi erbjuder verktyg som gör det enklare att övervaka och hantera datasäkerhet och som ger bättre kontroll och synlighet. Det underlättar för administratörer som behöver underhålla domäner. Inbyggda automatiserade skydd erbjuder övervakning, datakryptering, förebyggande av dataförlust, identitets- och åtkomsthantering och mycket annat, dygnet runt.

Administratörer hittar centraliserade inställningar i [Administratörskonsolen](#) och kan hantera integritet, säkerhet, data och enheter. Därifrån erbjuder [säkerhetscentret](#) automatiska varningar och hanteringsverktyg som förhindrar, upptäcker och åtgärdar säkerhetshot. Det gör det möjligt för administratörer att agera så fort en incident upptäcks.

[Med Chrome Education Upgrade](#) centraliseras hanteringen av Chromebook-enheter och användarna får tillgång till alla funktioner i ChromeOS, inklusive åtkomstkontroller och avancerad integrerad säkerhet för Chrome-enheter.

Hur skyddas yngre elever av Googles produkter?

Elever som uppges vara under 18 år skyddas av inbyggda standardinställningar. Administratörer kan ställa in åtkomst till vissa tjänster utifrån användarnas ålder, på distrikt-, skol-, klass- och individnivå. Skolor kan till exempel begränsa YouTube-innehåll och aktivera [SafeSearch](#) och Safe Sites för att filtrera bort olämpliga resultat och förhindra att elever besöker osäkra webbplatser.

Digitala säkerhetsstandarder gäller även EdTech-appar och -tillägg från tredje part som förekommer i Google for Educations App Hub. I Google for Education finns kontrollmärken, applicensiering och innehållsmedvetna åtkomstregler. De här verktygen ger skalbar kontroll och översikt åt administratörer med uppåtkomst.

Hur kan föräldrar och vårdnadshavare hjälpa sina barn att använda internet på ett säkrare sätt?

Integritet och säkerhet i företagsklass är inbyggt i själva grunden till Google for Education. Vi ger dessutom vårdnadshavare och familjer tillgång till flera olika resurser som gör det enkelt att förstå och skydda barnens digitala undervisningsmiljö, till exempel:

- [Vårdnadshavarens guide till integritet och säkerhet](#): En översikt över hur verktyg i Google for Education interagerar i syfte att tillhandahålla säkrare undervisning
- [Familjeguiden Be Internet Awesome](#): Innehåller resurser om säkerhet på internet och digitalt medborgarskap i hemmet
- [Teknikverktyg för familjer och vårdnadshavare](#): En kort video om hur Google for Education tillhandahåller säkerhet med hjälp av inbyggda skydd
- [Familjeguide till digitalt välmående](#): Samtalspunkter om tuffa teknikfrågor och hur man navigerar den digitala världen som familj
- [Family Link](#): En app som gör det möjligt för vårdnadshavare att ange skärmtid, hitta bra innehåll och skapa hälsosamma digitala vanor
- [Säkerhetscenter för föräldrar](#): Råd från experter och pedagoger om hur man hanterar teknik i familjen
- [Families.google](#): Resurssamling om hur du uppföstrar digitalt ansvarsfulla barn

