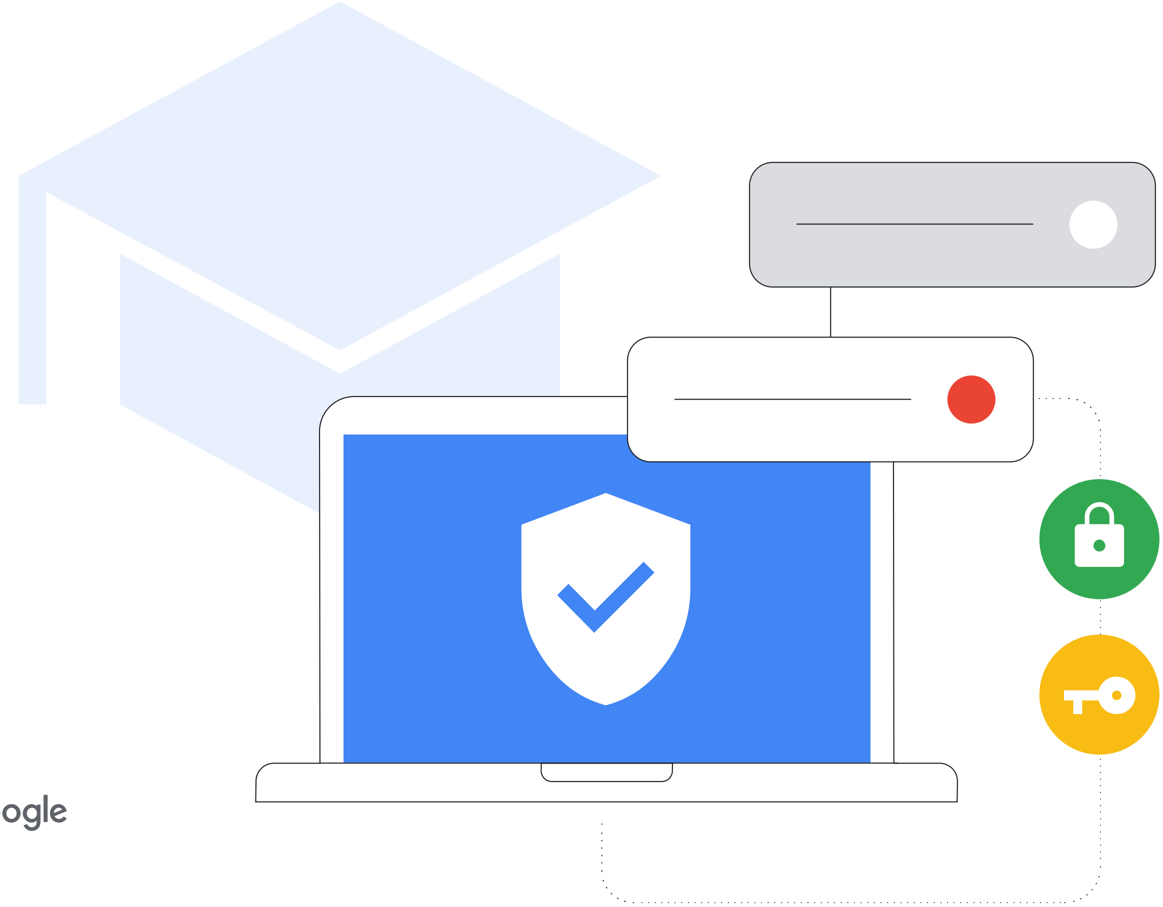
Google for Education

K-12 Cybersecurity Guidebook

Updated August 2023



Safer with Google

Executive summary

As CISA's Protecting Our Future report highlights, it is critical for K-12 institutions to invest in cybersecurity in order to protect their students, their families, teachers, staff, and communities. This document provides guidance and best practices for school IT administrators on setting up and configuring hardware and software in K-12 institutions to strengthen cybersecurity. It includes both general best practices, as well as specific guidance for Google products and services. Google's mission to organize the world's information and make it universally accessible and useful is a critical driver of the work we do on the Google for Education team: building tools designed for teaching and learning. We'll share lessons from that work in this guide.

We provide security best practices by topic that give a more in-depth look into configuration, set-up, and risk mitigation strategies. We also explain how Google approaches cybersecurity for our services, especially our tools for education. While we provide detailed guidance in this document agnostic of product or service, we believe our products offer superior protection against common attacks out-of-the-box.

The risk

Educational institutions are top targets for cyber attacks, with bad actors looking to exploit schools' data-rich environments for their own profit. 46% of schools who have yet to be targeted believe they'll eventually be hit because ransomware attacks are getting more sophisticated — and harder to stop. And 42% of these schools think ransomware is so prevalent that an attack is just *inevitable*. The need for schools to rapidly transition to distance learning in 2020 was a strong contributor to cybersecurity gaps, leaving schools vulnerable to attacks.

The defense

These attacks can be mitigated. And while no technology completely eliminates your risk, the education sector and edtech vendors can work together to adopt and implement best practices to create a safe, secure and comprehensive approach to significantly reduce your risk. With the right precautions and policies in place to protect users, secure devices, and ensure data privacy, educational institutions can better manage risk and mitigate attacks.

Key recommendations

- **Use secure authentication** to keep sensitive information safe, protect emails, files, and other content, and prevent unauthorized users from accessing education systems. Use best practices for user authentication, including strong passwords and two-step verification (2SV), passkeys, and password managers where possible, especially for IT administrators and staff who work with sensitive information.
- **Apply appropriate security settings** to keep your users, data, and environment safe. While Google products are built secure by default, it is critical that admins also properly utilize and configure networks and systems to ensure security. To keep schools secure, apply the principles of zero trust and least privilege: users should only have access to the software, data, applications, and systems that they need to do their work effectively.
- **Update and upgrade your systems** to ensure that users are protected from the latest threats. Use modern operating systems (OS) and browsers and ensure that users are running the latest software versions on all devices (or approved long-term stable versions) and that they update automatically. Upgrading to a more secure solution, such as Chromebooks, can increase security. No ransomware has ever been detected on any ChromeOS device, ever.
- **Use real-time alerting and monitoring systems** to increase your security posture and mitigate potential issues quickly. You can use these features built into your primary collaboration and communication software, such as Google Workspace for Education, or deploy separate security logging and monitoring solutions. Ensure comprehensive tracking of activities across your school's network, devices, applications, users, and data. Monitor account logins, file sharing, email volume (especially phishing and malware attempts), device activity, and configuration changes. Keep your alerting and monitoring solution current to receive notifications about threats, critical events, and system changes.
- **Train teachers, staff, and students** on how to use devices and software safely, recognize and report potential threats, and share data appropriately to help protect against some of the most common attacks. Schools or districts can create branded training materials alongside using freely available ready-made materials, resulting in a comprehensive toolkit for schools.

Recommendations specific to users of Google products
Google's products, like Google Workspace for Education and Chromebooks, can enhance your school's cybersecurity and make each of these recommendations easy to implement. Together, they provide a comprehensive solution that helps protect user privacy and provides best-in-class security for your institution.

These strategies, along with the additional guidance provided in the following paper, form an excellent foundation for K-12 institutions' security.

Google's approach for education

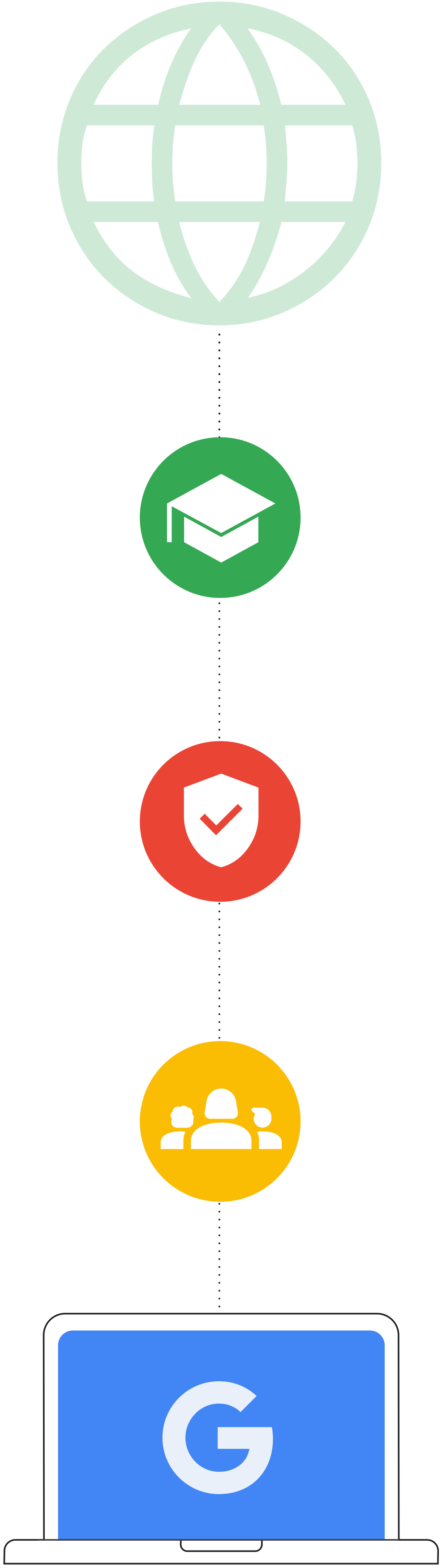
Google's mission is to organize the world's information and make it universally accessible and useful, and that's no less true in the education sector. On the Google for Education team, we do this by building tools like Chromebooks and Google Classroom that make it simple and safe for students and teachers to create, share, and organize their own content and to access and use educational resources and online tools.

Schools deserve technologies which are secure by default, private by design, keep you in control, and have trustworthy content and information. With products like Chromebooks and Google Workspace for Education, schools get best-in-class security that's compliant with the highest global educational standards, IT admins get full visibility and painless control of their data and security policies, and students can fully immerse themselves in learning within a safer digital environment that serves age-based content and mitigates spam and cyberthreats.

We have prioritized built-in security features and controls, the highest levels of privacy standards, and options for more proactive security tools to ensure secure learning for everyone. ChromeOS devices help to mitigate threats facing schools, and are the best defense against the number one threat to schools - ransomware - having never had a successful ransomware attack against Chromebooks.

Meanwhile, Google Workspace for Education is one of the world's most popular and secure cloud-based communication and collaborations suite. For more information about how each protects cybersecurity in connection to the recommendations here, please see the last section.

This paper is broken up into two sections - the first section on practical and general security guidance for K-12 institutions regardless of products, and the second section on specific configuration guidance for institutions using Google for Education products such as Google Workspace for Education and Chromebooks. Both sections provide information to help keep you and your students safe online.



Introduction

K-12 institutions - both their devices and networks - are at high risk of cyber attack. It is crucial that K-12 institutions employ the best security possible to protect students and prevent the loss of data, services, resources, time, and money that can result from these attacks. (Source: https://www.gao.gov/products/gao-20-644)

This guide is a tool to promote cybersecurity best practices for school administrators and school systems to implement in order to better secure their environments. By implementing these best practices, K-12 institutions can mitigate or prevent serious and costly cyber attacks on educational systems and protect students, families, teachers, and staff.

Cyber attacks targeting schools are increasing in frequency and severity. According to the K-12 Cybersecurity Resource Center, there were over 1,300 publicly disclosed cyber incidents involving education organizations across all 50 states between 2016 and 2021. Today's education leaders must protect the data and personal information of students, teachers, and staff, as well as their institution's systems and information. It's a tall task, especially considering education has traditionally had a harder time keeping pace with cybersecurity compared to other sectors.

Successful cyber attacks, including ransomware, phishing, malware and more, can lead to large-scale data breaches of personally identifiable information (PII), costly payouts (the average ransom payout increased 5x since 2020 to $812,260), and cause lengthy disruptions to instruction and other school operations. Recently, a successful ransomware attack shut down an entire school system, causing ripple effects across the entire community as students were unable to attend school for days on end. With limited resources and funding, K-12 organizations will continue to find themselves a prime target of opportunity unless an investment in increased cybersecurity is made.

Cybersecurity is always best served by communication, collaboration, and partnership. This document has been compiled from Google's safety and security tips, the National Institute for Standards and Technology (NIST)'s Cybersecurity Framework, and the 2023 CISA K-12 Cybersecurity Toolkit and Recommendations - widely accepted sources of cybersecurity practices. This document discusses general steps that IT administrators should take or consider, some of Google's own best practices and guidance for our products, and also references security tips and services offered by other companies. Administrators should review all security guidance provided by the relevant companies and implement their latest guidance, since the responsible company is best able to describe their own products and any changes that may have occurred.

Before taking action on recommendations listed below, you should also consider the following factors:

Considerations

1. **Protecting your student population.**
   Each school's needs vary, and certain populations may require additional steps to protect security and privacy. Many edtech tools have features to help with age based access, such as limiting inappropriate content or making sure their location and contact data is private.

2. **The types of data that you store.**
   If you store sensitive data, you may want to encrypt the data or store it in a separate location.

3. **What types of devices you use and your deployment model.**
   Devices and their applications should get automatic updates to maximize security, encrypt data, and isolate accounts to ensure that users only have access to their own information.

4. **Your school, district, or regional policies.**
   Your school may have specific policies in place regarding the use of technology. You will need to ensure that all safeguards are set up in accordance with these policies.

Every day

100 million

phishing attempts are blocked by Gmail.

Every week

300,000

unsafe websites are identified by Google.

Every day

74 million

users get help from Google's Password Manager.

Every year

700 million

people strengthen their security with Security Checkup.

Use secure authentication

Secure authentication must be a top priority for schools and other institutions. In the fourth quarter of 2022, weak or non-credentialed accounts accounted for 48% of all compromise factors in breaches. Implementing some key recommendations can help verify that users are who they say they are and limit access to information appropriate to each user's role.

IT administrators should enforce the use of two-step verification (2SV, also known as two-factor or multi-factor authentication), and move to passwordless authentication (i.e., passkeys) whenever possible, and especially whenever someone is remotely accessing the educational institution's systems. 2SV adds an extra layer of security to your online accounts, making it much harder for attackers to gain access.

2SV is core to Google's own security practices and we continue to work to develop more secure authentication methods.

There are many device types and deployment models used by schools today and there is a varied technical aptitude in a K-12 environment. Account and device security varies across user roles and types with defined best practices: IT administrators, teachers and staff, older students using assigned devices, and younger students using shared devices. We discuss specific recommendations for each group below.

There are several kinds of authentication methods that are best practice in most settings

- **Strong passwords**
  Prompt users to create their own password on first sign-in and require length and complexity minimums. Longer passphrases provide an extra element of security due to length and complex character usage. Users should not be required to regularly change passwords since that encourages users to use simpler passwords or make immaterial changes (like updating a single character).
- **Two-step verification**
  2SV protects accounts with a second step - often something that a user has with them, such as a security key or app on a mobile phone that creates a one-time verification code. Although any form of 2SV adds account security, administrators should avoid the use of verification codes sent by texts or calls which can be vulnerable to phone number-based attacks.
- **Passwordless authentication**
  Passkeys are a safer and easier alternative to passwords. Users can sign in to apps and websites with a PIN, pattern, biometric sensor (such as a fingerprint or facial recognition), or security key tap, freeing them from having to remember and manage passwords. While these may not be appropriate for every educational context, they are increasingly replacing traditional forms of authentication and make for safer, faster sign-ins. Passkeys protect users from phishing attacks since they work only on their registered websites and apps.
- **Single sign-On (SSO)**
  SSO allows users to access multiple applications and websites with a single set of credentials. When users only have to remember one set of credentials, they are less likely to write them down. Additionally, when schools don't have to manage multiple sets of user credentials, they can save money on IT support and help desk costs. Google Workspace for Education supports SSO natively so users can use their Google account credentials to login into 3rd party applications, or they use another provider's credentials to log into their Google accounts.
- **Password managers**
  Password managers can help users create strong, unique passwords across accounts and services that they use during their school and work days (when not using SSO). These don't assist in logging into a device's operating system, but they can manage passwords once the user has logged on. Google users can use Password Manager across Chrome on any platform, ChromeOS, and Android.

The unique needs of various groups will benefit from specialized subsets or combinations of these authentication approaches, according to their role within an educational institution, the kind of systems and data they have access to, and their age.

School administrators

Administrators control the systems and much of the data for any K-12 institution. The protection of their accounts is key to the security of the entire system: from infrastructure to account data to devices administered by the institution. As such, they should adopt the gold standard among authentication, including using strong passwords, a robust password manager, and 2SV. Each of these provides a layer of protection that, when used together, provides the strongest security for the Administrator account and enterprise services.

- Administrators should use a physical security key or a cryptographically secure 2SV method that requires a trusted device and prompts. This can include a service such as Google Authenticator or another app that creates one-time verification codes.
- Administrators should use a trusted password manager that supports 2SV to store their passwords for different services.

Older students using assigned devices

(typically grades 4+)

Older students are better educated in how to protect themselves and are usually capable of using more protective authentication mechanisms, which is appropriate to the types of services they are likely to be using. They should only have access to their own account and information that has been shared with them.

- Students on Chromebooks should be given the option to create a device-specific PIN to expedite sign-in on that device. Biometric options may not be appropriate or feasible in many school environments.
- Every student should be supported in creating a unique password that does not include personal information (e.g. name, homeroom, or birthday). Students should be taught how the use of passphrases can provide complexity while making the password easy to remember.

Teachers and staff using assigned devices

Like administrators, teachers and staff have access to sensitive data, but they don't control the digital infrastructure and have more varied technical aptitude.

- Teachers and staff on Chromebooks should be given the option to sign in with biometric verification where legally allowed, like fingerprint.
- Administrators should enforce the use of 2SV and move to passwordless authentication whenever possible and whenever a member of staff is remotely accessing the educational institution's systems.

Young students using shared devices

(typically grades K-3)

The youngest students are still learning how to use educational technology, and will benefit from simple authentication - which is appropriate for use with limited services and data.

- Schools that use third-party password-alternatives like QR codes or picture logins for their youngest students and those unable to login with passwords should put precautions in place for security, since they are less secure. Administrators should modify a student's password and update the code whenever a code has been lost or exposed to others.
- Schools should educate both students and parents on the importance of keeping passwords secret and securely storing alternative credentials like QR codes.
- For assigned devices like tablets, a device-specific PIN can be used as an alternative secure authentication method.

Apply appropriate security settings

School devices and networks are a high-visibility, high-value target for attackers around the world, so it's critical to employ the best security possible to prevent the loss of services, resources, time, and money. System administrators should implement effective and appropriate security features available in the products their institutions use, but they also need to make sure that these systems remain easy to use for teachers, staff, and students. Important security and privacy settings should be configured such that individual users cannot disable or modify them, and other settings should have protective defaults set by the administrator. It's critical to employ the best security possible to prevent the loss of services, resources, time, and money.

If you are using Chromebooks, you can see our suggestions for setting device policies in the last section.

Finally, build "data minimization" into your practices by limiting the purposes and means of collection, use, and disclosure of individuals' personal information to what is reasonably necessary and proportionate to provide the service or is otherwise consistent with the context of the relationship.

Applications & updates

Limit and minimize the apps your users are able to install as each application installed on a device is a potential attack vector to exploit. If possible, use applications from trusted sources. For example, recommend users check for the verification badge on the Google Play Store to ensure users are downloading the official applications that have gone through a security review. Any OS or hardware modifications (jailbreaking or rooting) introduce significant security flaws and should be avoided.

Access & visibility

Administrators should ensure that users only have access to the data, software, services, and systems that they need to perform their duties or learn effectively. This helps to limit unintended access and track who has access to what resources. Give special attention to highly sensitive data, such as user PII, and systems (such as HR, payroll, grading, security, and configuration) by auditing which users can access the data and under what circumstances by limiting access to school-owned devices, and ensuring only specific members of staff have access.

Review your data sharing policies in collaboration tools to prevent inappropriate or over-sharing and unauthorized access. Limit or block sharing outside your environment (especially for students) and enable policies that monitor sharing of sensitive content.

Device loss or theft

Losing a device doesn't need to mean you lose data. Administrators should standardize a plan to ensure access to information and documents in the case of loss or theft of a device, such as maintaining documents in a cloud environment. Download and print backup codes for your 2SV processes to prevent account access interruption.

When a device is reported lost or stolen, ensure that the device is remotely locked down if possible, and that associated accounts are locked down or flagged to ensure they are not used to gain unauthorized access. Chromebooks can be remotely wiped if they are lost, and Google Workspace for Education accounts can be monitored for suspicious activity or suspended (locked) if needed.

Advanced protection for high risk users

For users with high visibility and sensitive information (including Google Workspace for Education administrators), Google provides the Advanced Protection Program (APP). APP gives users additional protection against targeted attacks, such as phishing attempts, harmful downloads, and password breaches. APP is specifically designed to thwart targeted online attacks on Google Accounts, and automatically uses strong authentication, security keys, and restricts third party access to account data. Other online account providers also provide strong account protections for high risk users, and administrators and staff should always use them if they have access to personal information or technology systems.

Update and upgrade your systems

One of the most important things that anyone can do to protect themselves is to keep their device operating system and applications updated. This is even more important for K-12 institutions, since they are such an important part of a child's education and day to day life. Most malware attacks in both educational contexts and in other high-risk contexts have been Windows-based, including SolarWinds, the Los Angeles Unified School District ransomware attack, Little Rock School District hack, the Microsoft Exchange Server data breach, the Albuquerque School District ransomware attack, and the recent Microsoft federal agency breach. This is another place where using cloud products and services should make an administrator's task easier by reducing their attack surface and ensuring that their systems and applications stay up to date - automatically.

Upgrade to a modern operating system and keep it up to date

The most recent version of any operating system (OS) usually contains new security features to help prevent against known attack vectors. You should enable automatic update functionality inside the device OS, or if automatic updates are impossible, download and install patches and updates from a trusted vendor at least monthly.

Chromebooks run on ChromeOS, so they have frequent, automatic updates with the latest security patches to enable rapid adoption of the latest security innovations and they verify the integrity of the read-only operating system before booting. They also encrypt all data stored on the device, protecting it from unauthorized access and running every web page and application in a separate sandbox, so if one website or app is infected with malware, it can't spread to other parts of the device.

If your school isn't ready to move to Chromebooks, ChromeOS Flex is a version of ChromeOS that is made to modernize your school's devices. ChromeOS Flex provides everyone with a unified, modern teaching and learning experience that has proactive, built-in security and cloud-based management capabilities. Flex can provide automated protection and block malicious executables and apps without replacing your existing hardware.

Upgrade to a modern browser and keep it up to date

It's important to ensure that the browser is also updated and secure. Modern browsers offer more advanced security features and can prompt users to enable them easily or be configured by administrators to turn these features on by default on institutional computers - allowing them to help protect the confidentiality of sensitive information in transit over the Internet. The browser should be kept up to date. Whether working, learning, or other online activity, an updated, modern browser will:

- **Use robust security**, including site isolation and safe browsing protection to prevent users from accidentally going to dangerous websites
- **Enable automatic updates** to ensure that your browser gets security updates quickly
- **Ensure that the connection is secure** Modern browsers should use transport layer security, and users can click next to the URL and check that the connection is marked secure

Chrome has been built with security in mind, with security features like safe browsing turned on by default. And there's an integrated password manager that can autofill passwords as you browse the web, letting you use strong passwords easily.

Use real-time alerting and monitoring systems

Real-time alerting and monitoring systems can help schools identify and respond to threats quickly, before they cause damage. It is important to ensure that security tools are running in the background, collecting and logging security events from across your systems. AI tools are particularly good at sifting through the large amounts of collected data and finding anomalies and patterns, which could be used to more quickly and easily detect threats and to process and address vulnerabilities. This allows for prioritization of which activities need to be reviewed by the IT administrator or staff.

Schools can use alerting and monitoring features built into their primary collaboration and communication software, such as Google Workspace for Education, or deploy separate Security Information and Event Monitoring (SIEM) solutions.

Real-time alerting and monitoring systems can track a variety of activities across a school's network, devices, applications, users, and data, such as user logins, access to files, potential intrusions, successful or attempted theft of data and administrator activities.

If the system detects any suspicious activity, it can send an alert to a school's IT staff. This allows admins to investigate the issue and take action to mitigate the threat.

Additionally, alerting and monitoring tools can be used to gain a deeper understanding of the threats that schools face. By analyzing data from these real-time systems, schools can identify trends and patterns that can help them to better protect themselves.

Here are some best practices for using alerting and monitoring (including SIEM) systems

1. **Define your security goals**
   Identify which information and systems are most critical to the school and what types of threats present the greatest risk to them. Then work to identify the data you need to collect to monitor for those threats.

2. **Collect the right data & configure properly**
   It is important to collect the right data and configure applications to address your most relevant security goals. This may include data from firewalls, content filters, intrusion detection systems, web servers, and other security devices, along with communication and collaboration software, School Information Systems and Learning Management Systems.

3. **Investigate and respond to alerts**
   When your monitoring system generates an alert, it's important to investigate the issue and take appropriate action. This may involve bringing multiple teams together to investigate the source of the alert, determining if it's a false positive, or taking steps to mitigate the threat, such as suspending accounts, resetting user passwords, quarantining or deleting emails, changing file permissions, or wiping devices.

Train teachers, staff & students

K-12 institutions should elevate the security awareness and habits of school communities, using campaigns and partnerships to empower their users. Educating teachers, staff, and students about the importance of security is critical to helping them protect themselves online and helps to prevent serious cybersecurity threats. Teach them how to use the products and services in place across the institution, how to spot and report threats like phishing emails, and most importantly how to take action to prevent these attacks.

How to use devices and software safely

Administrators can partner with teachers and experts in developing cybersecurity curricula at age-appropriate levels to help students understand how to use devices, software, and systems safely. Creating school or district-branded training materials helps to contextualize the recommendations for your teachers and students, but you can also take advantage of ready-made material available, such as Be Internet Awesome available on Safety.Google, and the Khan Academy, and tailor it to your needs. These programs can help your users stay safe no matter where they are - in school or within their community.

Recognizing threats

Training teachers, staff, and students to recognize threats is an important part of keeping them safe. Teaching children how to tell whether something is a threat or not is important, since they might not know how to know if something is legitimate. There are a few types of threats that they should recognize and understand how to report, and administrators should focus on those topics that they think will have the most return on investment. Importantly, training should not just teach users to recognize the threat, but to take action. Common threats that users should recognize include ransomware, phishing, social engineering, malware, and scams - but if certain threats are more prevalent within a given institution, it is worth ensuring that the school community is educated about them.

Secure data and file sharing

Teachers and staff should be trained about appropriate sharing of files and data and how to recognize inappropriate requests through email. Critically, they should ensure that sensitive personal information is only shared or processed when necessary and with additional layers of protection for the data, such as never being shared via email or with external parties. They should use data-loss prevention capabilities (included with ChromeOS and Workspace for Education) to warn and prevent end users from sharing files with sensitive data (like social security numbers) or copying and pasting sensitive content outside of the domain.

Google's approach in action: Devices and services for education

Software procurement is one of the most powerful tools a school district has to protect itself. Software should be robustly architected and designed to minimize risk of vulnerabilities, with security built in at every layer. By requiring that schools purchase secure software, or software from companies with a proven security track record, the broader cyber-risk can be significantly reduced. At Google, we've hardened our ChromeOS, for example, while continuing to deploy more proactive, intelligent solutions that leverage the strength of our machine learning, cloud, and identity expertise.

Google is committed to building products that help protect student and teacher privacy and provide best-in-class security for your institution. You can trust that Google for Education products and services continuously protect users, devices, and data from increasingly complex threats. This section walks school IT administrators through security recommendations when using Google for Education products.

Google Workspace for Education

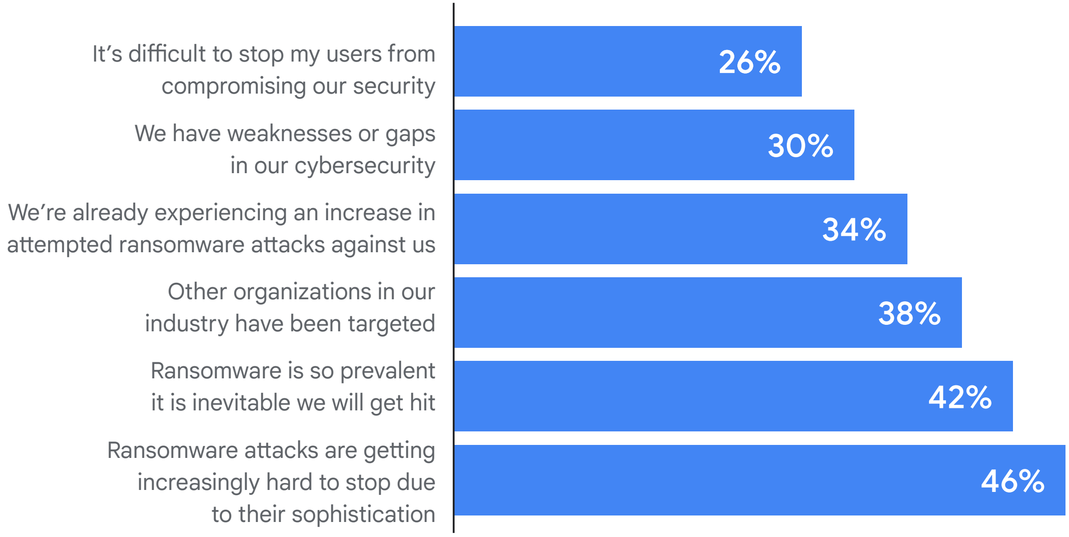
Google Workspace for Education is a set of Google tools and services that are tailored for schools to collaborate, streamline instruction, and keep learning safe. Google for Education products and services continuously protect users, devices, and data from increasingly complex threats, and provide tools such as alert and security centers, a vault for eDiscovery, identity and access management, and data loss prevention.

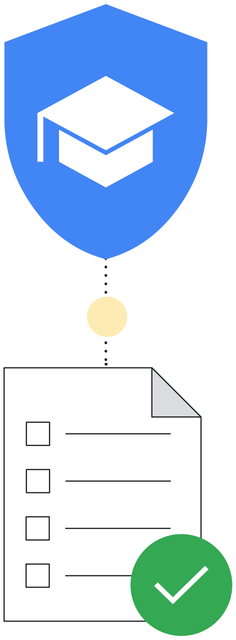
We've put together helpful materials if you're just getting started with Google Workspace for Education, and many of them can help you set things up in line with the recommendations with this guidance. For help getting started with Google Workspace for Education, see the Quickstart IT setup guide.

Security checklists

Review the security checklists, provided in the sources section, to learn more about how to strengthen the security and privacy of your institution. Schools with Google Workspace for Education Standard and Plus editions can also use the Security Health page to monitor the configuration of your Admin console settings. For example, you can check the status of settings like automatic email forwarding, device encryption, Drive sharing settings, and much more. If needed, you can make adjustments to your domain's settings based on general security guidelines and best practices, while balancing these guidelines with your organization's business needs and risk management policy.

Why the education sector expects to be hit





Source: https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6q/sophos-state-of-ransomware-in-education-2021-wp.pdf

Here are some other helpful tips to make sure that you're maximizing the protections built into Google Workspace for Education:

Set up organizational units (OUs)

No one would argue that everyone in your Google Workspace for Education account needs to have the same settings. Organizational units are groups of users that let you give different services, settings, and permissions to different users - for example, using 2SV for teachers and staff, and age-appropriate authentication for young students. Set up separate organizational units for staff, teachers, and students to apply policies to each group of users separately.

A well-designed structure is critical to effectively and flexibly manage your Google Workspace for Education account.

Set up password policies and admin account protections

As we discussed, user authentication is a critical part of keeping your institution safe. That's why we've set up flexible ways to manage authentication for administrators that will allow you to make sure that users have appropriate and secure account protections.

Set password policies to ensure that users create strong passwords, and consider requiring the use of 2SV where appropriate based on the recommended groupings in the Secure Sign-On section. You can enforce the use of 2SV for a subset of users (giving them time to set it up) and deploy 2SV using a variety of methods, including security keys (most secure), a Google prompt (using Google's apps on Android and iOS), verification app generators (like the Google Authenticator), and text messages or phone calls (though these are the least secure method).

If your organization uses an identity provider (IdP) other than Google, you can set up Single Sign On (SSO) via a third party Identity provider. You can still use 2SV with SSO for non-super admin accounts if preferred.

Turn services on or off

Administrators can control which Google services users can access with their Google Workspace for Education account from the Google Admin console. You can control access to Google services such as Calendar, Drive, and Meet, by turning services on or off by organizational unit (OU) (you can also turn services on when using groups). You can also review the differences between Workspace Core and Additional services before enabling additional services like YouTube, Google Maps, and Blogger.

Administrators are encouraged to set access to Google services based on age, and bear in mind that users designated as under the age of 18 automatically have restrictions in some Google services when they're signed in to their Google Workspace for Education account.

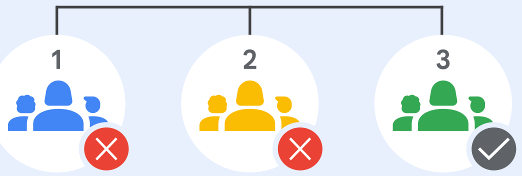
You can also use Context-Aware Access (available in Workspace for Education Standard and Plus) to allow or block access to Google apps such as Gmail, Drive, and Calendar based on a device's IP address, geographic origin, security policies, or OS. For example, you can allow Drive for desktop only on company-owned devices in specific countries/regions.

Methods of giving users access to services

In the Google Admin console, you can turn off an organizational unit's access to a Google service, such as Google Drive. If some users in that organizational unit need to use Drive, you have 2 options:

1. Move the users to an organizational unit that has Drive turned on.
2. Add the users an access group and turn on Drive for the group. Each member can access the service, even if their organizational unit has the service turned off.

Organizational units



Google Drive is turned off for organizational units 1 and 2

With an access group

But a **group of users** within organizational units 1 and 2 can use Google Drive

Source: https://support.google.com/a/answer/9050643?sjid=4805599982673626852-NA

Set data sharing policies and retention rules

As an administrator, you can control if users can share Google Drive files and folders with people outside your organization. This can help prevent unintended or overly broad sharing of data and files, preventing data leakage. Separation of files and drives, creating organizational units, and operating under the principle of least privilege is important to prevent attackers from moving across networks if they infiltrate one account. The less data and network access a potential attacker has access to, the less damage can be done.

Turn off external file sharing for students (or restrict external sharing to allowed domains only) and set "Access checker" to "Recipients only." If you allow some or all users to share files outside your domain, turn on a warning when a user does so. Additionally, disable file publishing on the web, and require external collaborators to sign in with a Google Account.

Additionally, Workspace for Education Standard and Plus customers can use Target Audiences and Trust Rules to set sharing recommendations and restrictions on a more granular level. For example, with Target Audiences, you set the default link sharing audience for teachers to "teachers and staff," rather than everyone at your institution. With Trust Rules, you could block elementary students from sharing files with older students.

- Review shared drive policies to ensure that only appropriate users can create shared drives and prevent external users from accessing shared drives. It's recommended that you allow only admins (or staff and teachers) to create shared drives and that you manage shared drive access closely.
- Consider limiting Directory visibility and contact sharing when possible, either by disabling contact sharing for some or all users, or by creating custom directories to limit which users are visible to whom.
- Set up data loss prevention (DLP) policies in Drive and Gmail to detect and block sensitive information. There are pre-built policies that can be leveraged to protect common sensitive information (such as bank or credit card numbers). You can also create custom policies based on keywords, word lists, and regular expressions (Regex).

Manage Gmail settings

Gmail is one of the core services within Google Workspace for Education, and there are many settings that administrators can take advantage of to protect their institution and their users.

Prevent spam, spoofing, and phishing with Gmail authentication. Customize spam filter settings, including requiring sender authentication for all approved senders and disabling bypassing spam filters for internal senders.

Disable POP/IMAP access when possible and enable enhanced pre-delivery message scanning and advanced phishing and malware protection. If you allow external emails for some or all users, you can enable external recipient warnings.

Google Workspace for Education Standard and Plus customers can also help protect against malware and ransomware by setting up rules to detect harmful attachments using Security Sandbox.

3rd party applications

Use built-in approval workflows to approve 3rd party applications which access account data through APIs. This helps to prevent unauthorized data from being shared with 3rd party applications not approved for school use.

Leverage the security center

Google Workspace for Education Plus and Standard administrators can utilize the security center, which provides advanced security information and analytics, and added visibility and control into security issues affecting your domain.

Security center includes the Security Investigation Tool, which can help administrators to identify, triage, and take action on security and privacy issues, such as phishing attacks, inappropriate file sharing, suspicious user and device activity, and much more.

Reports and monitoring

As an administrator, you can see reports and log events in the Google Admin console to review activity in your organization such as potential security risks, see who signs in and when, and understand how users create and share content. You can view domain-level data alongside granular, user-level details through graphs and tables. Use reports and audit logs (including the alert center) to identify security risks, analyze service usage, diagnose configuration problems, track user activity, and much more.

Google Workspace for Education Standard and Plus administrators can leverage the Security Dashboard to see an overview of different security reports, identify trends, and compare current and historical data, such as file sharing in Drive, spam, phishing, and malware activity in Gmail, suspicious user account logins, and suspicious device activities. Most usage, activity, and audit logs — including Admin, Drive, Meet, and Chat log events — and security reports, are available for six months.

Google Workspace is the world's most secure cloud-native communication and collaboration suite

0

actively exploited software vulnerabilities in Workspace since November 2021*

2x fewer

security incidents for organizations using Workspace vs Microsoft 365

2.5x fewer

security incidents for organizations using Workspace vs Microsoft Exchange

50%

potential savings on cybersecurity insurance premiums by using Workspace

*According to the CISA, this is significantly less than other productivity vendors in this space.

Chromebooks

Chromebooks are highly secure, scalable, and easy-to-use computers for students and teachers thanks to Chromebooks' built-in, out-of-the-box security features. There has never been a reported ransomware attack on any business, school, or consumer ChromeOS device. Chromebooks help protect schools from evolving threats with updated features, and updates happen automatically in the background so users get back to work in seconds.

Automatic OS and application updates, with built in malware protection

Attackers are constantly attempting to take advantage of bugs and loopholes in operating systems, browsers, and popular apps to install malware and steal user data. To protect you and your users, Chromebooks keep your OS and applications up to date because it is built secure by default with security updates - and cloud applications never need software updates the way local apps do.

The Google-designed security chip on Chromebooks helps to keep devices secure, protect user identity, and ensure system integrity.

Chromebooks in your fleet will run the latest malware-protection updates automatically. Students and educators are protected from cyber threats with built-in security features like data encryption, verified boot, sandboxing, and automatic updates.

Secure user data

When you sign into a Chromebook with your Google Account, all of your data is stored in encrypted files, thus ensuring that no one else on the device can see your data or sign-in to applications using your account. This makes it very easy and secure for students to share devices within a classroom and for schools to reduce their total cost of computing.

For more advanced security features, Chrome Education Upgrade, the device management license, offers enhanced visibility.

Remote user-managed device security policies

School administrators can configure ChromeOS policies and install/update applications remotely using Google Admin console. With just the click of a button, a single IT administrator can update the policies and configurations of hundreds of thousands of Chromebooks in a moment.

These policies can ensure that

- Students can only access school-approved content and applications
- All applications and extensions are updated with the latest security fixes
- Users can't copy, transfer, or share school data off-device
- Administrators can make data-driven decisions with customized security recommendations from Google to address security threats
- Administrators can centrally manage security and identity and access management policies for all users right in the Admin console

Some highlighted policies that administrators may want to configure are:

Device Policies

- **Guest mode**
  It's recommended to disable your devices' Guest mode so that students and teachers have to log in using their own credentials instead of using the device anonymously.
- **Sign-in restrictions**
  You may not want your students and teachers logging in to your school Chromebooks using their personal Gmail accounts. Enforce sign-in restrictions to be limited to your Workspace domain only for devices used exclusively by students.
- **User and device reporting**
  Admins should consider turning on user and device reporting so that they can gather metrics on how often Chromebooks are being used, who's using them, and the condition of their hardware.
- **Forced re-enrollment**
  It's critical that a Chromebook belonging to a school stay at the school unless an administrator deprovisions it. Admins should consider enabling forced re-enrollment of Chromebooks so that a Chromebook will always re-enroll itself if it were to be wiped or attempted to be stolen.

User Policies

- **Incognito mode**
  Students should be set up to be successful when they're using school Chromebooks. This includes limiting them to their authenticated browser so that web content filters can keep them off of inappropriate websites. Admins should disable Incognito mode so that students are unable to circumvent web filters.
- **Proxy mode**
  While some schools may use proxies for web filtering, it is important to prevent your users from being able to change proxy settings themselves.
- **Multiple sign-in access**
  If users are allowed to log in to a secondary account while using your school's Chromebooks and Workspace accounts, it may allow for a user to easily exfiltrate sensitive student or school data/information to that secondary account. Admins should consider blocking multiple sign-in access.
- **Browser history**
  For students, it may be beneficial to disable their ability to clear their browser history. If an internet security incident were to occur, those internet history logs could be beneficial during an investigation.

This list is a good starting point to ensure your networks are secure from the most common types of mistakes that lead to significant cyber incidents. Other additional recommended security policies can be found in our Security Checklist.

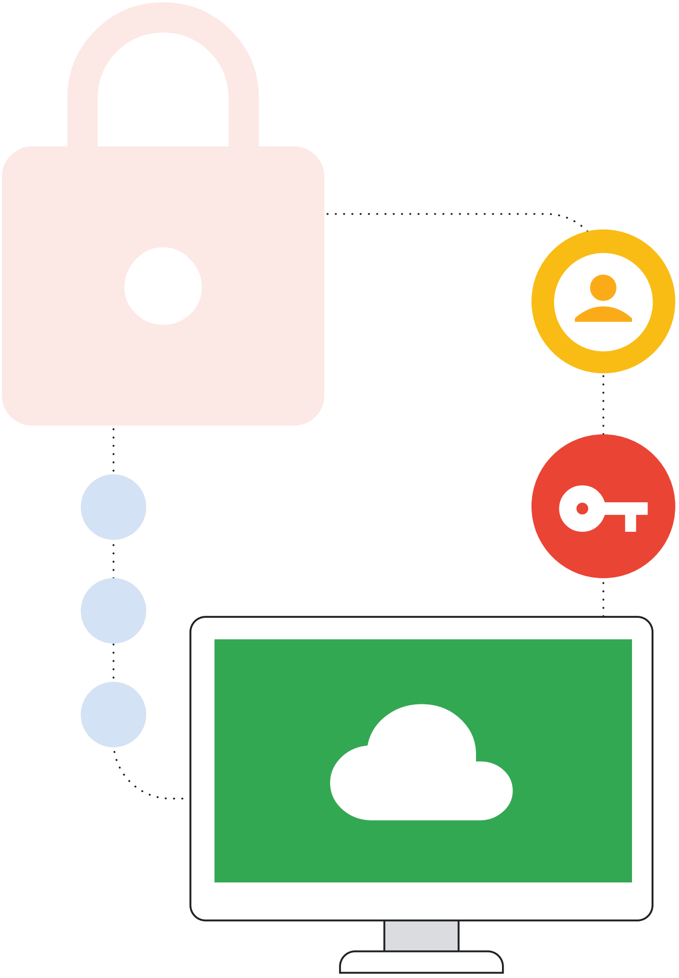
Endpoint management for secure use anytime, anywhere

ChromeOS' remote policy management system enables school administrators to apply security settings and run security tools like content filtering systems on the device rather than on the school's network servers. This ensures that students enjoy the same security benefits on school Chromebooks at home as they do in the classroom. This is increasingly important as schools migrate towards digital textbooks and online learning tools and need to send computers home with students to do their homework.

Conclusion

The challenges of securing K-12 institutions from cyber incidents is a complex endeavor, but well worth the investment in protecting yourself, students, teachers, staff, and the wider online ecosystem. The items covered in this document are a good start, however each school will need to mold the recommendations to their unique needs, and continue to keep pace with the evolving threat landscape and emerging technologies. This resource is a solid foundation of any K-12 security program, providing a resource for potential next steps and implementable action items.

Google also has a variety of resources, training, and skilled cybersecurity professionals available to aid schools and organizations following this guidebook and on emerging technologies like AI. Tailored for education, Google's products provide ready-made solutions to many of the cybersecurity pitfalls outlined in this document. We are eager to work with you as you design and implement your security programs.



Resource List

Discussion of the landscape for K-12 educational technology and associated risks

U.S. government reports

- CISA's Protecting Our Future report explores cybersecurity risks facing elementary and secondary schools and provides recommendations that include cybersecurity guidelines designed to help schools face these risks, published January 2023
- Educational institutions are top targets for cyber attacks, according to CISA's Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data advisory, published December 2020
- GAO's report on Data Security: Recent K-12 Data Breaches Show That Students Are Vulnerable to Harm, published October 15, 2020
- CISA, FBI, and MS-ISAC released a joint advisory called #StopRansomware
  Vice Society advisory notes that some threat actors disproportionately targeting the education sector with ransomware attacks, published September 2022: Upgrading to a more secure solution, such as Chromebooks, can increase security. No ransomware has ever been detected on any ChromeOS device, ever.

Discussion of cybersecurity threats in education and other contexts

- Sophos' The State of Ransomware in Education 2023 report found that ransomware hit 80% of K-12 institutions surveyed, published July 2023
- Zscaler research showing a Nearly 50% Increase in Phishing Attacks with Education, Finance, and Government Being the Most Targeted, published April 2023
- An article reporting on an example of a ransomware attack on a school district, Everything we know so far about the ransomware attack on Los Angeles schools, published September 2022
- Another ransomware attack, that forced school closure in A cyberattack in Albuquerque forces schools to cancel classes, published January 2022
- Information about a recent email hack, Microsoft says Chinese hackers breached email, including U.S. government agencies, published July 2023

Getting started with Google for Education

General information to get started with Google for Education products

- The Google Workspace for Education Quickstart IT Set Up Guide has eight steps to get your institution set up
- For more about Chromebooks in education
- The About Chrome Device Management page has a guide to help administrators who manage ChromeOS devices for a school get started

- The Security checklist for medium and large businesses has tips for setting up Google Workspace for Education and Chromebooks applicable in the education context
- For more about the Google Workspace for Education Fundamentals, Standard, and Plus editions, see features here
- Learn how to connect, enroll, manage, and update Chromebooks and Chrome devices
- For more information on how Google for Education can help you protect your institution, see the Google for Education Privacy and Security Center

Use secure authentication

- How to use a security key for 2-Step Verification
- Information about how to us passwordless login with passkeys
- For Google Workspace for Education, how to set
  - Password requirements for users
  - A third party SSO identity provider
  - How 2-Step Verification works with these third-party identity providers
- How to force users to sign in using 2-step or multi-factor authentication on Chromebooks or ChromeOS
- Account protection for High Risk Users
  - How to protect users with Google's advanced protection program

Apply appropriate security and privacy settings

- How to control which third-party & internal apps access Google Workspace data
- How to manage access for users designated as under 18 years old to unconfigured third-party apps
- How to manage Gmail settings
  - Prevent spam, spoofing & phishing with Gmail authentication
  - Add custom spam filters to Gmail
  - Turn POP & IMAP on or off for users, to prevent the use of third party email applications
  - Help prevent phishing with pre-delivery message scanning
  - Protect users from incoming mail with phishing and malware
  - Control whether Gmail shows external recipient warnings
  - Set up rules to detect harmful attachments with the Security Sandbox
- To add an organizational unit

- How to turn Google Workspace for Education services on or off
  - An explanation of Google Workspace for Education Core and Additional services
  - How to turn a service on or off for Google Workspace users
  - How to control access to Google services by age
  - Protect your business with granular access control security policies for apps based on attributes such as user identity, location, device security status, and IP address
- Set data sharing policies and retention rules
  - How to manage external sharing for your organization
  - Restrict the access users can give to files
  - How to set target audiences for sharing, such as departments or teams
  - Create and manage rules for Drive sharing
  - Allow users to create shared drives and set default sharing settings
  - Manage the members of shared drives and their access level in your organization
  - Turn Directory on or off to control access to organizational and external contacts
  - Customize a directory for a team or group within an organization
  - Protect sensitive information using data loss prevention policies

Update and upgrade your systems

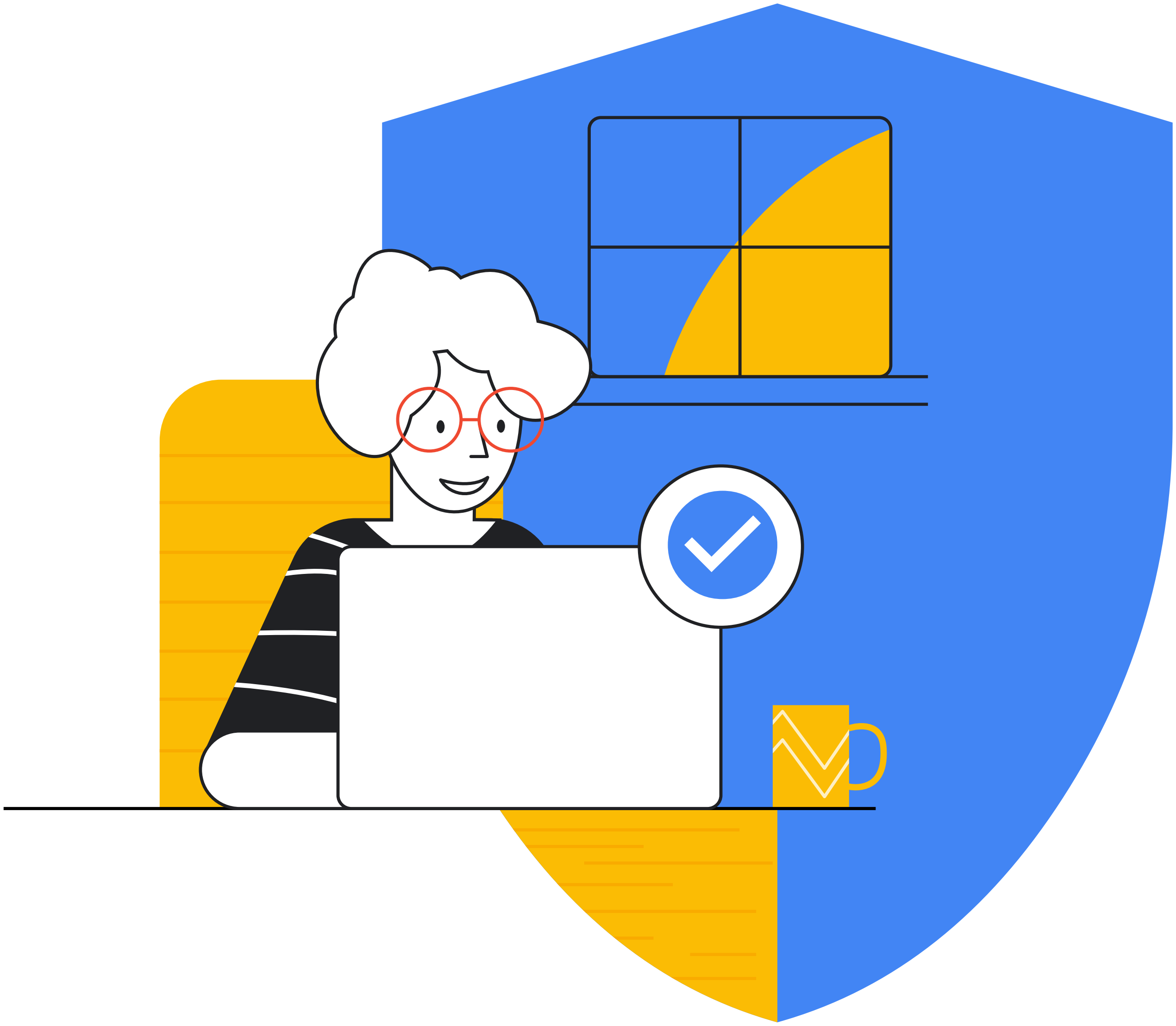
- How to manage ChromeOS device updates
- Chrome is a modern browser that is simple to manage and has enterprise-grade security and management controls
- Chrome OS Flex is a cloud-first, fast, easy-to-manage, and secure operating system for PCs and Macs that can modernize devices you already own:

Use Real-time alerting and monitoring systems

- Best practices for monitoring your ChromeOS fleet using the Google Admin console
- Google Workspace alerting and monitoring
  - Information on how to monitor usage and security reports to identify security risks and track user activity
  - Information of how to use the alert center and how the alert center differs from admin email alerts
  - Information on how to use the security dashboard, including answers to frequently asked questions
  - For information about how the Google Workspace security center can provide advanced analytics and increased visibility into security issues
  - For information on how the security investigation tool can be used to identify and address security and privacy issues through dashboard reports, the investigation tool, and security health page

Train Teachers, Staff & Students

- Google's tips to stay safe and secure online at the Google Safety Center
- Helping kids be safe, confident explorers of the online world
- Khan Academy provides free online courses, including for online security



Google for Education