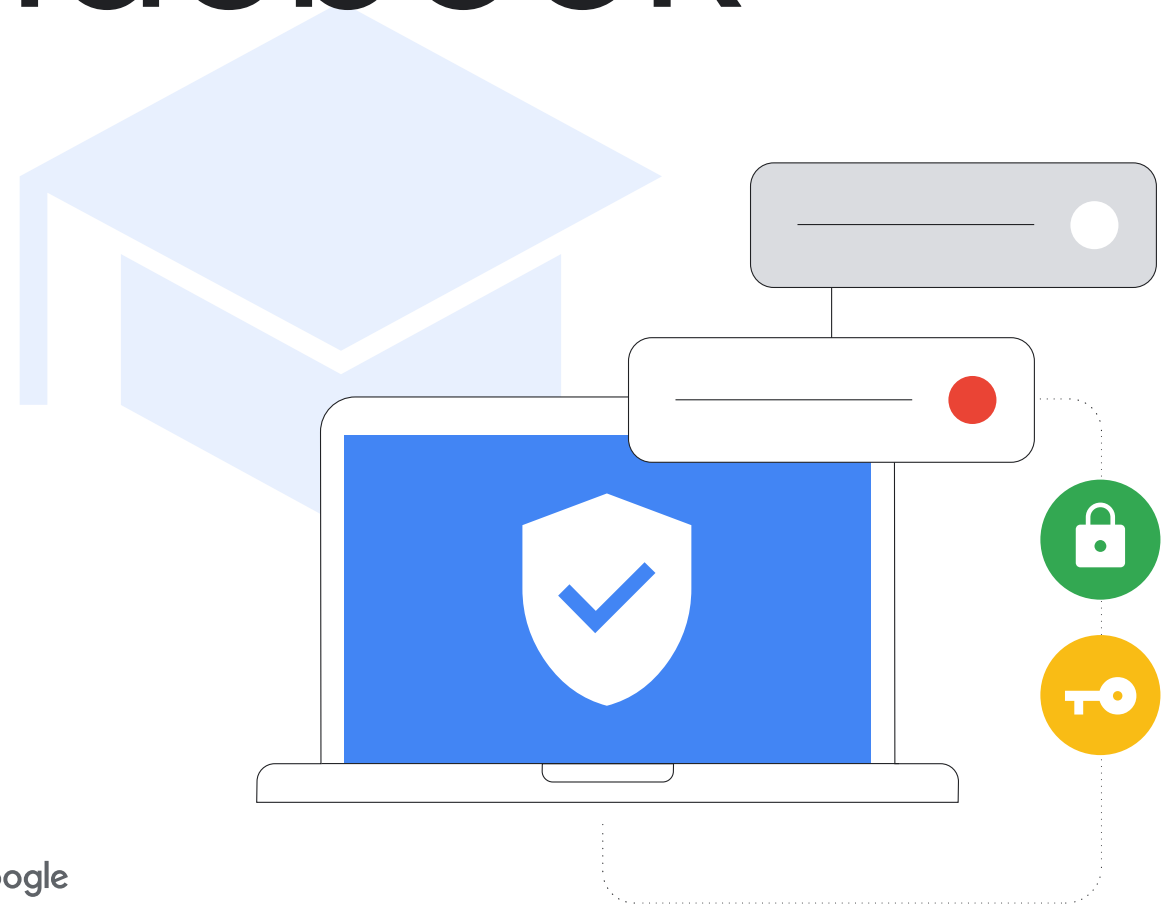
Google for Education

K-12 Cybersecurity Guidebook



Safer with Google

Important Note: This document provides guidance to better secure primary and secondary schools, but no guidance can guarantee complete protection from cybercriminals, and Google does not take responsibility for the implementation or effectiveness of steps mentioned in this guidance. Additionally, nothing in this document should be followed if it is inconsistent with guidance provided by a government agency

Executive summary

As CISA's *Protecting Our Future*[1] report highlights, it is critical for primary and secondary schools to invest in cybersecurity in order to protect their students, families, teachers, staff and communities. This document provides guidance and best practice for school IT administrators on setting up and configuring hardware and software in primary and secondary schools to strengthen cybersecurity. It includes both general best practice, as well as specific guidance for Google products and services. Google's mission to organise the world's information and make it universally accessible and useful is a critical driver of the work that we do on the Google for Education team: building tools designed for teaching and learning. We will share lessons from that work in this guide.

We offer security best practice by topic, providing a more in-depth examination of configuration, setup 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 that our products offer superior protection against common attacks right from the outset.

The risk

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

The defence

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 practice 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 unauthorised users from accessing education systems. Use best practice for user authentication, including strong passwords and two-step verification (2SV), passkeys and password managers where possible, especially for IT administrators and other 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 administrators also properly use 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..
- **USE REAL-TIME ALERTING AND MONITORING SYSTEMS** to increase your security 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, recognise 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 to complement freely available ready-made materials, resulting in a comprehensive toolkit for schools.

1 https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

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 school.

These strategies, along with the additional guidance provided in the following paper, form an excellent foundation for primary and secondary schools' security.

Google's approach for education

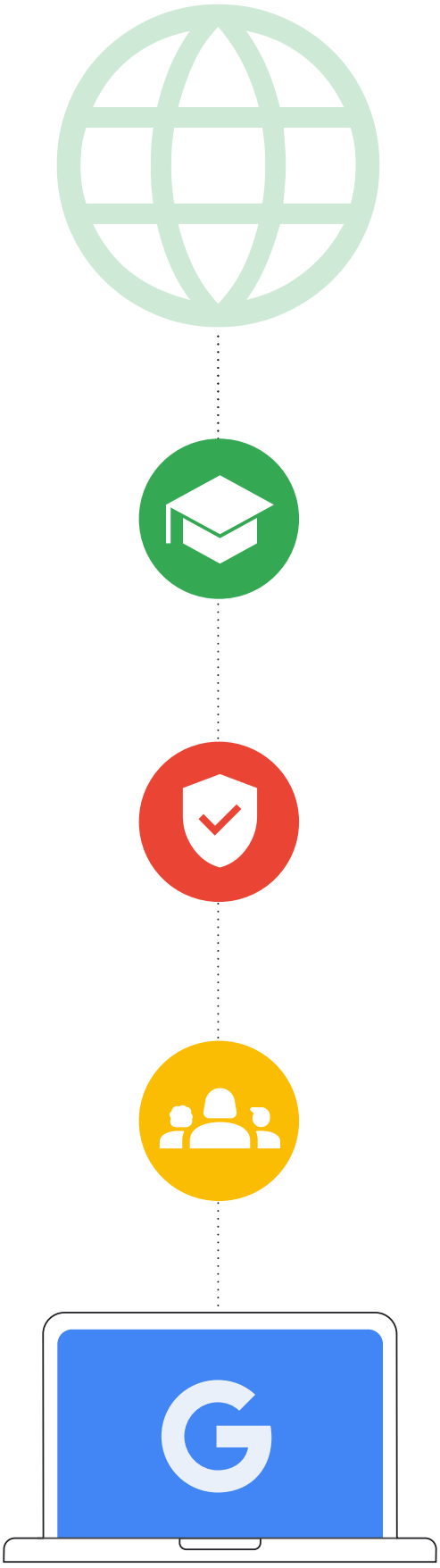
Google's mission is to organise the world's information and make it universally accessible and useful, and that's no less true in the education sector. On the Google for Education team, we do this by building tools like Chromebooks and Google Classroom that make it simple and safe for students and teachers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

Schools deserve technologies that 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 prioritised 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 defence 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 collaboration suites. 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 primary and secondary 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

Primary and secondary schools – both their devices and networks – are at high risk of cyber attack. It is crucial that primary and secondary schools 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)

This guide is a tool to promote cybersecurity best practice for school administrators and school systems to implement in order to better secure their environments. By implementing this best practice, primary and secondary schools 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 in the United States, there were over 1,300 publicly disclosed cyber incidents involving educational organisations across all 50 US states between 2016 and 2021. Today's headteachers must protect the data and personal information of students, teachers and staff, as well as their school's systems and information. This is a big challenge, especially considering the fact that the education sector has traditionally had a harder time keeping pace with cybersecurity compared to other sectors.

Successful cyber attacks, including ransomware, phishing and malware, 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 education 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, primary and secondary schools will continue to find themselves a prime target of opportunity unless a significant 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) 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 practice and guidance for our products and also references Protecting Our Future: Cybersecurity for K-12 | CISA 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 that 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 maximise 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 ensure 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 authentication (2FA)), 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.

There are many device types and deployment models used by schools today and there is a varied technical aptitude in a primary or secondary school environment. Account and device security varies across user roles and types with defined best practice: 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 technically 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 them to use simpler passwords or make immaterial changes (like updating a single character).
- **Two-step verification (2SV):**
  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 that can be vulnerable to phone number-based attacks.
- **Passwordless authentication:**
  Passkeys are a safer and easier alternative to passwords. Users can sign into 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 do not have to manage multiple sets of user credentials, they can save money on IT support and help desk costs. Google Workspace for Education seamlessly supports SSO so that users can use their Google Account credentials to log into third-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 specialised subsets or combinations of these authentication approaches, according to their role within an educational institution, the kind of systems and data that they have access to and their age.

School administrators

School administrators control the systems and much of the data for any primary or secondary school. 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. Chromebooks released after 2019 with a TPM chip contain a power button which can be used for two-factor authentication.
- Administrators should use a trusted password manager that supports 2SV to store their passwords for different services.

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.

Older students using assigned devices

(typically year 5+)

Older students are better educated in how to protect themselves and are usually capable of using more protective authentication mechanisms, which are appropriate to the types of services that 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, tutor group or birthday). Students should be taught how the use of passphrases can provide complexity while making the password easy to remember.

Young students using shared devices

(typically reception to year 4)

The youngest students are still learning how to use educational technology, and will benefit from simple authentication that 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 log in with passwords should put precautions in place for security, since these alternatives 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 cybercriminals around the world, so it is 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 that 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 so that individual users cannot disable or modify them, and other settings should have protective defaults set by the administrator. It is vital 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 minimisation' 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 and updates

Limit and minimise the apps that your users are able to install as each application installed on a device is a potential vulnerability to exploit. If possible, use applications from trusted sources. For example, we recommend that users check for the verification badge on the Google Play Store to ensure that 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 and 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. Prioritise the safeguarding of highly sensitive data, such as user PII, and systems (such as HR, payroll, grading, security and configuration). Carry out audits to scrutinise user access to this data, specifying the circumstances under which access is permitted. Limit access to school-owned devices, and ensure that only specific members of staff have access.

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

Device loss or theft

Losing a device doesn't need to mean that you lose data. Administrators should standardise 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 that they are not used to gain unauthorised access. Chromebooks can be wiped remotely 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 Programme (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 primary and secondary schools, 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 risk profile 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 the 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 unauthorised 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 modernise 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 is important to ensure that the browser is also updated and secure. Modern browsers come equipped with advanced security features that can be easily enabled by users or configured by administrators to be turned on by default on school computers, providing enhanced protection – 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 performing another 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 the IT administrator or other staff to prioritise the activities needing review.

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 administrators to investigate the issue and take action to mitigate the threat.

Alerting and monitoring tools can also be used to gain a deeper understanding of the threats that schools face. By analysing 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 and 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 is 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 is 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 and students

Primary and secondary schools should improve 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 school, 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 contextualise the recommendations for your teachers and students. However you can also take advantage of ready-made material, such as Be Internet Awesome available on Safety. Google, and the Khan Academy, and tailor it to your needs. These programmes can help your users stay safe no matter where they are – in or out of school.

Recognising threats

Training teachers, staff and students to recognise threats is an important part of keeping them safe. Teaching children how to identify a threat is important, since they might not know how to identify whether or not something is legitimate. There are a few types of threats that they should be able to recognise and 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 how to recognise the threat, but to take action. Common threats that users should be able to recognise 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 receive training on proper file and data sharing practices, as well as how to identify and respond to inappropriate requests via 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 sharing the data 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 national insurance 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 that a school district has to protect itself. Software should be designed with a robust architecture to minimise risk of vulnerabilities, with security built in at every layer. Requiring schools to purchase secure software, or software from companies with a proven security track record, can significantly reduce the broader cyber-risk. At Google, we have improved the security of our ChromeOS, for example, while continuing to deploy more proactive, intelligent solutions that harness the capabilities of our expertise in machine-learning, cloud computing and identity management.

Google is committed to building products that help protect student and teacher privacy and provide best-in-class security for your school. 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

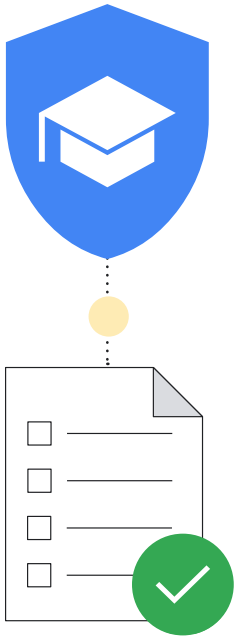
Google Workspace for Education is a set of Google tools and services that are tailored for schools to collaborate, streamline teaching and keep learning safe. Google for Education products and services continuously protect users, devices and data from increasingly complex threats, and provide tools such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

We have put together some helpful materials for those new to Google Workspace for Education. Many of these materials can help you set things up in line with the recommendations outlined in this guidance. See this Quickstart IT setup guide to help you get started with Google Workspace for Education.

Security checklists

Review the security checklists to learn more about how to strengthen the security and privacy of your school. Schools with Google Workspace for Education Standard and Plus editions can also use the Security health page to monitor the configuration of their Admin console settings. For example, you can check the status of settings such as automatic email forwarding, device encryption, Drive sharing, and much more. If needed, you can also make adjustments to your domain's settings based on general security guidelines and best practice, while balancing these guidelines with your organisation'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 maximising the protections built into Google Workspace for Education:

Set up organisational units (OUs)

No one would argue that everyone in your Google Workspace for Education account needs to have the same settings. Organisational units are groups of users that allow you to give different services, settings and permissions to different sets of users; for example, using 2SV for teachers and staff, and age-appropriate authentication for young students. Set up separate organisational units or staff, teachers and students to apply policies to each group of users separately. A well-designed structure is critical to allow you 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 school safe. That is why we have set up flexible ways for you to manage authentication for administrators. This will allow you to ensure 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 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 organisation 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 organisational 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 to bear in mind that users designated as under the age of 18 automatically have restrictions in some Google services when they're signed into 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 organisational unit's access to a Google service, such as Google Drive.

If some users in that organisational unit need to use Drive, you have 2 options:

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

Google Drive is turned off for organisational units 1 and 2

Within an access group

But a **group of users** within organisational 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 whether or not users can share Google Drive files and folders with people outside of your organisation. This can help prevent unintended or excessive sharing of data and files, thereby helping to prevent data leakage. Separating files and drives, creating organisational units, and adhering to the principle of least privilege are important measures to prevent attackers from moving across networks in the event of infiltrating an account. The less data and network access that a potential attacker has access to, the less damage they can do.

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 of your domain, turn on a warning when a user does so. In addition, disable file publishing on the web and require external collaborators to sign in with a Google Account.

Workspace for Education Standard and Plus customers can also use target audiences and trust rules to set sharing recommendations and restrictions at a more detailed level. For example, with target audiences, you set the default link-sharing audience for teachers to 'teachers and staff', rather than everyone at your school. With trust rules, you could block primary school 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. We recommend that you allow only administrators (or other staff such as 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-configured policies that can be used 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 school and their users.

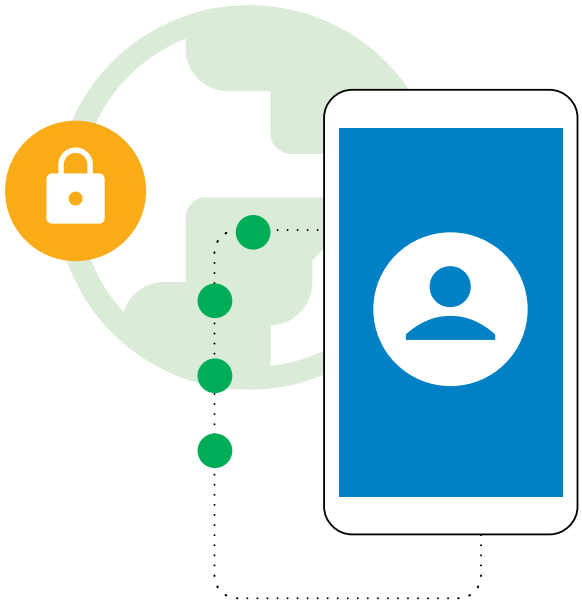
Prevent spam, spoofing and phishing with Gmail authentication. Customise spam filter settings, which should include requiring sender authentication or all approved senders and disabling the ability to bypass spam filters for internal senders.

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 to protect against malware and ransomware by setting up rules to detect harmful attachments using Security Sandbox.

Third-party applications

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



Reports and monitoring

As an administrator, you can see reports and log events in the Google Admin console to review activity in your organisation 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 detailed, user-level information using graphs and tables. View reports and audit logs (including the alert centre) to identify security risks, analyse service usage, diagnose configuration problems, track user activity and much more.

Google Workspace for Education Standard and Plus administrators can use 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.

Leverage the security centre

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

Security centre includes the security investigation tool, which can help administrators to identify, prioritise and take action on security and privacy issues, such as phishing attacks, inappropriate file sharing, suspicious user and device activity and much more.

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

0

actively exploited software vulnerabilities in Workspace since November 2021*

50%

potential savings on cybersecurity insurance premiums by using Workspace

2x fewer

security incidents for organisations using Workspace vs Microsoft 365

2.5x fewer

security incidents for organisations using Workspace vs Microsoft Exchange

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

Google Chromebooks for Education

Chromebooks are highly secure, versatile 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 that users can 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 they are built secure by default with security updates – and cloud applications never need software updates the way that local apps do. The Google-designed security chip on Chromebooks helps to keep devices secure, protect user identity and ensure system integrity.

Chromebooks will run the latest malware-protection updates automatically. Students and educators are protected from cyberthreats 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, ensuring that no one else on the device can see your data or sign into applications using your account. This makes it very easy and secure for students to share devices within a classroom and enables schools to reduce their total cost of computing. For more advanced security features, Chrome Education Upgrade, the device management licence, 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.

This ensures that:

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

Some highlighted policies that administrators may want to configure are:

Device policies

- **Guest mode**
  We recommend that you 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 into 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**
  Administrators should consider turning on user and device reporting so that they can gather metrics on how often Chromebooks are being used, who is using them and the condition of their hardware.
- **Forced re-enrolment**
  It is critical that a Chromebook belonging to a school stays at the school unless an administrator deprovisions it. Administrators should consider enabling forced re-enrolment of Chromebooks so that a Chromebook will always re-enrol itself if it were to be wiped or an attempt is made to steal it.

User policies

- **Incognito mode**
  Students should be set up to be successful when they are using school Chromebooks. This includes limiting them to their authenticated browser so that web content filters can keep them off of inappropriate websites. Administrators 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**
  Allowing users to log into a secondary account while using your school's Chromebooks and Workspace accounts might enable someone to easily exfiltrate sensitive student or school data/information to that secondary account. Administrators 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.

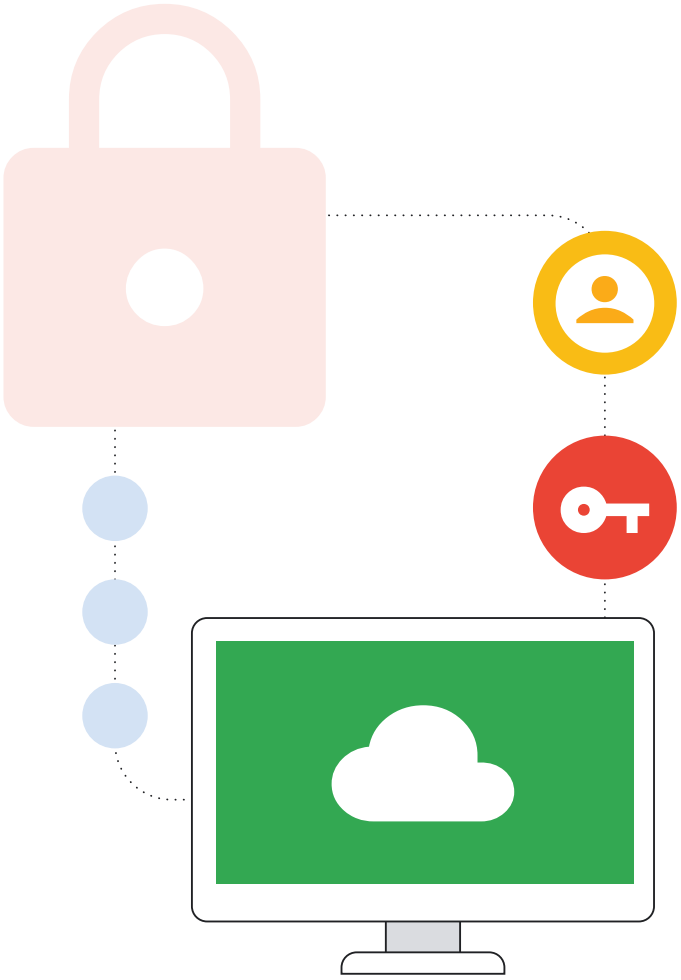
This list is a good starting point to ensure that your networks are secure from the most common types of mistakes that lead to significant cyber incidents. Other additional recommended security policies can be found in our Security checklist.

Endpoint management for secure use at any time, 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.

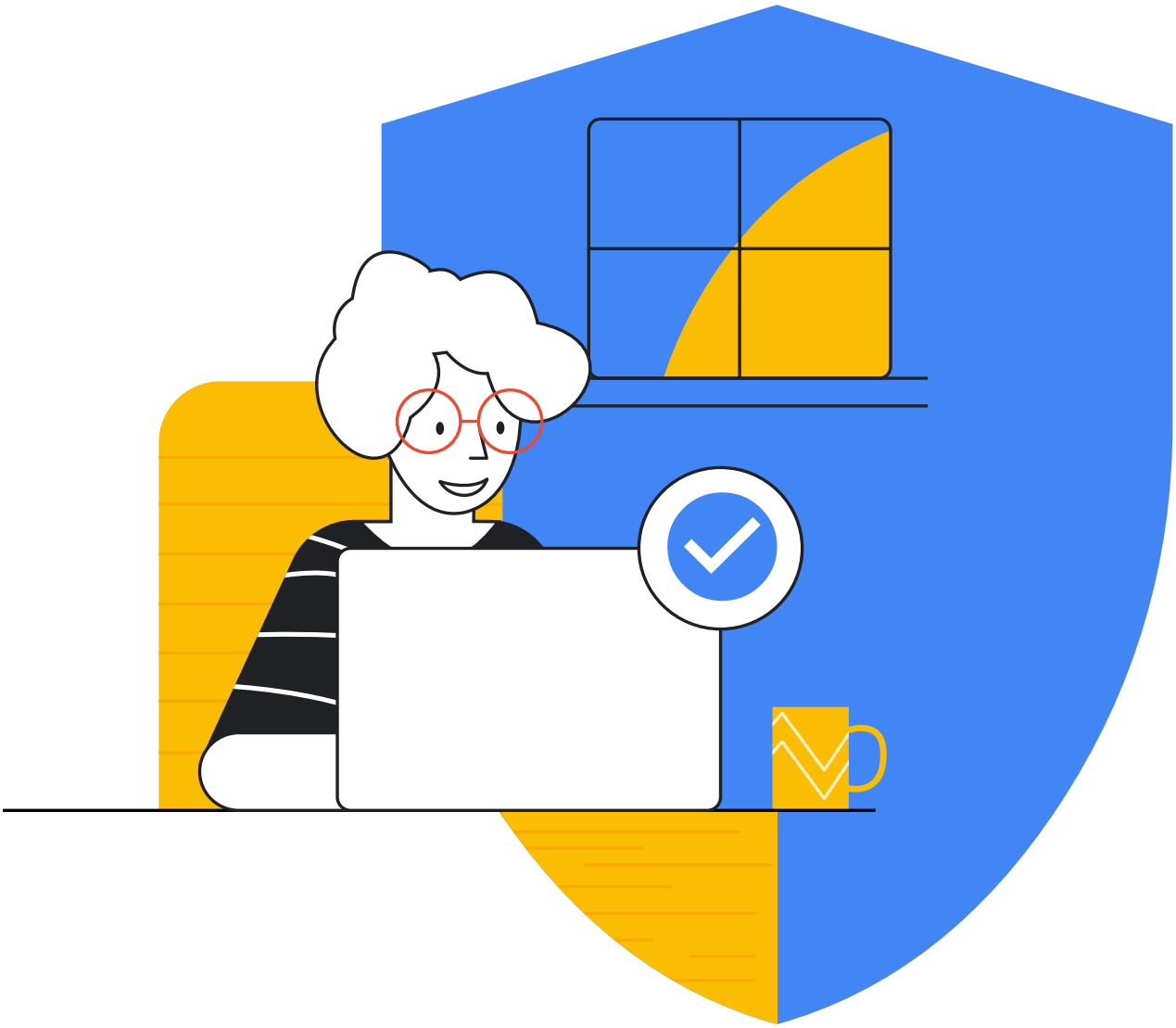
Conclusion

The challenges of securing primary and secondary schools, from cyber incidents is a complex endeavour, 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 starting point. However, each school will need to mould the recommendations to their unique needs, and continue to keep pace with evolving threats and emerging technologies. This resource is a solid foundation of any primary or secondary school security programme, providing a resource for potential next steps and implementable actions. Google also has a variety of resources, training and skilled cybersecurity professionals available to help schools and other organisations using this guidebook. It also provides support for schools to deal with 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 programmes.



Resource list

- Google. 'Tips to stay safe and secure online'. Google Safety Centre, https://safety.google/security/security-tips/. Accessed 6 October 2022.
- NIST. 'Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1'. NIST Technical Series Publications, 16 April 2018, https://doi.org/10.6028/NIST.CSWP.04162018. Accessed 6 October 2022.
- Microsoft. 'Microsoft AccountGuard Program'. Microsoft AccountGuard Program, https://www.microsoftaccountguard.com/en-us/. Accessed 6 October 2022.
- Google. 'Advanced Protection Programme'. Google Advanced Protection Programme, https://landing.google.com/advancedprotection. Accessed 6 October 2022.
- Google. 'Google Safety Centre'. Google Safety Centre – Stay safer online, https://safety.google. Accessed 6 October 2022.
- Meta. 'Basics: Help secure your account'. Help secure your account, https://www.facebook.com/gpa/resources/basics/security. Accessed 6 October 2022.
- Meta. 'Facebook Protect'. Facebook, https://www.facebook.com/gpa/facebook-protect. Accessed 6 October 2022.
- NIST. 'SP 800-124 Rev. 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise'. NIST Technical Series Publications, https://doi.org/10.6028/NIST.SP.800-124r1. Accessed 6 October 2022.
- Passkeys: https://developers.google.com/identity/passkeys
- CISA Protecting Our Future Cybersecurity K-12 Report https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- GAO Report https://www.gao.gov/products/gao-20-644
- For more information on how Google for Education can help you protect your institution, see the Google for Education privacy and security centre.
- Zcaler Phishing Report



Google for Education