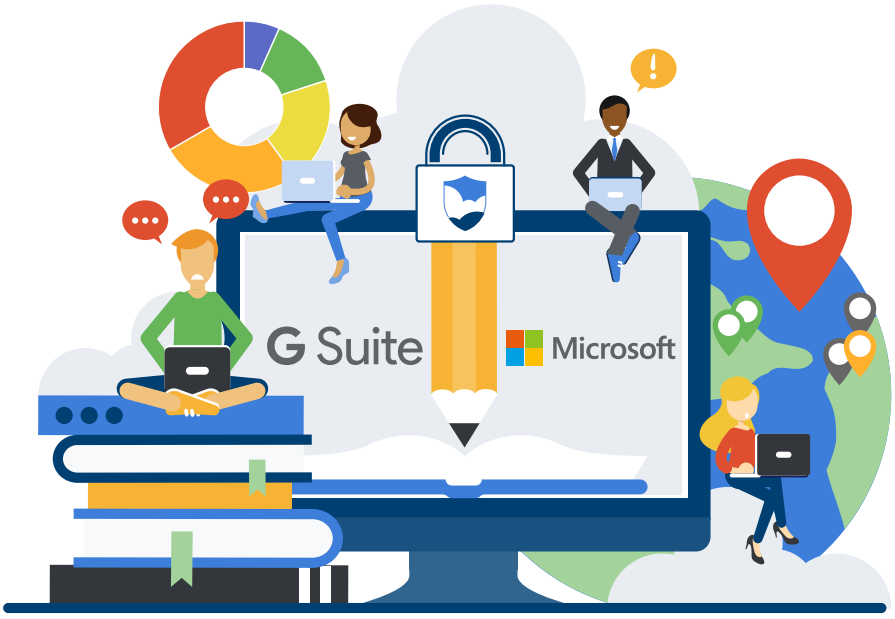
Managed Methods

G Suite & Office 365 Security Made Easy

Remote Learning Security CHECKLIST

12 Step Remote Learning Checklist for Office 365 & Google Admins



managedmethods.com | info@managedmethods.com | 303.415.3640

Remote Learning & K-12 Cybersecurity

K-12 school districts across the country are shutting down to increase “social distancing” and help slow down the outbreak of COVID-19. Many are either considering or preparing for a shift to remote learning for the remainder of the year.

Technologies focused on learning management, online teaching, collaboration, and video conferencing will help districts provide students and staff with the tools needed to move forward with remote learning. This shift requires a lot of time and effort for district IT teams to vet, implement, and support in the coming weeks.

But K-12 IT teams must also plan for the adjustments in cyber safety and security this shift will require.

Students and staff will be accessing their Google and/or Microsoft accounts from locations outside of the school’s networks. They will also be using new, often OAuth-enabled, EdTech SaaS for a variety of learning and student management purposes. Both of these trends expose district information systems to data security and student data privacy risks.

What Is Cloud Application Security?

Cloud application security is a series of defined policies, processes, controls, and technology governing all information exchanges that happen in collaborative cloud SaaS applications like Microsoft Office 365 and Google G Suite.

As your district moves to a remote learning and working environment using cloud apps, your perimeter security safeguards become less effective. K-12 IT teams need to start securing data and monitoring for student safety risks by deploying a cloud-based, zero trust data security framework.

managedmethods.com | info@managedmethods.com | 303.415.3640

Document Remote Work Security Policies

If your district hasn't done so already, now is the time to create and document remote work security policies.

Start by developing a document outlining a list of approved cloud applications to be used for remote learning purposes. If your district doesn't have a learning management system (LMS) or other remote learning tools already available, consider looking into tools such as BrainPop, Discovery Education, Agilix, Edmentum, and more. Other cloud applications your district's IT team may want include Zoom, Google Hangouts, Cisco's Webex, or another popular video conferencing tool that your district is comfortable with using.

Once your team has decided which cloud apps are approved, make sure to include the list in your district's remote work security policy document. You may also consider including a list of apps that shouldn't be downloaded and installed.

Create Employee Cybersecurity Training & Testing

Simple human error is the number one reason cybersecurity incidents happen in any organization. Educate your district's staff, students, and parents on common cybersecurity best practices and what to look for in terms of possible red flags.

Create guidelines that encourage students, staff, and parents to look at who emails are coming from. You may also want to consider testing your users' ability to recognize a suspicious email.

Monitor Student & Staff Account Logins

Students and staff will be logging into their school accounts from outside of your district's security perimeter—and from an unmanaged device if your district isn't 1:1.

Your IT team must monitor account logins and look for anomalous behavior that may indicate an account takeover attack. Anomalous behavior might include multiple unsuccessful logins, failed multi-factor authentication checks, and successful logins from an unapproved location such as another country.

Check For Unsanctioned 3rd Party SaaS Apps

Now that students will be using their school device—or a personal device—outside of school, monitoring for risky 3rd party apps is especially important. This is because malicious apps and apps with insufficient infrastructure security pose far-reaching risks to your district's information systems.

Additionally, the flood of "free" teaching and learning apps on the market creates openings for serious OAuth security risks. Teachers and students alike may take advantage of these tools with the best intentions, but EdTech that hasn't been properly vetted can lead to a variety of cybersecurity risks.

Monitor which apps are granted OAuth access to district Google and/or Microsoft accounts, check what permissions are granted, and be able to remove the apps that don't meet your infrastructure security, data security, and/or student data privacy policies.

Monitor For Improper File Sharing & Access

Student data privacy laws still apply when your district transitions to remote learning, and keeping track of data becomes more difficult when students and staff access everything remotely.

To help prevent any financial, staff, and/or student data from leaving your district's G Suite or Office 365 environment, look for drives, folders and files that have given external accounts access to view and/or edit. If any external shares are found, make sure to break them and set up policies to automatically remediate when a future external share is granted.

Secure Personally Identifiable Information (PII) & Create Data Loss Prevention Policies

Data loss prevention is a strategy to ensure the sensitive information of students and staff are protected and don't inadvertently leave the network. Have your IT team start by checking email and files for PII, such as social security numbers, W2s, and bank account information. Then, delete, quarantine, or revoke access to any information that is being improperly shared.

Once complete, set up automatic policies to remediate all PII that leaves your district's network to ensure FERPA requirements are met.

Create Student Safety Monitoring & Policies

Just because your district's students are distanced from one another as a result of school closures and self-isolation, doesn't mean that they aren't communicating via their school Google or Microsoft accounts.

Students may be using their school accounts to send emails or use Google Docs as a chat board. It's important for your IT team to continue monitoring for signals of cyberbullying, self-harm, inappropriate content, abuse, and other forms of student safety threats. Unfortunately, it may be easier for these issues to go undetected during this time.

Enable Anti-Phishing & Malware Protections

With dispersed students and staff, cybersecurity risks in your district are going to increase. Your IT team will need to ensure they have anti-phishing and anti-malware protections enabled.

Students and staff will be logging in from their home networks and maybe from a personal device, which means school firewalls, web content filters and endpoint security may not be effective for the time being.

The best option for your team at the moment is to start with configuring your district's G Suite and Office 365 anti-phishing and anti-malware capabilities, and layer additional safeguards to ensure district cloud applications are protected—regardless of the device or the location.

Monitor For Lateral Phishing Activity

In the event a student or staff member at your district does fall victim to a phishing scheme, it's important for your IT team to be monitoring the activity that is taking place *within* district cloud apps.

This means not only monitoring the email traffic coming from external sources, but also monitoring and analyzing emails sent from internal accounts to others. Doing so is critical to reveal signs of an account takeover and lateral phishing attack.

Are you getting phishing email alerts from an internal email address? Is a student or staff member sending an unusual number of emails to other school accounts that they don't usually interact with? Is an account suddenly sharing and/or downloading more files than usual? These are a couple examples of trends your team will need to look for more often in a remote learning environment.

Make Multi-Factor Authentication Mandatory

Multi-factor authentication requires your district's students and staff to take a second step, after entering the correct password, to prove they have authorized access. Students and staff will be logging in from unrecognized devices, which makes this security tool a critical one for your district to have enabled during this time.

It's also incredibly quick and easy to set up through your Google and/or Microsoft admin portal.

Multi-factor authentication typically includes entering a code that is sent to their phone via SMS. It can also include phone calls, answering security questions, mobile app prompts, and more.

Reset Passwords Across All Accounts & Set A Password Strength Policy

Set policies and standards for your district's cloud app passwords now that students and staff are accessing remotely.

At a minimum, enable your system's "require a strong password" feature. You can also set minimum and maximum password lengths, password expiration, and more.

If your district already has policies in place, now is a good time to check current passwords to see if there are any passwords that are out of compliance and force password changes through your admin console.

Run A Data Security & Student Safety Audit

With this checklist, now is an opportune time to run a cloud security audit of your district's G Suite and/or Office 365 environment. An audit will check for any configuration errors, sharing risks, files containing sensitive information, risky 3rd party SaaS apps, and more.

It's also important to run an audit on a periodic basis more frequently now that districts are closing or moving to remote learning. Weekly reports can be automated and provide you with detailed information into the security health of your cloud applications, and the activity taking place between students, staff, and external environments.

Managed Methods

G Suite & Office 365 Security Made Easy

Monitor, Audit & Contol Cloud Risks — Made Easy!

If your district uses SaaS applications such as G Suite and Office 365, protecting the data and accounts in these apps is a critical layer in your cybersecurity infrastructure. Without it, monitoring and controlling behavior happening on the inside is impossible.

This blind spot creates critical vulnerabilities in your district stakeholders' sensitive information.

ManagedMethods makes securing your district's cloud applications easy. The platform provides malware and phishing protection and data loss prevention for cloud-based email, files, and shared drive applications. ManagedMethods uses advanced machine learning technology to detect account takeovers, a growing issue in cloud security.

Using ManagedMethods, system admins can quickly and easily determine where security risks exist, remediate seucrity issues, set up customizable data loss prevention policies, and more.

Experience how ManagedMethods provides easy visibility and control

Watch A 10 Minute Demo On-Demand

managedmethods.com | info@managedmethods.com | 303.415.3640