Managed Methods

The K-12 Cyber Safety Checklist

Although the internet has done wonders for learning and collaboration, it's also home to malware, phishing, cyberbullying, and more. Avoiding these risks isn't simple, but it's easier if you take the necessary precautions. Here's a checklist of what staff members, parents, and kids can do to stay safe online:

- **Practice safe browsing.** Use a content filter to block malicious websites and inappropriate content, such as graphic violence, nudity, or unlawful behavior.
- **Use strong passwords.** Combine numbers, letters, and characters to make them more difficult to crack, and avoid basing them off personal information that can be guessed.
- **Teach digital literacy.** Share the basics and best practices your people should know about staying safe online, avoiding risks, and protecting their privacy.
- **Don't fall for phishing.** Suspicious emails and messages may be hackers trying to trick users into sharing login credentials, clicking on harmful links, or downloading malicious attachments.
- **Think before you share.** Cloud apps like Google Workspace and Microsoft 365 make file sharing easy, but you may accidentally expose sensitive information to unauthorized users.
- **Supervise online activity.** Monitoring tools help uncover potential safety risks, whether they be cyberattacks, cyberbullying, violence, or cases of self-harm.
- **Plan ahead.** Know what steps you'll take if a cyber incident occurs so you can get ahead of the threat and contain its damage.
- **Backup important data.** This can help you recover lost information if it's accidentally or maliciously impacted during a cyber incident.
- **Choose apps wisely.** Some are more privacy-safe than others. Understand how your applications access and use your data before approving them for regular use.
- **Automate software updates.** Outdated apps and resources are more easily exploited. Regularly download the newest version, which usually patches known vulnerabilities.