Google for Education

Safeguard your data with secure authentication

Stay ahead of potential breaches in your institution by verifying that your teachers, students, and staff are who they say they are.
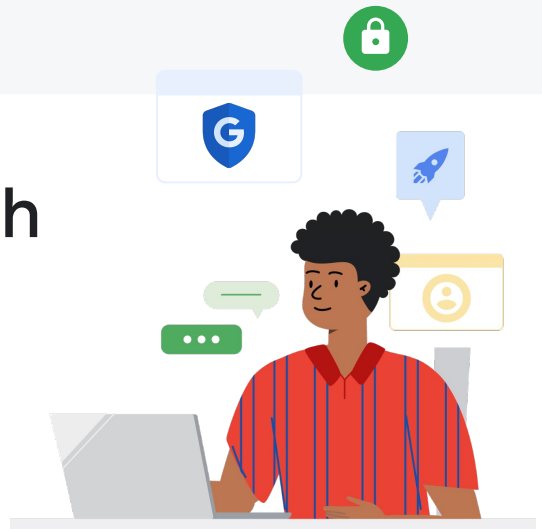
Educational institutions are top targets for cyberattacks, with bad actors looking to exploit schools' data-rich environments. With the prevalence and sophistication of today's ransomware, having students, educators, and staff with weak or noncredentialed accounts can lead to breaches. But there are things you can do to secure your institution's data.

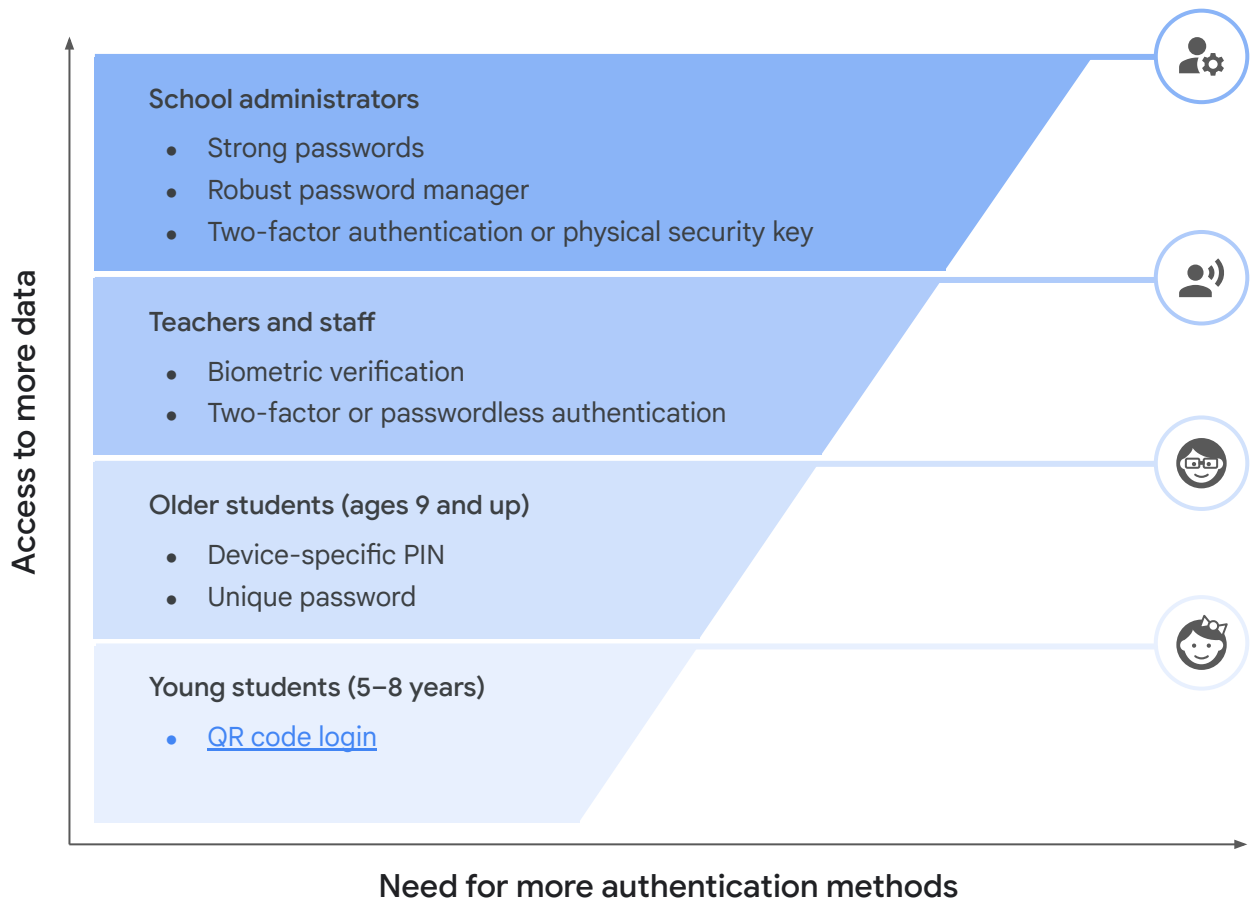## Best practices for using authentication tools

Method	Practice		Pro tip
Strong passwords	Provide users with clear guidelines for password length and complexity minimums.	>	Don't ask users to regularly change their password as it can result in the user making simpler passwords.
Two-factor authentication	Prompt users to input a one-time verification code from a security key or app on their mobile phone.	>	Avoid verification codes by texts or calls as these can be vulnerable to phone number-based attacks.
Passwordless authentication	Instead of remembering a password, use an app or website with a PIN, fingerprint, or facial recognition login.	>	Combat phishing with passkeys that work only on users' registered websites and apps.
Single sign-on	Use tools like Google Workspace for Education to access multiple apps with one set of credentials.	>	With just one password to remember, users are less likely to write it down, which boosts security.
Password managers	Help users create strong passwords for various accounts by encouraging the use of a password manager.	>	When searching for a password manager, pay attention to features, usability, and how it encrypts data. Explore Google's Password Manager.

Learn more about secure authentication at goo.gle/k12-cyber-guide

Ensure everyone knows how to secure their accounts

Each person in your school should secure their data with strong passwords and the right authentication tools – and the more access they have to personal data, the stronger their account security should be. Here are the methods we recommend by role and age group:

Access to more data →

School administrators
- Strong passwords
- Robust password manager
- Two-factor authentication or physical security key

Teachers and staff
- Biometric verification
- Two-factor or passwordless authentication

Older students (ages 9 and up)
- Device-specific PIN
- Unique password

Young students (5–8 years)
- QR code login

Need for more authentication methods

Explore these digital safety resources

One of the best ways to combat breaches is to educate your whole school community on staying secure online. Share these resources with students, guardians, educators, and staff to encourage everyone to take part in protecting their institution from cyberthreats.

- K-12 Cybersecurity Guidebook
- Digital Citizenship and Safety Course
- Be Internet Awesome
- Guardian's Guide to Privacy & Security
- Family Link
- Google for Education Privacy and Security Center

→ **Learn more about secure authentication at goo.gle/k12-cyber-guide**