



Acceptable-Use Guidelines

Cybersecurity skills are powerful. We teach defense, and we only practice on systems we have permission to use. Every member reads these guidelines with a parent or guardian and agrees to them online before starting labs.

Updated September 2026

The one rule behind all the others

Only test, access, or change systems, accounts, devices, networks, and locks that you own or have clear permission to use. If you aren't sure you have permission, you don't. Stop and ask a coach.

Practicing security skills

- 1 Practice in approved places.** Use the club's lab environments, your own devices, or legal practice platforms and competitions a coach has approved, such as picoCTF or Hack The Box. Stay within each platform's rules and scope.
- 2 Never target real systems without permission.** That includes school networks and devices, home or public Wi-Fi you don't manage, websites, apps, games, and other people's accounts or devices. "Just looking" or "just testing" still counts.
- 3 Leave school technology alone.** Don't scan, probe, bypass filters on, or try to get around security on school networks or devices, even to prove a point.
- 4 Lockpicking is for practice locks only.** Only pick locks you own that are not in use, or practice locks the club provides. Never pick a lock that protects someone else's property, even your own family's, without their okay.
- 5 Found a problem? Report it, don't use it.** If you discover a security weakness in a real system, don't explore it further or share it publicly. Tell a coach, who will help you report it responsibly to the owner.
- 6 Keep tools in the lab.** Security tools and techniques learned in the club stay in approved environments. Don't share them with anyone to use against real targets.

Accounts, data, and privacy

- 7 Protect your accounts.** Use the separate club accounts we set up for club tools, turn on multi-factor authentication, and never share passwords, including with friends.

- 8 **Respect other people's data.** Don't collect, read, copy, or share anyone else's personal information, messages, or files. Lab data stays in the lab.
- 9 **Don't impersonate anyone.** No fake accounts, phishing, or pretending to be someone else, including as a joke, outside an approved lab exercise.
- 10 **Be careful with shared devices.** Don't install software on club or borrowed devices without permission, and log out when you're done.

Competitions and events

- 11 **Follow competition rules.** Attack only the targets you're given, never the competition's own infrastructure or other teams, and don't share flags or answers when the rules say not to.
- 12 **Follow event rules.** At conferences and events, follow the organizers' policies, including rules about photography, recording, and participating in villages or contests.

Why this matters

Accessing a computer, account, or network without permission can be a crime, even for minors and even when nothing is damaged. Laws such as the federal Computer Fraud and Abuse Act and California Penal Code section 502 apply. It can also lead to school discipline. Following these guidelines keeps you, the club, and other people safe.

If the guidelines aren't followed

Breaking these guidelines is taken seriously. Depending on what happened, it may lead to a conversation with the member and their parent or guardian, loss of lab or competition access, or removal from the club. Anything that may be illegal or put someone at risk may be reported to parents, guardians, or the appropriate authorities.

Agreement

- I have read these Acceptable-Use Guidelines with my parent or guardian, and I agree to follow them in and outside club meetings.
- I understand that if I'm not sure whether something is allowed, I will stop and ask a coach first.

Members agree to these guidelines in the online club application. Parents and guardians confirm they've reviewed them with their student in the online consent form. There's nothing to sign on paper.