

CLASSROOM LESSON · GRADES 6-8

# Private by design

Audit a profile, tighten the settings and respect other people's information

Students run a privacy audit on a fictional seventh grader's profile, find the location clues, public settings, shared screenshots and photos of friends posted without asking, then recommend the setting fixes and finish with their own privacy check-up.



GRADE BAND  
**6-8**

TIME  
**45 minutes**

FORMAT  
**Whole class + groups**

PREP  
**Print & cut, ~10 min**



**BIG IDEA**

**You get to decide what your profile shares about you, and other people get to decide what you share about them.**



**Students will be able to**

- ☐ Find at least five privacy leaks in a fictional student profile, including location clues, schedule clues and other people's information
- ☐ Recommend specific setting changes (private account, location sharing limited to chosen people, message and tag controls) and explain what each one costs and protects
- ☐ Explain what a screenshot does to a private message or disappearing post, and apply the ask-first rule before posting or forwarding someone else's photo or information
- ☐ Complete a personal privacy check-up and name an adult to tell if something they shared gets passed around



**Materials**

- Projector or board for the slide outline
- Worksheet 1: Privacy audit of Jordan's profile (1 per student; it contains the full fictional profile)
- Worksheet 2: My privacy check-up (1 per student)
- Scenario cards (1 set per group of 3-4, cut apart)
- Highlighters or colored pencils for marking privacy leaks
- Sticky notes or half sheets for the exit ticket

**Before class**

- Print both worksheets double-sided and one set of scenario cards per group.
- Read the fictional profile on Worksheet 1 so you can point to each clue quickly.
- Write the name of your school counselor and the school's reporting option for online problems (for example, the front office or an online form) on the board.
- Check your district's acceptable-use and student conduct policy so you can describe in one sentence what happens when students post others' images without permission.
- Decide whether students will open their own app settings in class. If personal phones are not allowed, Worksheet 2 works as a take-home check-up instead.



**Vocabulary**

- **Digital footprint** — Everything that can be found about you online, including what you post, what others post about you and what apps collect in the background.
- **Privacy settings** — The controls in an app that decide who can see your posts, message you, tag you or find your profile.

## Vocabulary (continued)

- **Location sharing** — A feature that shows your real-time or last-known location on a map to the people you choose. It can usually be turned off or limited to a few people.
- **Location data (metadata)** — Hidden information saved with a photo or post, such as where and when it was taken, if the camera's location setting is on.
- **Screenshot** — A picture of whatever is on a screen. It makes a permanent copy, even of a disappearing message, and the sender usually cannot take it back.
- **Consent** — Clear permission. Asking a person before you post or forward their photo, video, name or number, and respecting a no.
- **Public account** — A profile anyone can see and follow, including people you have never met. A private account lets you approve who sees your posts.
- **Oversharing** — Posting details that let strangers figure out who you are, where you will be or how to reach you.

## Standards alignment

- **ISTE Standards for Students 1.2.a** — Digital footprint (paraphrased): students manage their digital identity and understand that what they do online has lasting effects on themselves and on other people.
- **ISTE Standards for Students 1.2.b** — Online interactions (paraphrased): students treat others with empathy and respect online, which here means asking before posting or forwarding someone else's image or information.
- **ISTE Standards for Students 1.2.d** — Digital privacy (paraphrased): students take action to protect their privacy on their devices and manage their personal data and security online.
- **CSTA PK-12 Computer Science Standards (2026) MS-DAT-IM-28** — Paraphrased: explain the benefits and risks of letting apps and websites collect and use personal data and metadata such as location, including questions of privacy and who controls the data.
- **CSTA PK-12 Computer Science Standards (2026) MS-SYS-SE-32** — Paraphrased: explain what happens when confidentiality, integrity or availability of data is not protected, for example when personal information is shared beyond the people it was meant for.
- **CSTA K-12 Computer Science Standards (2017) 2-IC-23** — Paraphrased: describe the tradeoffs between making information public and keeping it private and secure.

Aligns with commonly used digital citizenship frameworks (ISTE Standards for Students) and with both the 2026 CSTA PK-12 and the 2017 CSTA K-12 computer science standards; Georgia districts can map it to their state computer science and digital literacy expectations and to local acceptable-use and student conduct policies.

## Lesson sequence · 45 minutes

### **5'** Warm-up

- 1 Show slide 1. Ask students to raise a hand (no names, no details) if they have ever seen a screenshot of a private chat get passed around.
- 2 Ask: If a stranger had five minutes and only your public posts, what could they figure out? Collect quick answers on the board: school, team, neighborhood, schedule, friends' names.
- 3 Tell students that today they will play privacy auditor on a fictional student, not on each other.

**Say:** *Nobody in this room is getting graded on their own accounts today. We are going to look at a made-up seventh grader named Jordan and figure out what a stranger could learn. Then we will fix it.*

### **10'** Mini-lesson

- 1 Slide 2: A digital footprint is what you post, what others post about you and what apps collect in the background. Ask for one example of each.
- 2 Slide 3: Location sharing. Explain that many phones and apps can show your location to friends on a map. The safer setting is off, or on only for a few people you know in real life, with a parent or guardian aware.
- 3 Slide 4: Photo clues. Show the list: house numbers, street signs, school logos, ID badges on lanyards, team jerseys with a school name, the inside of a bus with its number. Mention that some cameras also save location data inside the photo file.
- 4 Slide 5: What a screenshot does. A disappearing message disappears from the app, not from someone's camera roll. Once screenshotted, the sender loses control of it.
- 5 Slide 6: Other people's information and images. The ask-first rule: ask before you post or forward someone's photo, video, name, number or chat, and take it down if they ask.

**Say:** *Privacy settings are not about hiding. They are about choosing your audience. You would not hand your schedule to every person at the mall, so your profile should not hand it out either.*

## 17' Activity

- 1 Hand out Worksheet 1. Students read Jordan's full profile in the box at the top and highlight every detail a stranger could use (about 3 minutes, individually).
- 2 In groups of 3-4, students work through the six audit items: name the risk, choose the best fix and write one sentence explaining why (about 8 minutes).
- 3 Each group then draws two scenario cards and agrees on what the student in the card should do (about 4 minutes).
- 4 Circulate. Push groups to name the exact setting (for example, 'location sharing: off' or 'tags need my approval') instead of 'be careful'.
- 5 Call time and have each group share one fix they think Jordan would actually do (about 2 minutes).

**Say:** *For every leak you find, I want two things: what could go wrong, and the exact setting or action that fixes it. 'Be careful' does not count as a fix.*

## 8' Discussion

- 1 Use two or three of the discussion questions. Start with the Maya photo, because it is about someone else's privacy, not Jordan's.
- 2 Ask students to name a tradeoff: what does Jordan give up by going private or turning off location sharing, and is it worth it?
- 3 Close by pointing to the board: if something you shared gets passed around, tell a trusted adult or the school counselor. Nobody gets in trouble for asking for help.

## 5' Exit ticket

- 1 Students answer the three exit ticket questions on a sticky note or half sheet.
- 2 Hand out Worksheet 2 (My privacy check-up) to finish at home with a family member, along with the family take-home sheet.

## Discussion questions

1. **Jordan's friend Maya asked Jordan not to post the sleepover photo. Jordan posted it anyway because 'it's a cute picture.' Whose decision should that be, and why?**  
Listen for: Students recognize that a person's image belongs to their own decision-making, that a no is a no, and that the fix is to take it down and apologize. Strong answers mention that people can have reasons they do not share, including safety reasons.
2. **What does Jordan give up by making the account private and turning off location sharing? Is the tradeoff worth it?**  
Listen for: Honest tradeoffs (fewer followers, friends cannot see where Jordan is) weighed against risks (strangers knowing the home address and weekly schedule). Strong answers suggest middle ground such as sharing location with two or three trusted people only.
3. **A message disappears after it is opened. Why is it still not really private?**  
Listen for: Anyone can screenshot or use a second phone to take a picture of the screen, and the copy can be forwarded forever. The app may also keep data on its servers. The sender loses control once it is sent.
4. **Which detail in Jordan's profile surprised you most as a privacy leak, and why?**  
Listen for: Specific detail such as the volleyball schedule plus the park name, the house number in the background or the teammates' phone numbers in the screenshot. Students explain how pieces combine into a pattern.
5. **If something you shared gets screenshotted and passed around, what are your first three moves?**  
Listen for: Do not respond with anger or more posts; save evidence; report and block on the platform; tell a trusted adult or the school counselor; ask friends not to forward it.

## Exit ticket

Answer on a sticky note. No names needed.

1. Name two details in a photo background that can reveal where you live or go to school. → **Any two of: house number, street sign, school logo or mascot, ID badge or lanyard, team jersey with school name, bus number, a recognizable local landmark.**
2. What is the safest location-sharing setting for most middle schoolers? → **Off, or on only for a few specific people they know in real life, with a parent or guardian aware. Not 'all friends' or 'all followers'.**
3. Before you post or forward a photo or screenshot that shows someone else, what do you do? → **Ask them first, respect a no and take it down if they ask later. Do not forward other people's chats or numbers without permission.**



### Support

- Give students a word bank for the audit: location, schedule, school, address, phone number, consent, screenshot, public, private.
- Pre-highlight two leaks in Jordan's profile so students see the pattern before searching on their own.
- Let students answer the audit items by choosing the multiple-choice option first, then adding the why sentence with a partner.



### Extend

- Ask students to write a short 'privacy settings guide' for a younger sibling: five settings, in order of importance, with one sentence each.
- Have students research how one setting (for example, photo location tagging on a phone camera) is turned off on a device they use, and present the steps without naming accounts.
- Debate prompt: Should apps set new teen accounts to private and location-off by default? Students argue both sides using the tradeoffs from today.



### Multilingual learners

- Pair key terms with icons on the board: a map pin for location, a camera for screenshot, a lock for private account, a handshake for consent.
- Provide sentence frames: 'The risk is \_\_\_\_\_. The fix is \_\_\_\_\_. This protects \_\_\_\_\_.'
- Allow students to discuss in their home language within groups and report out in English or with a partner's help. Share the Spanish family sheet with Spanish-speaking families.



### Accessibility

- Provide the profile on Worksheet 1 in large print or digitally so screen readers can read it; every leak is described in words, not shown only by color or images.
- Students who cannot highlight can underline, circle or list the leaks by number.
- Read the profile and audit items aloud for students who benefit from audio, and allow oral answers for the exit ticket.



### Family extension

**Private by design: a family privacy check-up.** Today your student practiced finding privacy leaks in a made-up student's profile, such as a house number in a photo, a weekly schedule in a post and location sharing turned on for everyone. They also learned to ask before posting or forwarding photos of other people. Please spend 10 minutes doing the check-up together.

Send home the family sheet (English and Spanish) included in this lesson pack.



### Follow-up: free 2-minute lesson

[k12cyberforward.com/learn/student-identity-location](https://k12cyberforward.com/learn/student-identity-location)

Project it for a quick review or share the link with families.

Related Cyber Academy course: [academy-students-6-8](#).

### Sources and further reading.

- FTC — Net Cetera: Chatting with Kids About Being Online (privacy settings, location services, asking permission before posting photos): [https://consumer.ftc.gov/sites/default/files/articles/pdf/netcetera\\_2018.pdf](https://consumer.ftc.gov/sites/default/files/articles/pdf/netcetera_2018.pdf)
- NCMEC NetSmartz — Smartphones (location sharing, photo location tags, privacy settings): <https://www.missingkids.org/netsmartz/topics/smartphones>
- ISTE Standards for Students: <https://iste.org/standards/iste-standards-for-students>
- CSTA — 2026 PK-12 Computer Science Standards: <https://csteachers.org/pk12standards/>
- CSTA — K-12 Computer Science Standards (2017): <https://csteachers.org/wp-content/uploads/2025/03/csta-k-12-computer-science-standards-revised.pdf>