

Teaching Students to Share Safely

Students often treat game and chat spaces like ordinary social spaces. Teach them that several harmless-looking details can combine to identify where they live, learn, play, or spend time.

Recommended classroom use: Grades 5-9

SMALL DETAILS ADD UP. A first name, school mascot, town, sports team, photo background, and usual play time can identify a student even when no single detail seems sensitive.

TEACH THE SHARE CHECK

- Who is asking, and do I know this person offline?
- Why do they need this information?
- Does it reveal who I am, where I live or go to school, or my routine?
- Could it help someone contact, locate, impersonate, or access my account?
- If the answer is yes or unsure: do not share; ask a trusted adult.

INFORMATION TO PROTECT

- Full name combined with school, club, team, class, or location details.
- Home address, phone number, personal email, exact birthday, or live location.
- Daily routines, travel plans, or times a student may be alone.
- Passwords, MFA/verification codes, recovery codes, or account answers.
- Photos showing uniforms, street signs, house numbers, schedules, or intimate content.

GAME / CHAT RED FLAGS

- Quickly asks age, school, city, selfie, phone number, or social accounts.
- Pushes a student to move to a private app, DM, video call, or encrypted chat.
- Offers skins, currency, gifts, cheats, or favors for information or secrecy.
- Uses pressure such as "prove you trust me" or "do not tell anyone."
- Threatens, blackmails, or tries to arrange an in-person meeting.

WHEN A STUDENT TELLS YOU

- Stay calm, thank the student for telling you, and focus on immediate safety.
- Do not investigate the account, search the student's personal phone, or ask the student to open explicit content.
- Follow district child-protection procedures. If state law makes you a mandated reporter, use the required reporting route and timeframe; an internal referral may not satisfy your individual duty.
- If conduct may be sex-based harassment connected to the school education program or activity, involve the Title IX coordinator under district policy; do not use Title IX as the default route for an external-stranger case.
- Call 911 for immediate danger. Report suspected online child sexual exploitation through NCMEC's CyberTipline.

IF A SEXUAL IMAGE OF A MINOR MAY BE INVOLVED

Record only non-image details you can see without opening content: username/account name, platform, and date/time. Do not open, save, download, copy, forward, email, AirDrop, photograph, or screenshot suspected sexual imagery. Do not take possession of a student's personal device in order to inspect or search it. Follow district procedure if a device must be secured, and hand the incident to the designated school administrator or child-protection contact and/or law enforcement.

3 CLASSROOM ACTIONS

1. Teach the Share Check.
2. Practice with realistic, non-explicit chat scenarios.
3. Name the trusted adults and reporting routes students can use.

Official guidance: Child Welfare Information Gateway - mandated reporting; U.S. Department of Education - Title IX; U.S. Department of Justice - child sexual abuse material; NCMEC - CyberTipline and Take It Down; FTC - Kids and Video Games.

School review note: No accounts or sign-ups; no student details requested; no advertising cookies. Basic security/server logs may include an IP address.

Free educational resource: GetIntoCyberJobs.com | © 2026 Paul David Cuffe | CC BY-NC 4.0 | v3 | August 2026 | Page 1 of 3



getintocyberjobs.com/school.php

Think Before You Share

Games, group chats, voice chat, DMs, and social apps can be fun. You can enjoy them without giving other people clues that identify you, locate you, or help them get into your accounts.

Student handout - Recommended for Grades 5-9

YOU CAN ASK FOR HELP. If someone pressures, tricks, or threatens you, it is not your fault and you are not in trouble for asking for help. Tell a trusted adult as soon as you can.

KEEP THIS PRIVATE

- Your full name, school, home address, phone number, or personal email.
- Exact birthday, live location, daily routine, or when you are home alone.
- Passwords, login codes, verification codes, or recovery information.
- Photos showing a school badge, street, house number, schedule, or location clues.
- Nude, partially nude, or sexual images - even if someone promises to keep them secret.

SHARE MORE SAFELY

- Use a gamertag that does not include your real name, school, birth year, or location.
- Keep profiles, friend lists, and location settings private where possible.
- Chat about the game and general interests without giving exact personal details.
- Do not scan QR codes or click links sent by people you do not trust.
- Ask a parent or trusted adult before moving a new online friendship to another app or video call.

WATCH FOR THESE TRICKS

- "What school do you go to?" or "What city are you in?"
- "Send a selfie" or "turn your camera on."
- "I'll give you skins / currency if you tell me..."
- "Move to another app so nobody can see our chat."
- "Do not tell your parents or teacher" or "prove you trust me."
- "Send me the code so I can verify your account."

IF SOMETHING FEELS WRONG

- Stop replying and leave the chat, match, party, or call.
- Write down the username/account name, platform, and time - do not copy or resend explicit content.
- Block and report the account using the game or platform tools.
- Tell a trusted adult quickly - even if you already shared something.
- If you shared login information, change the password and turn on MFA.
- If someone threatens you about an image: do not pay, send more, or try to handle it alone.

IF AN INTIMATE IMAGE IS INVOLVED

Never screenshot, download, forward, or resend a sexual image of anyone under 18. NCMEC says Take It Down can be used when the image or video is already on the device where it was originally taken. The image stays on that device while a digital fingerprint (hash) is created. Do not download the image, or ask anyone to send it to you, just to use the service. If you do not have access to the original device, ask a trusted adult for help and make a CyberTipline report.

3 THINGS TO DO TODAY

1. Check your privacy settings.
2. Choose a non-identifying gamertag.
3. Pick the trusted adult you would tell first.

Official guidance: NCMEC - Take It Down FAQ, CyberTipline, and NetSmartz; FTC - Kids and Video Games; FBI - Sextortion. Take It Down: takeitdown.ncmec.org | CyberTipline: report.cybertip.org

School review note: No accounts or sign-ups; no student details requested; no advertising cookies. Basic security/server logs may include an IP address.

Free educational resource: [GetIntoCyberJobs.com](https://getintocyberjobs.com) | © 2026 Paul David Cuffe | CC BY-NC 4.0 | v3 | August 2026 | Page 2 of 3



getintocyberjobs.com/school.php

Safer Sharing at Home

The goal is not to ban games or chat. It is to make privacy rules clear, use available safety settings, and make it easy for a child to come to you early when something goes wrong.

Family guide supporting students in Grades 5-9

MAKE DISCLOSURE EASIER. Agree in advance that when your child brings you an online problem, the first priority is safety and help - not punishment or blame.

SET SIMPLE FAMILY RULES

- Do not share identifying information with people your child only knows online.
- Ask before moving a new online contact to private chat, video calls, or another app.
- Never share passwords, verification/recovery codes, or intimate images.
- Do not meet an online-only contact without parent/caregiver involvement and a safe plan.
- Treat gifts, trades, skins, currency, or "free" items that require personal information as a warning sign.

CHECK THE SETTINGS

- Set profile visibility and friend requests to the most private age-appropriate option.
- Limit voice/text chat to approved friends, or switch it off where appropriate.
- Review camera, microphone, location, photo, and contact permissions.
- Use parental controls to reinforce family rules and age limits.
- Protect game/platform accounts with unique passwords, MFA, and spending/PIN controls.

KEEP CONVERSATIONS OPEN

- Ask who your child plays with, not only how long they play.
- Ask whether anyone has requested personal details, selfies, another app, a video call, secrecy, money, or gifts.
- Explain that friendly behavior, shared interests, or gifts do not prove an online identity is genuine.
- Review new games and chat features together, especially after updates.
- Make sure your child knows another trusted adult they can tell if you are not available.

IF YOUR CHILD TELLS YOU

- Stay calm, believe the disclosure, focus on safety, and avoid blaming the child.
- Record the username/account name, platform, and date/time - not the image itself.
- Block/report the account and secure any account whose login information was shared.
- Report suspected online child sexual exploitation to NCMEC's CyberTipline and contact law enforcement as appropriate.
- Call 911 if a child is in immediate danger.

IF A SEXUAL IMAGE OF A MINOR MAY BE INVOLVED

Do not ask your child to resend it. Do not screenshot, photograph, copy, email, AirDrop, forward, or download it onto another device. Record usernames, platform, and timestamps only. NCMEC says Take It Down should be used on the device where the image or video was originally taken; do not download or share an image just to submit it. If that original device is unavailable, make a CyberTipline report for help. Report threats, sextortion, or suspected exploitation through the CyberTipline.

3 THINGS TO DO TODAY

1. Review one game together.
2. Agree what information stays private.
3. Agree what should be reported to an adult immediately.

Official guidance: NCMEC - Take It Down FAQ, CyberTipline, and NetSmartz; FTC - Kids and Video Games and parental controls; FBI - Protecting Your Kids and Sextortion. Take It Down: takeitdown.ncmec.org | CyberTipline: report.cybertip.org

School review note: No accounts or sign-ups; no student details requested; no advertising cookies. Basic security/server logs may include an IP address.

Free educational resource: [GetIntoCyberJobs.com](https://getintocyberjobs.com) | © 2026 Paul David Cuffe | CC BY-NC 4.0 | v3 | August 2026 | Page 3 of 3



getintocyberjobs.com/school.php