



CONNECTED WITHOUT COMPROMISE

GAMER MODE

Online Games, Voice Chat, Esports & Digital Safety

Includes a Parent Field Guide for healthy, safe gaming



LANCASTER SOLUTIONS LLC SAFETY EDUCATION TEAM

Secure. Fast. Built to grow.

LANCASTER SOLUTIONS LLC

CONNECTED WITHOUT COMPROMISE GAMER MODE

A Teen Gamer's Guide to Online Games, Voice Chat,
Discord, Esports, and Digital Safety

WITH A PARENT FIELD GUIDE FOR SUPPORTING HEALTHY, SAFE GAMING

ACCOUNTS • CHAT • DISCORD • SCAMS • ESPORTS • HEALTH • RECOVERY

Prepared by the Lancaster Solutions LLC Safety Education Team

Ages 13–18 • Families • Educators • Coaches • Youth-Serving Professionals

Research and platform guidance reviewed through July 2026

Connected Without Compromise: Gamer Mode

Second Publication Edition - July 2026

Prepared and edited by the Lancaster Solutions LLC Safety Education Team.

Copyright © 2026 Lancaster Solutions LLC. All rights reserved.

Educational-use permission: educators, libraries, counselors, and nonprofit youth-serving organizations may reproduce the checklists, discussion prompts, worksheets, and pocket action cards for noncommercial instruction when the material is unmodified and attribution is retained.

Free website edition license: the complete PDF may be shared without charge only in its original, unmodified form. It may not be sold, rebranded, altered, or represented as legal, medical, mental-health, financial, tax, or individualized safety advice.

Product, platform, game, company, and service names are used descriptively. Their owners retain their respective trademarks. No platform, publisher, school, government agency, or child-safety organization endorses this book unless a written endorsement states otherwise.

Facts, laws, school rules, platform settings, and reporting processes change. Use the update center before relying on a platform-specific instruction.

Updates and corrections: Connected Without Compromise update center

Accessibility: this edition uses structured headings, descriptive navigation, high-contrast text, and tagged-PDF export. Readers who need another format may contact the publisher through the Lancaster Solutions LLC website.

ISBN: not assigned for this website educational edition.

Publication and Safety Note

This book is educational. It is not legal, financial, medical, mental-health, cybersecurity, or tax advice. Platform features, age rules, parental controls, game economies, tournament requirements, and reporting systems change. Verify current settings and policies before acting, especially when a minor's safety, money, travel, contracts, or evidence is involved.

All scenarios are fictional composites. "Gaming" includes console, PC, mobile, cloud gaming, virtual worlds, social games, voice chat, Discord-style communities, livestream play, esports, modding, trading, and related creator activity.

! IMMEDIATE DANGER

Call emergency services if anyone is in immediate physical danger. In the United States, call 911. If a young person is in emotional crisis or at risk of self-harm, call or text 988. If a minor is being sexually exploited, groomed, or threatened with intimate material, contact the National Center for Missing & Exploited Children CyberTipline and involve a safe adult.

RESET: The Gamer Incident Response

Games reward speed: queue again, answer the message, defend your rank, save the trade, prove you are not scared. During a safety incident, speed can make the damage spread. RESET gives you a practiced way to stop the match from controlling the next decision.

R REMOVE YOURSELF — Leave the lobby, call, server, trade, stream, or argument. Do not keep engaging to win the exchange.

E EVIDENCE — Save usernames, profile links, server names, timestamps, messages, trade records, payment details, clips, and report numbers without redistributing harmful material.

S SECURE — Protect the primary email, game account, device, payment methods, active sessions, recovery information, and linked accounts.

E EXPLAIN — Tell a usable adult, coach, school professional, tournament official, or another person who can act calmly and help coordinate the response.

T TELL THE RIGHT SYSTEM — Report through the platform and contact law enforcement, NCMEC, a bank, school, or crisis service when the incident involves threats, exploitation, fraud, stalking, swatting, or immediate harm.

■ THE RULE BEFORE EVERY RULE

The match can end. The streak can break. The server can wait. The person matters more than the inventory, rank, reputation, or team schedule.

The Series Safety Backbone

Every response framework in the Connected Without Compromise series maps to the same five actions. The mode-specific acronym helps you remember the context; the backbone helps you act even when you forget the acronym.

1. **PAUSE OR LEAVE** - Stop the interaction, stream, lobby, payment, upload, or automated action.
2. **PRESERVE EVIDENCE** - Save usernames, links, timestamps, messages, transaction records, and report numbers without redistributing harmful material.
3. **SECURE ACCESS** - Protect the primary email, accounts, devices, sessions, recovery methods, and payment tools.
4. **TELL A USABLE ADULT** - Bring in a calm adult or qualified professional who can help without making disclosure feel like punishment.
5. **REPORT AND FOLLOW UP** - Use the correct platform, school, bank, child-safety, crisis, or law-enforcement route, then record what happens next.

Memory line: Stop the pressure. Save the facts. Secure the door. Bring in help. Keep following up.

A Note to Teen Gamers

Gaming can be competition, art, friendship, problem solving, identity, teamwork, and a serious skill. This book will not pretend that every online friend is fake, every game is harmful, or every hour spent playing is wasted. It will treat your gaming life as real enough to deserve real boundaries and real recovery plans.

You do not have to accept abuse to prove you belong. You do not owe a teammate your password, a stranger your real name, a guild leader your private photos, or a coach unlimited access to you. You can be competitive without letting a rank become your worth. You can be social without making yourself available to everyone.

KEEP THIS SENTENCE

A mistake does not cancel your right to help. The next safe move matters more than the last unsafe one.

A Note to Parents and Caregivers

Games are often where teenagers talk, cooperate, recover from a difficult day, and maintain friendships. Treating gaming as automatically meaningless can close the door to the information adults most need. A usable adult learns enough about the game, platform, people, and pressure to respond accurately without turning every incident into a reason to confiscate everything.

The parent field guide focuses on transparent supervision, family agreements, spending controls, healthy routines, team and travel safety, and calm crisis response. The goal is not to monitor every word. The goal is to make sure a teenager knows what to do, whom to tell, and what adult support will look like when something unsafe happens.

How to Use This Book

Teen gamers can read Parts I–V in order or begin with the chapter closest to a current problem. Parents can start with Part VI and then complete the drills together. Each chapter includes a fictional scenario, practical guidance, a checklist, discussion questions, and a Make It Stick exercise that rehearses the first safe move under pressure.

PLATFORM SNAPSHOT: JULY 2026

Twitch does not permit children under 13 and requires minors to use the service under parent or guardian supervision. Discord has expanded teen-default safety protections and Family Center controls, including settings for friend requests, server direct messages, message requests, and sensitive-content handling. Roblox, Xbox, PlayStation, Nintendo, and Epic provide family or parental controls for communication, content, spending, and playtime, but the available settings vary by platform, game, age, and region. Verify current controls on the official support page for each account.

Contents

Copyright, Permissions, and Updates

RESET: The Gamer Incident Response

The Series Safety Backbone

PART I PROTECT YOUR PLAYER IDENTITY

1. Player Is a Role, Not Your Whole Identity
2. Lock the Account Stack
3. Gamer Tags, Profiles, and Privacy
4. Safe Downloads, Mods, Cheats, and Malware
5. Screen Sharing, Devices, Networks, and Location

PART II SURVIVE THE SOCIAL LOBBY

6. Voice Chat Is a Room Full of Strangers
7. Discord, Guilds, Clans, and Private Servers
8. Online Friendships and Grooming
9. Sexual Pressure, Sextortion, and Image Abuse
10. Toxicity, Harassment, Dogpiles, and Hate
11. Doxxing, Swatting, Stalking, and Violent Online Networks

PART III PROTECT YOUR MONEY AND INVENTORY

12. Virtual Currency, Skins, and Spending
13. Loot Boxes, Gacha, and Gambling-Like Design
14. Trades, Marketplaces, Giveaways, and Fake Support
15. Account Selling, Boosting, Cheating, and Bans
16. Sponsorships, Creator Codes, Coaching, and Opportunities

PART IV COMPETE WITHOUT LOSING YOURSELF

17. Esports Teams, Coaches, and Safe Competition
18. Tournaments, Travel, LAN Events, and Meeting Online Friends
19. Rage, Tilt, Trash Talk, and Emotional Regulation
20. Sleep, School, Body, Hearing, and Healthy Play
21. Rankings, Burnout, Identity, and Knowing When to Stop

PART V RECOVER AND KEEP PLAYING

22. Helping a Teammate in Crisis
23. RESET: Incident Response for Gamers

- 24. Stolen Accounts, Lost Inventory, and Payment Fraud
- 25. Raids, Reputation Damage, Appeals, and Starting Again

PART VI PARENT FIELD GUIDE

- 26. Support Without Treating Games as the Enemy
- 27. Readiness, Supervision, and the Family Gaming Agreement
- 28. Platform Controls, Communication, and Privacy
- 29. Money, Esports, Contracts, Travel, and Workload
- 30. Crisis Response, Growing Independence, and the Long-Term Plan

TOOLS CHECKLISTS, AGREEMENTS, CHALLENGE, RESOURCES, GLOSSARY, SOURCES

PART I

PROTECT YOUR PLAYER IDENTITY

The safest gaming life is built before the lobby fills, the trade opens, or the account becomes valuable.

CHAPTER 1

Player Is a Role, Not Your Whole Identity

QUICK RECALL BEFORE YOU READ

What pieces of your gaming identity connect back to your real name, school, family, routines, or other accounts?

SCENARIO

Sixteen-year-old Lena is known in a competitive shooter by the same gamer tag she has used since middle school. The tag appears on her clips, Discord profile, school esports roster, and an old art account that includes her real first name. After a heated match, another player finds the school roster and starts posting her team schedule in chat.

A player identity is a boundary tool

A gamer tag can create useful distance between play and private life. It gives teammates a name to use without automatically giving them a legal name, school, home town, birthday, or family information. That distance is strongest when the account is designed intentionally rather than assembled from details that already identify you.

A player identity is not dishonesty. It is context. You may use a nickname at practice, a stage name on a channel, and a real name on school records. Different spaces need different amounts of information.

Linkability matters more than one secret

Most privacy losses do not come from one dramatic post. They come from clues that connect. A unique gamer tag used across a school team page, resale profile, public playlist, and social account can turn several ordinary facts into a map. Profile photos, bios, time zones, repeated backgrounds, friend lists, and writing style can also connect identities.

Search your main tag while logged out. Try variations, old spellings, and platform-specific versions. The goal is not to erase your existence. It is to understand what an angry opponent, curious stranger, or fake recruiter can assemble without special tools.

Decide what the audience gets

Write a public-information boundary before a tense moment. A practical version might allow your general region but not your town, a grade range but not your school, interests but not family names, and scheduled posts but not live routines. Decide whether teammates may know your first name and whether spectators may.

A boundary made before pressure is easier to keep when someone says, “Everyone else tells us,” or “We need your real name to trust you.” Trust should grow from behavior, not forced disclosure.

Keep the game from owning your self-worth

A rank, win rate, team role, inventory, or reputation can feel personal because you invested time and skill. But the account is a project, not a complete measure of you. When the player role becomes the only place you feel competent or respected, losses and bans can feel like the destruction of your identity.

Protect other parts of life on purpose: offline friendships, school goals, movement, sleep, creative interests, and people who know you without a leaderboard. A stronger whole life makes competitive setbacks easier to survive.

Chapter 1 Summary

- A gamer tag can create healthy distance between public play and private identity.
- Privacy risk often comes from linked clues rather than one obvious secret.
- Define public-information boundaries before another person pressures you.
- Trust does not require legal names, school details, or family access.
- Your account and rank are projects, not your entire identity.

Chapter 1 Safety Checklist

- ☐ Search my main gamer tags while logged out.
- ☐ Remove school, team, town, birthday, and family clues from public profiles.
- ☐ Use different profile images or names when separation matters.
- ☐ Write what teammates may know and what the public may know.
- ☐ Ask friends not to reveal my real name or routine in open chat.
- ☐ Keep at least two meaningful parts of life outside gaming.

Chapter 1 Discussion Questions

1. How can one gamer tag connect several accounts?
2. What is the difference between privacy and pretending?
3. Which details would help someone identify your school or routine?
4. Why are boundaries easier to keep when written in advance?
5. What non-gaming activities protect a player from rank becoming identity?

Make It Stick

MEMORY ANCHOR

YOUR TAG IS FOR THE GAME. YOUR WHOLE LIFE IS NOT PART OF THE LOADOUT.

PRESSURE TEST

A new teammate says the team cannot trust you unless you send a photo of your school ID.

- A. Send it with the address covered.
- B. Refuse, tell the team adult or organizer, and ask what legitimate verification is actually required.
- C. Leave the team without saving the message.

SAFEST FIRST MOVE

Choose B. A real organization can explain verification, involve an adult, and collect only necessary information through an appropriate process.

60-SECOND DRILL

Search one gamer tag in a private or logged-out browser. Write down every real-world clue visible in the first page of results.

SAY IT OUT LOUD

I can verify through the official process, but I do not send identity documents in chat.

CLOSED-BOOK RECALL

1. What makes identities linkable?
2. Name two facts that should stay out of a public gaming profile.
3. What should trust be based on?

CHAPTER 2

Lock the Account Stack

QUICK RECALL BEFORE YOU READ

Which single account could reset most of your gaming life? Start there.

SCENARIO

Marcus uses the same password pattern for his email, game launcher, console account, and Discord. A fake tournament page captures one version. The attacker enters his email, resets two game accounts, steals tradable items, and sends scam links to his friends before Marcus realizes that the first account lost was not the game - it was the recovery hub.

Your primary email is the control room

Game accounts rarely stand alone. They connect to email, console profiles, launchers, payment services, streaming accounts, phone numbers, cloud saves, and social logins. The account that can reset the others deserves the strongest protection. For most players, that is the primary email.

Use a unique password or passkey, strong multifactor authentication, current recovery details, and login alerts. Review forwarding rules after a compromise; an attacker may quietly redirect or hide security messages.

Unique credentials stop one breach from becoming a chain

Credential stuffing uses passwords exposed on one service against many others. Small changes such as adding a number or symbol do not create meaningful separation when the base phrase is reused. A password manager makes long, unique credentials practical and reduces the temptation to reuse.

Prioritize uniqueness for email, Steam or other launchers, console networks, Discord, payment accounts, cloud storage, streaming channels, and any game with valuable inventory.

Use the strongest second factor available

Multifactor authentication reduces the value of a stolen password. Passkeys and FIDO/WebAuthn security keys are designed to resist

common phishing attacks. Authenticator apps are generally stronger than text messages, though any supported MFA is usually better than password-only access.

Never approve an unexpected login prompt or share a verification code. Repeated prompts may be an MFA-fatigue attack. Deny, change the password from the official app or site, review sessions, and secure recovery information.

Recovery is part of security

A secure account you cannot recover is not a successful setup. Save backup codes somewhere separate from the device they unlock. Remove old phone numbers, unknown devices, outdated recovery emails, and third-party connections. Record account IDs and purchase receipts that may help prove ownership.

For Steam, official support recommends Steam Guard and offers a mobile authenticator. Other platforms provide their own security and recovery tools. Use official support pages reached from bookmarks or the app - not links sent by a stranger claiming to be support.

Chapter 2 Summary

- The primary email is often the recovery hub for the entire gaming stack.
- Password reuse allows one stolen credential to spread.
- Phishing-resistant MFA is strongest where available.
- Unexpected login prompts and codes should never be approved or shared.
- Backup codes, purchase records, and current recovery details improve recovery.

Chapter 2 Safety Checklist

- ☐ Secure the primary email first.
- ☐ Replace reused passwords with unique credentials.
- ☐ Enable passkeys, security keys, or authenticator MFA where supported.
- ☐ Save recovery codes away from the main device.
- ☐ Review active sessions and linked applications.
- ☐ Keep account IDs and legitimate purchase receipts.
- ☐ Use only official support routes.

Chapter 2 Discussion Questions

1. Why should email be secured before a game account?
2. What is credential stuffing?
3. Why can a one-time code still be phished?
4. Where should recovery codes be stored?
5. What records can help prove account ownership?

Make It Stick

MEMORY ANCHOR

ONE BREACH SHOULD OPEN ONE DOOR - NOT THE WHOLE HOUSE.

PRESSURE TEST

A "support agent" in Discord says your account is flagged and asks for the six-digit code that just arrived.

- A. Send the code because the alert is urgent.
- B. Stop, open the official account app independently, and report the impersonator.
- C. Ask the agent to prove identity with a screenshot.

SAFEST FIRST MOVE

Choose B. Verification codes are keys. Real support should not require you to hand over a code that the message says not to share.

60-SECOND DRILL

List your email, launcher, console, Discord, and payment accounts. Mark which ones reuse a password or lack MFA.

SAY IT OUT LOUD

I do not share login codes. I will contact support through the official site.

CLOSED-BOOK RECALL

1. Which account is usually the control room?
2. What should you do with an unexpected MFA prompt?
3. Name two records that support account recovery.

CHAPTER 3

Gamer Tags, Profiles, and Privacy

QUICK RECALL BEFORE YOU READ

What can someone learn from your avatar, bio, status, friends, clips, and linked accounts without asking you directly?

SCENARIO

Diego's profile only lists his first name and favorite team. His avatar is a photo taken in his bedroom. A jersey, school award, bus pass, and window view are visible behind him. Someone he argued with in a sports game identifies the school and starts calling him by his last name.

Profiles leak through context

A profile can reveal more than the fields you typed. Avatars show rooms, uniforms, badges, mail, reflections, and other people. Status messages reveal routines. Friend lists reveal school or family connections. Linked music, streaming, and social accounts may expose a real name or location.

Review the profile as a stranger. Check what is visible to everyone, friends, friends of friends, server members, and party members. Privacy settings can change after platform updates, so treat the review as maintenance rather than a one-time task.

Use separate lanes when the audience changes

A public esports profile, a private friend account, and a hobby account may need different names, images, contact methods, and visibility. Separation reduces accidental mixing, but only if the accounts do not reuse the same unique tag, profile photo, bio sentence, or public friend network.

Do not create so many identities that recovery becomes impossible. The goal is not complexity for its own sake. It is clear separation between public competition, known friends, and private life.

Status and activity are location clues

"At practice until 8," "home alone grinding ranked," or a visible local weather alert can reveal current circumstances. Automatic activity sharing may show when you are awake, which game you play, which server you joined, and whether you are in a private party.

Turn off activity visibility where it creates risk. Delay clips or posts that reveal a routine. Avoid announcing that a house is empty, a parent is away, or you are waiting alone after an event.

Privacy is not secrecy from safe adults

A private gaming space can be healthy. Dangerous secrecy is different: someone says no trusted adult may know, asks you to delete evidence, or threatens the friendship if you involve support. A safe friend or teammate does not need you isolated.

Choose at least one usable adult who knows which platforms and communities matter to you. They do not need every conversation. They do need enough context to help if a situation changes.

Chapter 3 Summary

- Avatars, status messages, links, and friend networks reveal context.
- Different audiences may need different account lanes.
- Activity visibility can reveal routines and current vulnerability.
- Privacy settings require periodic review.
- Healthy privacy can include a trusted adult; dangerous secrecy isolates you from help.

Chapter 3 Safety Checklist

- ☐ Review my profile from a non-friend view.
- ☐ Replace avatars that expose rooms, uniforms, documents, or other people.
- ☐ Remove unnecessary linked accounts.
- ☐ Limit activity and status visibility.
- ☐ Delay posts that reveal I am alone or away.
- ☐ Tell one usable adult which platforms and servers matter.

Chapter 3 Discussion Questions

1. What can an avatar reveal beyond a face?
2. When is a separate account useful?
3. How can activity status become a routine map?
4. What is the difference between privacy and dangerous secrecy?
5. Which account links expose more than they provide?

Make It Stick

MEMORY ANCHOR

SHOW THE GAME. DO NOT ACCIDENTALLY PUBLISH THE MAP TO YOUR LIFE.

PRESSURE TEST

A friend asks you to set a matching real-photo avatar in a large public server.

- A. Do it because matching avatars are harmless.
- B. Use a non-identifying matching design or keep your current avatar.
- C. Upload a photo and delete it tomorrow.

SAFEST FIRST MOVE

Choose B. Friendship does not require publishing a real-world identifying image to strangers.

60-SECOND DRILL

Open your profile permissions and write down who can see your friends, activity, connections, and status.

SAY IT OUT LOUD

I keep real-world photos for people I know, not for a public server.

CLOSED-BOOK RECALL

1. Name three profile clues besides a real name.
2. Why should activity visibility be reviewed?
3. Who should know enough to help during an incident?

CHAPTER 4

Safe Downloads, Mods, Cheats, and Malware

QUICK RECALL BEFORE YOU READ

What request should make you stop a download immediately: disable security, grant administrator access, or re-enter credentials? The answer is all three.

SCENARIO

A teammate offers Ava a “private performance mod” that promises better frames and undetectable aim assistance. The download is hosted on a file-sharing page and requires her to disable antivirus, run the program as administrator, and sign into her launcher again. The teammate says everyone on the team uses it.

Free advantage is a powerful lure

Malicious downloads are often packaged as cheats, cracked games, free currency generators, skin tools, optimization utilities, mods, or tournament software. The promise creates urgency and makes security warnings feel like obstacles. A person may even use a compromised friend account to recommend the file.

Treat “disable antivirus,” “ignore the warning,” “run as administrator,” and “log in through this custom tool” as stop signs. Legitimate software may sometimes need elevated access, but it should come from an official or well-established source with a clear purpose and reputation.

Mods need a trust chain

Mods can be creative, educational, and central to a game community. Safer modding uses the game’s official workshop, a recognized repository, or a creator with a long verifiable history. Read recent reports, permissions, dependencies, update history, and installation instructions. Back up saves before changing files.

A popular download is not automatically safe. Accounts can be compromised and files can be replaced. Keep the operating system,

launcher, browser, and security tools updated. Avoid pirated software; it removes the normal trust and update path.

Cheats create technical and social risk

Cheating tools may steal passwords, browser cookies, crypto wallets, payment details, or session tokens. Even a tool that contains no malware can lead to bans, loss of purchases, tournament disqualification, team damage, and permanent reputation consequences. "Undetected" usually means "not detected yet," not safe.

Do not allow another person to remote-control your device to install a cheat or "fix" an account. Remote access gives them the ability to see files, saved passwords, messages, and payment information.

Respond before cleaning erases evidence

If you ran a suspicious file, disconnect from sensitive accounts, tell a trusted adult, and use a clean device to change important passwords. Revoke sessions, protect email, scan the device, and contact school or work IT if their account or device was involved.

Do not keep launching the file to test it. Do not pay a stranger who claims they can remove it. If fraud, extortion, or account theft occurred, preserve the file name, source link, messages, and timestamps before a full reset when safe to do so.

Chapter 4 Summary

- Cheats, cracks, free currency, and optimization tools are common malware lures.
- Disabling security or granting unexplained administrator access is a stop sign.
- Safer mods come through a verifiable trust chain.
- Cheating can cost the account, team, purchases, and reputation even without malware.
- After a suspicious installation, protect accounts from a clean device and preserve evidence.

Chapter 4 Safety Checklist

- ☐ Use official stores, workshops, and established repositories.
- ☐ Keep the system and security software updated.

- ☐ Never disable protection for an unknown file.
- ☐ Do not enter credentials into a custom game tool.
- ☐ Back up saves before modding.
- ☐ Refuse remote access from strangers.
- ☐ Use a clean device to secure accounts after suspected malware.

Chapter 4 Discussion Questions

1. Why are cheat tools useful malware lures?
2. What makes a mod source more trustworthy?
3. Why is “undetected” not the same as safe?
4. What should be secured first after running a suspicious file?
5. Which evidence should be saved?

Make It Stick

MEMORY ANCHOR

A FILE THAT NEEDS YOU TO TURN OFF SAFETY IS TELLING YOU WHAT IT IS.

PRESSURE TEST

Your team captain says you will be benched unless you install an unsigned “latency tool” from his private link.

- A.** Install it because the captain is responsible.
- B.** Refuse, preserve the request, and ask the official tournament or team adult to verify the software.
- C.** Use a second computer so the risk does not matter.

SAFEST FIRST MOVE

Choose B. Authority inside a team does not replace an official software source or informed consent.

60-SECOND DRILL

Find the last three game-related files you downloaded. Record the source, publisher, permissions, and whether you still need them.

SAY IT OUT LOUD

I do not disable security or install private tools without independent verification.

CLOSED-BOOK RECALL

1. Name four download red flags.
2. What is a mod trust chain?
3. What is the first account to protect after suspected malware?

CHAPTER 5

Screen Sharing, Devices, Networks, and Location

QUICK RECALL BEFORE YOU READ

What could appear if you shared your entire screen right now: notifications, tabs, names, files, messages, addresses, or account codes?

SCENARIO

During a stream, Noah alt-tabs to answer a message. His email address appears in the browser tab, a school portal notification slides onto the screen, and a shipping confirmation shows his street for two seconds. A viewer clips the moment before Noah notices.

Share the smallest possible surface

Capture a game window or dedicated scene rather than the entire desktop when possible. Use separate browser profiles for gaming and private life. Close email, school portals, cloud drives, password managers, payment pages, and personal chats before sharing.

Create a “panic scene” or blank screen that can replace the capture instantly. Test transitions, overlays, voice channels, alerts, and window capture before going live or presenting in a team call.

Notifications are content

Lock-screen and desktop notifications may expose legal names, message previews, appointment details, codes, addresses, and family conversations. Turn on do-not-disturb, disable previews, and review which apps may display banners. Remember that a phone mirrored to a PC can leak notifications too.

Voice assistants and smart speakers can announce reminders or deliveries. Family members may call a real name from another room. A pre-game household signal reduces accidental disclosure.

Devices need physical boundaries

A strong account can still be compromised through an unlocked phone, shared console, borrowed laptop, or visible PIN. Use a device lock that is not based on a birthday, jersey number, address, or simple pattern. Create separate user profiles for siblings or guests.

Do not save payment methods on a shared device without purchase controls. Sign out on hotel, school, library, event, or borrowed systems. Avoid plugging in unknown USB devices or accessories offered at events.

Networks and location need realistic caution

Public Wi-Fi does not automatically expose everything, but it increases uncertainty and may present fake login portals. Prefer trusted networks, keep devices updated, and avoid sensitive account recovery on an unknown connection. Never install a certificate or management profile because a gaming hotspot asks.

Location may leak through IP-based region estimates, maps, fitness overlays, local server references, team schedules, camera backgrounds, weather, and live posts. Use broad regional language and delay content that reveals where you are now.

Chapter 5 Summary

- Capture only the window or scene needed.
- Notifications, tabs, overlays, and mirrored phones can leak private information.
- Physical device locks and separate profiles protect shared hardware.
- Unknown network portals and profiles deserve caution.
- Location can be inferred from routines, backgrounds, schedules, and regional clues.

Chapter 5 Safety Checklist

- ☐ Build and test a clean game-capture scene.
- ☐ Create a panic or blank scene.
- ☐ Turn off notification previews before sharing.
- ☐ Close private apps and browser tabs.
- ☐ Use separate profiles for guests and gaming.
- ☐ Remove saved payments from shared devices or add purchase controls.

- ☐ Delay location-revealing posts.

Chapter 5 Discussion Questions

1. Why is window capture safer than full-desktop capture?
2. What non-computer device can leak into a stream?
3. How should shared consoles be configured?
4. What should you refuse on an unknown Wi-Fi portal?
5. Which local clues can reveal location?

Make It Stick

MEMORY ANCHOR

CAPTURE THE GAME - NOT THE REST OF YOUR LIFE.

PRESSURE TEST

A tournament asks you to share your full desktop during a remote match.

- A. Share immediately because tournament staff are trusted.
- B. Ask what must be visible, close private material, use a dedicated user profile, and verify the request through official tournament channels.
- C. Refuse every screen-share request.

SAFEST FIRST MOVE

Choose B. Legitimate competition may require monitoring, but the scope should be clear and the device prepared to expose only what is necessary.

60-SECOND DRILL

Turn on screen sharing without starting a call. Scan every visible tab, icon, folder, notification, and overlay as though a stranger were watching.

SAY IT OUT LOUD

I can share the required game and tools, but I need the scope and official process first.

CLOSED-BOOK RECALL

1. What is a panic scene?
2. Name three notification risks.
3. How can location leak without GPS?

PART II

SURVIVE THE SOCIAL LOBBY

A healthy gaming community is designed, moderated, and
allowed to hear no.

CHAPTER 6

Voice Chat Is a Room Full of Strangers

QUICK RECALL BEFORE YOU READ

What information can escape in voice chat even when you never answer a direct personal question?

SCENARIO

Fourteen-year-old Priya joins a ranked squad with two friends. A stranger sounds funny and helpful, so they keep the party together for several matches. By midnight he is asking Priya where she lives, whether her parents are awake, and why she will not turn on her camera in another app.

Voice creates fast false familiarity

Hearing someone laugh, react, and cooperate can make a stranger feel known quickly. Good teamwork is real, but it is not the same as verified identity or earned trust. A person can sound your age, share your interests, and play well while still lying about who they are or what they want.

Treat early voice chat like a public room. Use a gamer tag, avoid school and location details, and do not move into private calls because someone says the platform chat is inconvenient.

Background audio is information

Family members may say names, school plans, appointments, addresses, or work schedules in the background. Television news, church bells, local announcements, weather alerts, and accents may narrow location. A teammate can also record the call without telling you.

Use push-to-talk, a mute key, headphones, and a household signal. Position the microphone away from other rooms. Do not discuss private family conflict or another person's information in a lobby.

Boundaries are not bad teamwork

You can say no to cameras, private calls, late-night sessions, sexual jokes, insults, or questions about your body and relationships. A good teammate

adjusts. A person who punishes boundaries, threatens to throw the match, or calls you disloyal is showing that control matters more to them than teamwork.

Mute and block are game tools, not moral failures. Use them before anger turns into a long argument or disclosure becomes evidence for harassment.

Record and report patterns, not every annoyance

Ordinary trash talk and dangerous conduct are not the same. Prioritize threats, sexual pressure, hate targeting, doxxing clues, repeated contact after blocking, coercion, and attempts to isolate a minor. Save the username, platform ID, match time, lobby or party details, and exact language when safe.

Do not provoke a person to obtain a “better” threat. Leave the room, tell a safe adult, and report through the platform. Immediate threats to physical safety require emergency help.

Chapter 6 Summary

- Voice creates closeness faster than trust can be verified.
- Background audio can reveal names, routines, and location.
- Push-to-talk, mute, and headphones reduce accidental disclosure.
- Healthy teammates respect no.
- Save and report dangerous patterns rather than arguing for more evidence.

Chapter 6 Safety Checklist

- ☐ Use a gamer tag in open voice.
- ☐ Turn on push-to-talk or a reliable mute key.
- ☐ Warn family before important calls.
- ☐ Keep camera and private-call boundaries.
- ☐ Mute or leave when sexual, hateful, or coercive behavior begins.
- ☐ Save identifying details for serious incidents.
- ☐ Tell an adult when someone returns after blocking.

Chapter 6 Discussion Questions

1. Why does voice feel more trustworthy than text?

2. Which background sounds can identify a person?
3. When is mute the strongest response?
4. What conduct should be documented?
5. Why should you not stay to collect a worse threat?

Make It Stick

MEMORY ANCHOR

A GOOD TEAMMATE NEEDS YOUR GAME CALLS - NOT YOUR PRIVATE LIFE.

PRESSURE TEST

A skilled player says he will coach you only through a private late-night video call.

- A. Join because coaching requires trust.
- B. Offer a scheduled, adult-aware call on an official team server with another person present.
- C. Send personal photos first so he knows you are real.

SAFEST FIRST MOVE

Choose B. Legitimate coaching can operate with transparent scheduling, clear scope, and adult awareness.

60-SECOND DRILL

Practice locating the mute, block, leave-party, and report controls in the platform you use most.

SAY IT OUT LOUD

I keep coaching in official team spaces, and another person knows when it happens.

CLOSED-BOOK RECALL

1. What makes voice familiarity misleading?
2. Name two tools that reduce background leaks.
3. What should happen after repeated contact following a block?

CHAPTER 7

Discord, Guilds, Clans, and Private Servers

QUICK RECALL BEFORE YOU READ

Who owns the server, who can see private channels, and what happens when a moderator becomes the problem?

SCENARIO

Eli joins a game server with thousands of members. The public channels seem normal, but a moderator invites him to a hidden “trusted” channel. The moderator asks members to share real photos, download a custom verification file, and keep the channel secret because outsiders “would not understand.”

A server is a privately governed space

Large community platforms provide tools, but server owners and moderators shape daily safety. Read the rules, moderator list, verification method, age expectations, appeal process, and whether private messages are encouraged. A polished server can still be poorly governed.

Notice whether rules apply to moderators, whether harmful behavior is documented, and whether members can report without retaliation. A healthy community does not depend on one charismatic owner who cannot be questioned.

Private channels are not private from the system

“Private” usually means limited to selected members, not invisible to administrators, bots, backups, screenshots, compromised accounts, or platform investigations. Do not place identity documents, intimate material, passwords, recovery codes, or highly sensitive family information in a server.

Bots and integrations may request broad permissions. Do not authorize a bot or application simply because a moderator says it is required. Review what it can read, post, manage, or access.

Use teen-default and family tools without assuming perfection

Discord has expanded teen-default protections and Family Center controls. These may help manage friend requests, server direct messages, message requests, and sensitive-content handling. They reduce exposure but cannot replace judgment, reporting, or adult support.

Review direct-message settings, friend-request permissions, server profiles, connected accounts, and who may add you to groups. Keep unknown DMs in a request lane when available. Leave servers that punish members for using safety settings.

Hidden status is a warning when it demands loyalty

Some private groups are ordinary team spaces. Risk increases when access depends on secrecy from parents, sexual content, humiliating tasks, self-harm, illegal activity, harassment campaigns, or “proof” of loyalty. The group may frame outsiders as weak or dangerous so leaving feels like betrayal.

You do not need permission from the group to leave. Save enough evidence to identify the server and conduct, tell a safe adult, report the content, and avoid announcing a plan that could trigger retaliation.

Chapter 7 Summary

- Servers are governed by people, not only platform rules.
- Private channels can still be logged, copied, or accessed by administrators and compromised accounts.
- Review DM, friend, sensitive-content, and integration settings.
- Bots should receive only necessary permissions.
- Secrecy tied to loyalty, sexual content, harm, or illegal acts is a major warning.

Chapter 7 Safety Checklist

- ☐ Read rules and moderator structure before becoming active.
- ☐ Keep identity documents and recovery information out of servers.
- ☐ Review connected apps and bot permissions.
- ☐ Limit server DMs and friend requests.
- ☐ Use different server profiles when useful.

- ☐ Leave groups that punish safety boundaries.
- ☐ Tell an adult before confronting a dangerous server.

Chapter 7 Discussion Questions

1. What makes a server well governed?
2. Who can access “private” server content?
3. Why are bots a security issue?
4. What makes secrecy different from ordinary team privacy?
5. How should a member exit a dangerous group?

Make It Stick

MEMORY ANCHOR

A PRIVATE CHANNEL IS STILL SOMEONE ELSE’S SYSTEM.

PRESSURE TEST

A moderator says you must install a “verification client” and temporarily disable antivirus to stay in the server.

- A.** Install it because the server is popular.
- B.** Refuse, leave, preserve the request, and report the server or moderator.
- C.** Ask another member to test it first.

SAFEST FIRST MOVE

Choose B. Popularity and moderator status do not make unsafe software trustworthy.

60-SECOND DRILL

Open one large server’s settings. Review direct messages, friend requests, integrations, roles, and the report route.

SAY IT OUT LOUD

I do not install private verification software or share documents in a server.

CLOSED-BOOK RECALL

1. Name two people or systems that may see private-channel content.
2. What teen-safety settings deserve review?
3. What type of secrecy is dangerous?

CHAPTER 8

Online Friendships and Grooming

QUICK RECALL BEFORE YOU READ

Which matters more: whether the profile is real, or whether the behavior respects your boundaries?

SCENARIO

Jordan has played with “Rex” almost every evening for two months. Rex sends rare items, listens after bad school days, and says Jordan is more mature than other fifteen-year-olds. Then Rex asks Jordan to hide the friendship, move to disappearing messages, and prove trust with a private photo.

Gaming friendships can be real

Shared goals, repeated teamwork, humor, and long conversations can create meaningful relationships. Safety guidance should not dismiss those bonds. It should help you judge whether the relationship makes you safer and more connected or more isolated and controlled.

A person can be exactly who they claim and still be manipulative. Identity verification reduces one uncertainty; it does not prove intentions.

Grooming is a pattern of changing access

Grooming may begin with praise, gifts, protection, coaching, or intense understanding. The person notices loneliness, conflict, money needs, identity questions, or ambition. They then create special access, move contact into private spaces, introduce sexual or degrading material, and use guilt or threats to maintain control.

Common lines include “mature for your age,” “your family would not understand,” “do not tell the team,” and “after everything I gave you.” Gifts do not create a debt of access.

Break isolation early

Tell a trusted person about important online relationships before a crisis. Keep early contact on platforms with reporting tools. Avoid sharing home address, school schedule, identity documents, live location, private photos, or financial accounts.

If something feels wrong, you do not need to prove grooming before asking for help. Show the messages and say, "I feel pressured and I need another person to look at this."

Do not run a private investigation

Do not continue sexual conversations, arrange a secret meeting, threaten the person, or ask friends to trap them. Save account details and relevant messages, involve a safe adult, and report suspected sexual exploitation of a minor to NCMEC's CyberTipline in the United States.

If the person knows your address or schedule, make a safety plan before blocking. The safest order may depend on the threat, relationship, and whether law enforcement needs evidence.

Chapter 8 Summary

- Online friendships can be genuine and still require boundaries.
- Behavior matters more than a convincing profile.
- Grooming often uses gifts, isolation, secrecy, sexualization, and control.
- Breaking secrecy early creates options.
- Do not investigate a suspected exploiter alone.

Chapter 8 Safety Checklist

- ☐ At least one trusted person knows my important online friendships.
- ☐ Keep early contact on reportable platforms.
- ☐ Do not share address, schedule, ID, or live location.
- ☐ Treat conditional gifts as pressure.
- ☐ Ask for help before I can prove intent.
- ☐ Preserve account links and relevant messages.
- ☐ Use the CyberTipline for suspected child sexual exploitation.

Chapter 8 Discussion Questions

1. Why can gaming friendships become emotionally intense?
2. What does "mature for your age" often try to justify?
3. How do gifts become leverage?
4. Why should a teen not investigate alone?
5. What should happen before blocking someone who knows an address?

Make It Stick

MEMORY ANCHOR

REAL FRIENDSHIP CAN SURVIVE A BOUNDARY AND A TRUSTED ADULT KNOWING.

PRESSURE TEST

An older teammate threatens to take back gifted items and ruin your reputation unless you move to a secret app.

- A. Move the conversation so the gifts are not lost.
- B. Save the threats, tell a trusted adult, stop private contact, and report.
- C. Threaten to expose the teammate first.

SAFEST FIRST MOVE

Choose B. The gifts are being used as leverage. Preserving evidence and breaking isolation reduces control.

60-SECOND DRILL

Write the names of three people who could review a concerning conversation without humiliating you.

SAY IT OUT LOUD

I am not sure what this is, but I feel pressured. Please look at the messages with me.

CLOSED-BOOK RECALL

1. Name four grooming tactics.
2. Why does verification not equal safety?
3. What reporting resource handles suspected exploitation of a minor in the United States?

CHAPTER 9

Sexual Pressure, Sextortion, and Image Abuse

QUICK RECALL BEFORE YOU READ

What are the first four moves after an intimate-image threat? Stop, save, tell, report.

SCENARIO

After a flirty conversation in a game chat, Sam sends a private image to someone who claimed to be sixteen. The person immediately threatens to post it in Sam's guild, school server, and family contacts unless Sam pays and sends more. A countdown begins.

The pressure is designed to create panic

Sextortion relies on shame, urgency, and isolation. The offender may threaten followers, friends, family, school, or team members. They may show screenshots of contact lists or claim that sending money will permanently delete the material.

Do not pay, send more images, provide account access, or negotiate. Payment often leads to further demands because it proves fear and access to money.

Use STOP - SAVE - TELL - REPORT

Stop replying. Save usernames, profile links, threats, dates, payment requests, and report confirmations without downloading or forwarding sexual material. Tell a usable adult immediately. Report the account to the platform and suspected exploitation of a minor to NCMEC's CyberTipline in the United States.

If an image was taken before age eighteen and remains on the original device, NCMEC's Take It Down service may help create a digital fingerprint without the image leaving the device.

Protect the person before the evidence

Sextortion can create intense fear, humiliation, and suicidal thinking. Do not leave the victim alone with the threats. Ask directly whether they feel safe and whether they are thinking about hurting themselves. Contact 988 in the United States for a mental-health crisis and 911 for immediate danger.

A calm adult response should begin: "I am glad you told me. You are not in trouble for asking for help. We will handle one step at a time."

Synthetic images still cause real harm

AI can create fake sexual images of a real person. The image being fake does not make the threat, humiliation, or distribution harmless. Preserve links, usernames, dates, and screenshots that do not unnecessarily redistribute the material. Report it through platform removal systems and involve adults and authorities as appropriate.

Do not circulate the image to prove it exists. Each additional copy increases harm and may create legal or school-policy consequences.

Chapter 9 Summary

- Sextortion uses panic, shame, deadlines, and isolation.
- Do not pay or send more material.
- Stop, save, tell, and report.
- Take It Down may help with eligible images created before age eighteen.
- Ask directly about immediate emotional safety.
- Fake intimate images cause real harm and should not be redistributed.

Chapter 9 Safety Checklist

- ☐ Memorize STOP - SAVE - TELL - REPORT.
- ☐ Know three adults I can contact at any hour.
- ☐ Save account and threat details without forwarding images.
- ☐ Use the CyberTipline and platform reports.
- ☐ Use Take It Down when eligible.
- ☐ Ask about self-harm risk.
- ☐ Contact 988 or 911 when needed.

Chapter 9 Discussion Questions

1. Why does payment often fail to end sextortion?
2. What evidence can be saved safely?
3. What should an adult say first?
4. How does Take It Down work at a high level?
5. Why should fake sexual images not be forwarded?

Make It Stick

MEMORY ANCHOR

STOP CONTACT. SAVE THE TRAIL. TELL AN ADULT. REPORT THE OFFENDER.

PRESSURE TEST

The offender says the image goes public in five minutes unless you pay with gift cards.

- A. Pay to buy time.
- B. Stop responding, get an adult, preserve the threat, secure accounts, and report.
- C. Delete every account immediately.

SAFEST FIRST MOVE

Choose B. Payment and panic deletion reduce options. Adult support, evidence, account security, and reporting create them.

60-SECOND DRILL

Add the CyberTipline, Take It Down, 988, and local emergency number to a written safety card.

SAY IT OUT LOUD

I am being threatened with private material. Stay calm and help me save evidence and report it.

CLOSED-BOOK RECALL

1. What four actions form the memory anchor?
2. Why should you not pay?
3. Which resource is for immediate mental-health crisis in the United States?

CHAPTER 10

Toxicity, Harassment, Dogpiles, and Hate

QUICK RECALL BEFORE YOU READ

Which responses reduce harm: arguing, limiting access, preserving serious evidence, or recruiting friends to attack back?

SCENARIO

Kai misses a final shot in a tournament. A clip spreads, and hundreds of people flood his profile with insults. Some comments are ordinary criticism; others target his race, send violent images, and contact his younger sister. Kai tries to answer every post and stays awake until morning.

Not every negative comment needs the same response

Criticism, trash talk, harassment, hate, and threats are different. A player can dislike your performance without losing the right to speak. Repeated targeting, identity-based abuse, sexual harassment, impersonation, contact with family, and threats require stronger action.

Sort instead of absorbing everything as one mass. Ignore or mute low-value bait. Correct important false claims once if necessary. Document and report targeted abuse and threats.

Attention can feed the pile-on

Public arguments provide new screenshots, clips, and emotional reactions. Replying to hundreds of accounts turns the attacker's schedule into yours. Use comment filters, limited replies, follower-only modes, slow mode, moderator help, blocked keywords, and temporary account restrictions.

A pause is not surrender. It is control over the conditions in which you respond.

Protect bystanders and family

Harassers may contact relatives, teammates, school accounts, sponsors, or employers to widen pressure. Warn people privately, lock down public

profiles, remove identifying links, and ask them not to engage. Preserve messages that show coordination or threats.

Do not send followers to retaliate. A counter-dogpile can harm uninvolved people, violate platform rules, and make evidence harder to interpret.

Recovery includes the nervous system

A dogpile can create constant alertness, nausea, anger, shame, and fear of opening the app. Limit notification exposure, hand evidence collection to a trusted person, sleep, eat, move, and reconnect with people who know the full you.

If harassment triggers thoughts of self-harm or immediate danger, use crisis and emergency support. The goal is not to prove you can withstand unlimited abuse.

Chapter 10 Summary

- Sort criticism, bait, harassment, hate, and threats instead of reacting to all alike.
- Limiting access is often stronger than public arguing.
- Protect family and teammates without recruiting retaliation.
- Preserve evidence of coordinated abuse and threats.
- Recovery requires reduced exposure and offline support.

Chapter 10 Safety Checklist

- ☐ Use filters, slow mode, mute, and block.
- ☐ Save serious threats and identity-based abuse.
- ☐ Warn affected family or teammates privately.
- ☐ Do not send followers to attack back.
- ☐ Let a trusted person help review evidence.
- ☐ Take a planned notification break.
- ☐ Use crisis support when safety is affected.

Chapter 10 Discussion Questions

1. How is criticism different from harassment?
2. Why can replying feed a dogpile?
3. What should family members be told?

4. Why is counter-harassment unsafe?
5. What physical reactions can online harassment cause?

Make It Stick

MEMORY ANCHOR

YOU DO NOT HAVE TO READ EVERY HIT TO PROVE YOU ARE STRONG.

PRESSURE TEST

A clip goes viral and strangers flood your messages with insults and one specific death threat.

- A. Answer everyone so silence does not look guilty.
- B. Limit messages, save the specific threat, tell an adult, and report it.
- C. Ask followers to find the person.

SAFEST FIRST MOVE

Choose B. Access controls reduce volume while evidence and adult support address the highest-risk message.

60-SECOND DRILL

Set up one blocked-keyword filter and locate the platform's message-limit or follower-only controls.

SAY IT OUT LOUD

I am not discussing this in a pile-on. Serious threats are being documented and reported.

CLOSED-BOOK RECALL

1. What should be ignored, and what should be documented?
2. Why should followers not retaliate?
3. What is one recovery action away from the screen?

CHAPTER 11

Doxxing, Swatting, Stalking, and Violent Online Networks

QUICK RECALL BEFORE YOU READ

What changes when an online threat includes a real address, physical surveillance, emergency services, or coercion to harm yourself or others?

SCENARIO

After an argument, a player posts what appears to be Taylor's home address and says police will arrive before the next match. Another account begins sending photos from near Taylor's school. A private group invites Taylor in, claiming they can "protect" her if she completes humiliating tasks and stops talking to adults.

Doxxing turns information into pressure

Doxxing is the publication or threatened publication of identifying information to intimidate, harass, or enable harm. The information may be accurate, outdated, or partly wrong; all versions can create danger. Save the post, URL, username, time, and any connected threats. Do not debate the address publicly.

Tell household members and a safe adult. Lock down linked accounts, remove exposed details where possible, and report to the platform. Contact local law enforcement when threats or physical risk are present.

Swatting is an emergency, not a prank

Swatting uses a false emergency report to trigger an armed law-enforcement response. The FBI describes it as a serious crime with potentially dangerous consequences. If a credible threat mentions swatting, involve an adult and contact local law enforcement through a non-emergency route when safe to ask about a safety plan.

If officers arrive, follow commands, keep hands visible, and do not run to record content. Family members should understand the plan. Do not post tactical details that could help the offender adapt.

Stalking patterns matter

Repeated new accounts, location references, unwanted gifts, tracking, photos near real-world places, or contact after blocking can indicate stalking. Preserve the timeline. Review location sharing, fitness apps, public schedules, data-broker listings, trackers, and shared accounts.

Do not meet or confront the person. A threat-assessment professional, school safety officer, domestic-violence resource, or law enforcement agency may help determine the safest next step.

Violent online networks use coercion and spectacle

The FBI has warned about violent online networks, often discussed under labels such as “764,” that target minors and vulnerable people through gaming and social platforms, build trust, and coerce victims into sexual, violent, humiliating, or self-harming acts. Group names change; the tactics matter more than the label.

Warning signs include demands for escalating “proof,” threats to expose private material, glorification of cruelty, instructions to harm yourself, animals, or others, and attempts to separate you from adults. Do not comply to buy safety. Break isolation, preserve evidence, and contact emergency or specialized authorities.

Chapter 11 Summary

- Doxxing should be documented without debating the information publicly.
- Swatting threats require adult and law-enforcement safety planning.
- Stalking is a pattern of unwanted access and real-world references.
- Do not confront or meet a suspected stalker.
- Violent networks may coerce minors into sexual, violent, or self-harming acts.
- Immediate danger requires emergency response.

Chapter 11 Safety Checklist

- ☐ Save URLs, usernames, timestamps, and exact threats.
- ☐ Tell household members and a usable adult.
- ☐ Contact local law enforcement about credible swatting or physical threats.
- ☐ Review location and shared-account exposure.
- ☐ Do not post the family response plan publicly.

- ☐ Do not complete coercive tasks.
- ☐ Use 911 for immediate danger and 988 for emotional crisis in the United States.

Chapter 11 Discussion Questions

1. Why should an exposed address not be debated publicly?
2. What is swatting?
3. Which behaviors suggest stalking?
4. Why do violent groups demand escalating proof?
5. What is the first goal when coercion depends on secrecy?

Make It Stick

MEMORY ANCHOR

WHEN THE THREAT CROSSES INTO THE PHYSICAL WORLD, BRING IN REAL-WORLD HELP.

PRESSURE TEST

Someone posts your address and says a SWAT team is already on the way.

- A.** Go live to prove where you are.
- B.** Tell an adult immediately, call emergency services or local law enforcement as appropriate, preserve the threat, and follow safety instructions.
- C.** Threaten to swat them back.

SAFEST FIRST MOVE

Choose B. Public performance and retaliation increase danger. Real-world coordination is the priority.

60-SECOND DRILL

Write the non-emergency number for local law enforcement and the household plan for an unexpected police response.

SAY IT OUT LOUD

My address was posted with a threat. We need to contact law enforcement and follow a safety plan now.

CLOSED-BOOK RECALL

1. What evidence should be preserved after doxxing?
2. Why should the response plan stay private?
3. What tactics identify a coercive violent network?

PART III

PROTECT YOUR MONEY AND INVENTORY

Virtual goods may be pixels, but the money, pressure, fraud, and consequences are real.

CHAPTER 12

Virtual Currency, Skins, and Spending

QUICK RECALL BEFORE YOU READ

Can you state the real-dollar cost of the last in-game item you bought without opening a calculator?

SCENARIO

Mia buys a \$10 currency pack to get a limited skin. The game converts dollars into gems, adds a bonus amount, and leaves a small balance. Over the next week she makes several “tiny” purchases because the remaining gems never match the item prices. Her family later finds more than \$180 in charges.

Conversion hides the real price

Coins, gems, points, credits, and bundles separate the decision from real money. Bonus currency and awkward package sizes make comparison harder. Before buying, translate the full purchase into dollars, including tax, fees, and leftover currency.

Do not treat leftover virtual currency as free money. It is often designed to pull the next purchase forward.

Fast purchase paths weaken the pause

Saved cards, one-click checkout, countdowns, rotating shops, and “last chance” banners reduce the time available to reconsider. Add friction on purpose: require a PIN, remove saved payment methods, use a written monthly budget, and wait before unplanned purchases.

A purchase pause is not punishment. It protects the difference between wanting an item and being pushed into acting now.

Ownership may be limited

Many virtual items are licensed for use inside an account rather than owned like a physical object. The platform may restrict transfer, resale, refunds, or access after a ban. Items can lose value when a game changes, closes, or updates its economy.

Read the purchase and refund terms for high-value transactions. Never spend money you need for food, transport, school, bills, or agreed savings.

Make spending visible without shame

Hiding purchases increases risk. Track the real amount, date, item, and reason. Parents should respond to an overspend by securing payment methods and reviewing the design and decision process before turning the conversation into humiliation.

A teen who can disclose a mistake early gives the family more time to request refunds, stop fraud, or adjust controls.

Chapter 12 Summary

- Virtual currency makes real cost harder to feel.
- Leftover balances and bundles encourage additional purchases.
- Purchase friction creates decision time.
- Virtual items may not be transferable or permanent.
- Visible tracking and calm disclosure improve recovery.

Chapter 12 Safety Checklist

- ☐ Convert virtual prices to real dollars.
- ☐ Set a monthly entertainment budget.
- ☐ Require a purchase PIN.
- ☐ Remove unnecessary saved payment methods.
- ☐ Wait before unplanned limited-time purchases.
- ☐ Save receipts.
- ☐ Tell an adult quickly about mistaken or unauthorized charges.

Chapter 12 Discussion Questions

1. Why do games convert money into currency?
2. How do leftover balances influence behavior?
3. What rights may be limited for virtual items?
4. Which purchase controls add useful friction?
5. What adult response encourages early disclosure?

Make It Stick

MEMORY ANCHOR

IF THE PRICE IS HARD TO SEE, SLOW DOWN UNTIL IT IS REAL MONEY AGAIN.

PRESSURE TEST

A bundle disappears in eight minutes and costs nearly your entire monthly budget.

- A.** Buy it because the timer proves rarity.
- B.** Wait, calculate the full cost, and accept that missing one item is safer than breaking the budget.
- C.** Borrow a friend's account to purchase it.

SAFEST FIRST MOVE

Choose B. Scarcity pressure is part of the sales design. A budget only works when it survives a countdown.

60-SECOND DRILL

Convert three store items from virtual currency into real dollars and write the leftover balance each package creates.

SAY IT OUT LOUD

I do not make money decisions while a timer is making them for me.

CLOSED-BOOK RECALL

1. Why is leftover currency not free?
2. Name two ways to add purchase friction.
3. What should happen after an unauthorized charge?

CHAPTER 13

Loot Boxes, Gacha, and Gambling-Like Design

Where Game Spending Becomes Real-Money Gambling

Not every randomized reward is legally classified as gambling, and laws vary. The practical risk changes when an item can be sold, wagered, converted to money, used on a third-party betting site, or entered into a paid chance-based contest.

Keep these categories separate:

- Game spending: buying a known item, subscription, battle pass, or currency.
- Gambling-like design: paying for a randomized result, streak, spin, pack, or chance.
- Skin betting or third-party casinos: wagering items or value outside the game.
- Paid wager matches: staking money or items on the result of play.
- Speculation: buying items mainly because someone promises their resale value will rise.

A platform label does not settle the legal question. Minors should not use gambling or betting services, should not bypass age checks, and should involve a parent or qualified adult before any real-money wager, item-cash-out system, or prize arrangement.

QUICK RECALL BEFORE YOU READ

Does a previous loss make the next random reward more likely? Usually, no.

SCENARIO

Owen wants one rare character. Each pull is inexpensive, and a friend gets the character on the first try. Owen keeps buying because he believes the next pull is "due." By the time the guaranteed reward appears, he has spent more than the price of a new console game.

Random rewards change the decision

Loot boxes and gacha systems exchange money or earned currency for uncertain rewards. The excitement comes from not knowing what will appear. The FTC has noted concerns about young players tracking real costs and understanding the odds of obtaining desired items.

Treat randomized purchases as entertainment spending, not a strategy for obtaining value. The rare item shown in advertising may be unlikely, and duplicates may have little practical worth.

The brain searches for patterns that are not there

Near misses, streaks, colorful reveals, social comparison, and stories of lucky pulls can create the feeling that a win is close. Unless the game clearly uses a published pity or guarantee system, previous outcomes usually do not change the next independent chance.

Even with a guarantee, calculate the maximum real-dollar cost needed to reach it. "Guaranteed eventually" can still mean unaffordable.

Set limits before the first pull

Decide the maximum number of pulls or dollars before opening the store. Do not chase losses, borrow money, hide purchases, or sell important items to continue. Use platform spending limits and purchase approvals where appropriate.

A safer option is to budget only for a directly priced item or to play without paid random rewards.

Know the warning signs

Risk is increasing when a player lies about spending, feels compelled to recover losses, becomes distressed when unable to purchase, uses family payment methods secretly, or continues despite serious consequences. These signs deserve a calm conversation and stronger controls.

Professional support may be appropriate when gambling-like behavior affects money, sleep, school, relationships, or mental health. The label matters less than the harm pattern.

Chapter 13 Summary

- Randomized rewards sell uncertainty, not a guaranteed item.
- Past losses do not usually make the next pull "due."

- Published guarantees still need a maximum-cost calculation.
- Limits should be set before entering the purchase loop.
- Secrecy, chasing losses, and serious consequences are warning signs.

Chapter 13 Safety Checklist

- ☐ Read the odds and guarantee rules.
- ☐ Calculate the maximum real cost.
- ☐ Set a pull and dollar limit in advance.
- ☐ Do not chase losses.
- ☐ Use spending approvals or limits.
- ☐ Track duplicates and total spending.
- ☐ Seek adult or professional help when behavior becomes compulsive.

Chapter 13 Discussion Questions

1. Why do random reveals feel exciting?
2. What is the “due” mistake?
3. How should pity systems be evaluated?
4. Which signs show that spending is becoming harmful?
5. What directly priced alternative may be safer?

Make It Stick

MEMORY ANCHOR

RANDOM REWARDS DO NOT OWE YOU A WIN.

PRESSURE TEST

You have already spent \$40 and the next ten-pull guarantees a higher rarity, but not the item you want.

- A.** Spend more because stopping wastes the first \$40.
- B.** Stop at the preset limit; previous spending is already gone and does not justify more.
- C.** Use someone else’s payment method and repay it later.

SAFEST FIRST MOVE

Choose B. Past spending is a sunk cost. The safest decision is based on what the next purchase costs and can actually deliver.

60-SECOND DRILL

Choose one randomized system you use. Find the published odds and calculate the maximum cost of its guarantee, if one exists.

SAY IT OUT LOUD

Past losses do not decide my next purchase. My limit does.

CLOSED-BOOK RECALL

1. What is a sunk cost?
2. Why can a guarantee still be unsafe?
3. Name two warning signs of harmful purchase behavior.

CHAPTER 14

Trades, Marketplaces, Giveaways, and Fake Support

QUICK RECALL BEFORE YOU READ

What is the safest place to confirm a trade or payment: a screenshot, a message link, or the official app opened independently?

SCENARIO

A buyer offers Zane twice the market price for a rare skin. The buyer says the official marketplace is broken and sends a “verification” link. The page looks identical to the launcher login. After Zane signs in, the buyer removes his authenticator and transfers the inventory.

A deal can be bait for the account

High offers, urgent buyers, fake middlemen, impersonated friends, and “verification” links are common ways to steal credentials or items. The attacker may use a real-looking profile or a compromised account with history.

Open the official marketplace or app yourself. Do not trust a login page reached through chat, a QR code from a stranger, or a screen-share instruction.

Screenshots are not proof

Payment, inventory, trade-confirmation, and support screenshots can be edited. Confirm the transaction inside the official account. Check item names, quantities, recipient IDs, hold periods, fees, and whether the offer changed during confirmation.

Slow down at the final approval screen. Scammers often rely on the player reading the conversation but not the actual transaction.

Giveaways and support impersonation use authority

Real companies do not need your password, verification code, remote desktop, or a payment to release a prize. A giveaway that requires

deposits, gift cards, cryptocurrency, recruitment, or “tax” paid to a private account is a warning.

Support agents should be reached through the official site. A profile badge, staff-like name, or server role can be copied or abused.

Off-platform trading removes protections

Moving outside the authorized marketplace may violate rules and remove dispute systems. Account selling and real-money trading can expose payment details, identity information, and the entire account.

If a scam occurs, preserve trade IDs, account links, payment records, and messages. Secure email and sessions, contact the platform, and notify the payment provider quickly. Recovery is not guaranteed, but delay reduces options.

Chapter 14 Summary

- Unusually favorable offers can be account-theft bait.
- Confirm trades and payments inside the official app.
- Screenshots and roles are not proof.
- Legitimate support does not require passwords or codes.
- Off-platform trading can remove protections and violate rules.
- Fast reporting improves recovery options.

Chapter 14 Safety Checklist

- ☐ Use only authorized trade systems.
- ☐ Open official apps independently.
- ☐ Read the final confirmation carefully.
- ☐ Never share verification codes.
- ☐ Reject remote-access requests.
- ☐ Save trade and payment IDs.
- ☐ Contact the platform and payment provider quickly after fraud.

Chapter 14 Discussion Questions

1. Why do scammers overpay?
2. What should be checked on the final trade screen?
3. Why are staff badges not enough?

4. What protections disappear off-platform?
5. Which records help after a scam?

Make It Stick

MEMORY ANCHOR

THE DEAL IS NOT REAL UNTIL THE OFFICIAL SYSTEM SAYS IT IS.

PRESSURE TEST

A "platform moderator" says your items are duplicated and must be transferred to a safe account for inspection.

- A. Transfer them because moderators can ban accounts.
- B. Stop, open official support independently, and report the impersonator.
- C. Send one low-value item as a test.

SAFEST FIRST MOVE

Choose B. Legitimate platform support does not inspect inventory by asking users to transfer it to a private account.

60-SECOND DRILL

Practice opening your trade history, payment history, support page, and active sessions without using a message link.

SAY IT OUT LOUD

I verify trades and support through the official account, not through chat.

CLOSED-BOOK RECALL

1. Why is a screenshot not payment proof?
2. What information should never go to support in chat?
3. What is the first account to secure after a trade-phishing theft?

CHAPTER 15

Account Selling, Boosting, Cheating, and Bans

QUICK RECALL BEFORE YOU READ

What do you give up when another person logs into your account: control, privacy, rule compliance, and recovery certainty.

SCENARIO

Nora pays a booster to raise her competitive rank. The booster asks for full account access and promises the login is safe. Two weeks later the account is banned for cheating, the payment is gone, and the booster threatens to leak Nora's messages unless she pays again.

Account access is broader than the game

A booster or buyer may see linked email hints, friends, messages, purchases, saved payment methods, region, account history, and other connected services. They may change recovery details, copy personal information, or use the account to scam others.

Never share an account password. If a legitimate coach needs to review play, use recordings, spectator tools, or supervised sessions that do not transfer control.

Rule-breaking creates delayed consequences

Cheating, boosting, account sharing, botting, smurfing, and account sales may violate game or tournament rules. Detection can occur later, after purchases and team results have accumulated. Penalties may include item loss, rank reversal, hardware restrictions, team disqualification, or permanent bans.

"Everyone does it" does not transfer the consequences to everyone else. The account owner is often the person who loses access.

Black markets create leverage

Unauthorized services cannot rely on formal dispute systems, so they may use reputation, threats, stolen accounts, fake reviews, or chargeback

fraud. A seller may recover an account after payment. A buyer may use a stolen payment method.

Once private messages show rule-breaking, the other person can use them for extortion. Do not pay to keep misconduct secret; involve an adult and preserve the threat.

Appeals work best with honesty and evidence

If an account is restricted, use the official appeal path. Provide dates, account identifiers, relevant security history, and a concise explanation. Do not buy an “unban service,” flood support, forge evidence, or threaten staff.

An appeal may fail. Recovery includes learning which behavior, security gap, or association created the risk and building a clean plan for future play.

Chapter 15 Summary

- Sharing credentials gives another person control over far more than rank.
- Cheating and boosting consequences may arrive later.
- Unauthorized markets create fraud and extortion leverage.
- Do not pay to keep misconduct secret.
- Official appeals require concise, honest evidence.

Chapter 15 Safety Checklist

- ☐ Never share account credentials.
- ☐ Use recordings or spectator tools for coaching.
- ☐ Read team and game rules before competitive play.
- ☐ Avoid account sales and unauthorized boosting.
- ☐ Preserve extortion messages.
- ☐ Use the official appeal system.
- ☐ Build a clean restart plan if access is not restored.

Chapter 15 Discussion Questions

1. What can a booster access besides gameplay?
2. Why can bans be delayed?
3. How do unauthorized markets enforce deals?

4. What should happen after an extortion threat?
5. What makes an appeal credible?

Make It Stick

MEMORY ANCHOR

NO RANK IS WORTH HANDING A STRANGER THE KEYS TO YOUR ACCOUNT.

PRESSURE TEST

A teammate offers a free boost if you provide the login for one night.

- A. Accept because no money is involved.
- B. Refuse and use coaching or review methods that do not transfer account access.
- C. Change the password afterward.

SAFEST FIRST MOVE

Choose B. Temporary access can still steal sessions, recovery information, inventory, and reputation.

60-SECOND DRILL

Review the game and tournament rules for account sharing, boosting, mods, and third-party software.

SAY IT OUT LOUD

You can review my gameplay, but no one else logs into my account.

CLOSED-BOOK RECALL

1. Why does changing the password later not remove all risk?
2. What is one safe coaching alternative?
3. What should an official appeal include?

CHAPTER 16

Sponsorships, Creator Codes, Coaching, and Opportunities

QUICK RECALL BEFORE YOU READ

Which adult should review a teen's sponsorship, coaching agreement, tournament contract, or paid promotion before acceptance?

SCENARIO

A company contacts sixteen-year-old Ben after an esports clip performs well. It offers free gear and a creator code but requires him to pay shipping, install a browser extension, sign a contract immediately, and promote a gambling-style skin site without telling viewers that he is paid.

Opportunity language can hide ordinary scams

Fake brands, teams, coaches, and agencies target ambition. Warning signs include payment before work, checks with instructions to send money onward, gift-card purchases, remote-control software, credential requests, and domains that imitate a known company.

Verify through contact information found independently. Search the organization, representative, address, and contract terms. A real deadline can tolerate adult review.

A gift may create legal and audience obligations

Free gear, game currency, travel, commissions, affiliate links, and creator codes can be compensation. Paid relationships should be disclosed clearly and in a way the audience can notice. A teen should not be pressured to hide sponsorship or present advertising as an independent opinion.

The parent or guardian may need to handle contracts, payment, taxes, and platform monetization requirements. Keep records of what was received and what the creator promised.

Coaching needs boundaries and qualifications

A coach should explain the service, schedule, communication channel, price, refund terms, and safeguarding rules. For minors, parents should

know when sessions occur. Private late-night calls, sexual comments, requests for secrecy, and unrestricted device access are not normal coaching requirements.

Team authority does not justify humiliation, threats, body comments, or control over a player's private relationships.

Some offers are simply not appropriate for minors

Gambling, wagering, adult content, unsafe supplements, deceptive financial products, and age-restricted services may create legal, platform, and ethical problems. The money does not make the audience fit.

A sustainable gaming career protects long-term trust. Declining one offer can be more valuable than earning from a promotion that harms viewers or the player's reputation.

Chapter 16 Summary

- Ambition makes fake opportunities believable.
- Verify organizations through independent contact routes.
- Gifts, affiliate income, and creator codes may require disclosure and records.
- Teen contracts and payments need adult review.
- Coaching requires transparent boundaries.
- Some products are not appropriate for a minor audience.

Chapter 16 Safety Checklist

- ☐ Route offers through an adult business contact.
- ☐ Verify the sender and domain independently.
- ☐ Do not pay to receive a job or sponsorship.
- ☐ Never install extensions or remote access for a deal.
- ☐ Disclose paid relationships clearly.
- ☐ Keep contracts, invoices, and payment records.
- ☐ Reject age-inappropriate or deceptive promotions.

Chapter 16 Discussion Questions

1. Which scam patterns appear in sponsorship offers?
2. What counts as compensation?
3. Why should a real deadline allow adult review?

4. What makes coaching boundaries safe?
5. Why can declining a deal protect future value?

Make It Stick

MEMORY ANCHOR

A REAL OPPORTUNITY CAN SURVIVE VERIFICATION, ADULT REVIEW, AND A CLEAR DISCLOSURE.

PRESSURE TEST

A sponsor says the deal disappears in one hour unless you sign and install its tracking extension.

- A. Sign because early creators must move fast.
- B. Pause, verify the company independently, and have an adult review the contract and software request.
- C. Install the extension first and read the contract later.

SAFEST FIRST MOVE

Choose B. Urgency and software access are risk signals. A legitimate deal can explain both in writing.

60-SECOND DRILL

Create a sponsorship checklist with sender domain, company verification, deliverables, payment, disclosure, data access, and adult approval.

SAY IT OUT LOUD

I do not sign, install, or promote until the company and terms are independently reviewed.

CLOSED-BOOK RECALL

1. Name three fake-opportunity warning signs.
2. What forms of compensation need records?
3. What coaching behavior is never justified by team authority?

PART IV

COMPETE WITHOUT LOSING YOURSELF

Performance matters, but the player must survive the schedule,
the pressure, and the scoreboard.

CHAPTER 17

Esports Teams, Coaches, and Safe Competition

Team Safeguarding Standards

A legitimate youth team should be able to explain who supervises adults, how communication is recorded, how travel is handled, and where a player reports misconduct without retaliation.

Minimum safeguards include:

- parent-visible schedules, rosters, travel plans, prize terms, and coach contact information;
- no secret one-on-one late-night communication between an adult coach and a minor;
- two-adult or parent-visible communication practices when practical;
- reference, screening, or background-check practices appropriate to the organization and jurisdiction;
- written room, transportation, supervision, photography, and emergency rules for travel;
- an anti-retaliation route for reporting harassment, exploitation, discrimination, or financial misconduct;
- written prize, sponsorship, ownership, and payment records.

A team that refuses basic safeguarding questions is giving you useful information before you join.

QUICK RECALL BEFORE YOU READ

What should a safe team make clear in writing: roles, communication, practice, conduct, reporting, travel, money, and adult supervision?

SCENARIO

Seventeen-year-old Tori joins a serious amateur esports team. The coach controls the roster, private server, practice schedule, and introductions to scouts. He begins holding one-on-one calls after midnight, insults players who ask for breaks, and says parents should stay out because “real competitors handle their own careers.”

A team needs governance, not only talent

A strong roster is not a safety system. Teams should identify the owner, coach, manager, safeguarding contact, code of conduct, discipline process, appeal route, and who handles money and travel. Minors need an adult outside the direct coaching chain who can receive concerns.

When one person controls selection, communication, payment, and complaints, players may feel that speaking up will end their opportunity. Separate authority where possible.

Coaching should have a defined lane

Coaches may review gameplay, plan strategy, set practice expectations, and give performance feedback. They do not need unrestricted private access, passwords, sexual information, humiliating punishments, or control over a player's dating, family, and school life.

For minors, use scheduled sessions, official team channels, visible calendars, and parent-aware communication. Recordings or another adult present can protect both the player and coach when appropriate and lawful.

Pressure does not excuse abuse

Competitive environments use direct feedback, but cruelty is not a performance method. Threats, slurs, sexual comments, forced sleep deprivation, public humiliation, retaliation for reporting, and demands to play through illness are warning signs.

A coach who says abuse is proof of seriousness is training obedience, not resilience.

Know what the team owns

Clarify ownership of accounts, content, prize money, sponsorship income, equipment, uniforms, travel deposits, and team-created intellectual property. Never let a team register your primary game or email account in its name.

A teen and parent should keep copies of agreements, schedules, payment records, and communications. Verbal promises become difficult to enforce when the roster changes.

Chapter 17 Summary

- Talent does not replace governance.
- Minors need a reporting route outside the coach who controls selection.
- Coaching should stay within a defined performance lane.
- Competitive pressure does not excuse abuse or sleep deprivation.
- Account, prize, content, and equipment ownership should be written.

Chapter 17 Safety Checklist

- ☐ Identify the team owner, coach, manager, and safety contact.
- ☐ Use official team communication channels.
- ☐ Keep parents aware of minor coaching sessions.
- ☐ Save team rules and agreements.
- ☐ Clarify prize and account ownership.
- ☐ Report retaliation or abusive conduct.
- ☐ Keep the primary email and account under family control.

Chapter 17 Discussion Questions

1. Why should reporting be separate from roster control?
2. What access does a coach legitimately need?
3. How is direct feedback different from humiliation?
4. Which ownership terms need writing?
5. What records should a family keep?

Make It Stick

MEMORY ANCHOR

A TEAM SHOULD BUILD YOUR SKILL - NOT REQUIRE CONTROL OF YOUR PRIVATE LIFE.

PRESSURE TEST

A coach says private midnight calls are mandatory and parents may not know what is discussed.

- A.** Comply to protect the roster spot.

B. Tell a parent or safeguarding contact, save the requirement, and request scheduled official-channel coaching.

C. Record the coach secretly and post it publicly.

SAFEST FIRST MOVE

Choose B. Secret one-on-one access and retaliation pressure are safeguarding problems that should be handled through adults and team governance.

60-SECOND DRILL

Write the names of the team owner, coach, organizer, and one person outside the coaching chain who can receive a concern.

SAY IT OUT LOUD

I can participate in scheduled coaching, but private secret calls are not part of my agreement.

CLOSED-BOOK RECALL

1. What power concentration creates risk?
2. Name two legitimate coaching activities.
3. What must remain under the player or family's control?

CHAPTER 18

Tournaments, Travel, LAN Events, and Meeting Online Friends

QUICK RECALL BEFORE YOU READ

What must be verified before travel: organizer, venue, supervision, transport, lodging, emergency plan, money, and return route?

SCENARIO

Andre's online squad qualifies for an out-of-state event. One teammate offers to pick Andre up and share a hotel room, but Andre has never met him offline. The event page lists a venue but no adult contact, refund policy, medical plan, or code of conduct.

An event is a real-world organization

Verify the organizer, legal entity, venue, schedule, age rules, registration process, contact information, refund terms, code of conduct, and emergency procedures. Search for independent history rather than relying on a server announcement.

A legitimate event should explain who is responsible for minors, how credentials work, what security is present, and how incidents are reported.

Transportation and lodging need independence

A minor should not depend on a newly met online contact for transport, housing, money, or a return trip. Parents should know drivers, routes, lodging, room assignments, supervision, and pickup plans. Use independent transportation and an exit plan whenever possible.

Do not change venues, hotels, or after-parties without updating the adult plan. Keep identification and travel documents under secure personal or parent control.

Meeting online friends requires ordinary precautions

Meet in a busy public place, bring a trusted person, stay sober, control food and drinks, and avoid private homes, vehicles, or hotel rooms. A person who cares about your safety will accept these conditions.

Video calls and long gaming history reduce uncertainty but do not remove risk. Tell someone the plan and use temporary location sharing with a safe adult when appropriate.

Protect equipment and accounts at the venue

Use device locks, cable locks where practical, separate event accounts or user profiles, and current backups. Do not leave unlocked devices at a station. Avoid unknown USB devices and charging cables. Verify tournament software before travel.

Sign out of shared systems, cover sensitive screens, and keep recovery codes separate. Equipment loss should not automatically become account loss.

Chapter 18 Summary

- Verify the organizer and safeguarding process.
- Minors need independent transport, lodging, and a return plan.
- Online history does not replace public-meeting precautions.
- Changes to the plan should be communicated.
- Physical equipment and account security both matter at events.

Chapter 18 Safety Checklist

- ☐ Confirm venue and organizer independently.
- ☐ Create a written travel and emergency plan.
- ☐ Use known transportation and lodging.
- ☐ Meet online friends in public with another person present.
- ☐ Protect food, drinks, ID, and devices.
- ☐ Verify event software.
- ☐ Back up data and separate recovery codes.

Chapter 18 Discussion Questions

1. What makes a tournament verifiable?

2. Why should return travel be independent?
3. What precautions still matter after years of online friendship?
4. How should plan changes be handled?
5. What device risks exist at LAN events?

Make It Stick

MEMORY ANCHOR

NO TROPHY IS WORTH TRAVELING WITHOUT A VERIFIED WAY HOME.

PRESSURE TEST

A teammate says the hotel arrangement changed and you must share a room with an adult coach you barely know.

- A. Accept because the event has started.
- B. Contact your parent or guardian and organizer immediately; do not enter the room until safe lodging is confirmed.
- C. Sleep in the venue instead.

SAFEST FIRST MOVE

Choose B. Lodging changes involving a minor require immediate adult review and a safe alternative.

60-SECOND DRILL

Build a one-page event plan: contacts, address, transport, lodging, check-in times, medical needs, equipment list, and exit route.

SAY IT OUT LOUD

The travel plan changed. I am stopping until my parent and the organizer confirm a safe arrangement.

CLOSED-BOOK RECALL

1. What should be independent from an online contact?
2. Name three event details to verify.
3. How can equipment loss be prevented from becoming account loss?

CHAPTER 19

Rage, Tilt, Trash Talk, and Emotional Regulation

QUICK RECALL BEFORE YOU READ

What are your first physical signs of tilt: heat, tightness, shaking, faster speech, tunnel vision, or the urge to queue instantly?

SCENARIO

After three losses, Malik feels his hands shaking and his thinking narrow. A teammate insults him, and Malik punches the desk, sends a threat in chat, and queues again immediately. The next match goes worse, and the threat is reported to school.

Tilt is a performance and safety state

Tilt is not simply being angry. It is a state in which emotion narrows attention, increases impulsivity, and makes the next decision less reliable. The player may chase losses, blame teammates, spend money, threaten others, or continue after the body needs a break.

Learn the earliest signals. The best time to interrupt tilt is before the outburst, not after the message is sent.

Use a prewritten stop rule

Decide in advance: two losses, one harassment incident, physical pain, missed medication, a certain time, or the first urge to break something means a ten-minute reset. Leave the queue, stand up, drink water, breathe slowly, and move away from chat.

The rule removes the need to negotiate while upset. A break protects rank better than continuing with impaired judgment.

Trash talk needs limits

Competitive banter can be consensual and contained. Threats, slurs, sexual comments, real-world references, and targeting family are not ordinary trash talk. Text and voice can be recorded and shared outside the

match. “I was mad” may explain a message but does not erase its impact or consequences.

Use game language, not real-world threats. If another player escalates, mute and report rather than proving you can escalate further.

Repair matters after a mistake

If you sent harmful messages, stop, preserve the context, apologize without excuses, and accept appropriate consequences. Do not pressure the recipient to withdraw a report. Tell an adult when the message could trigger school, team, or legal concern.

A repair plan may include communication limits, anger-management support, device changes, team accountability, and a temporary break from the mode that repeatedly triggers loss of control.

Chapter 19 Summary

- Tilt narrows judgment and increases impulsive behavior.
- Early physical signals are easier to interrupt than a full outburst.
- A prewritten stop rule removes in-the-moment bargaining.
- Threats and identity-based abuse are not ordinary trash talk.
- Repair requires accountability, not pressure to hide the incident.

Chapter 19 Safety Checklist

- ☐ Name my early tilt signs.
- ☐ Set a loss and time stop rule.
- ☐ Leave chat during a reset.
- ☐ Use mute instead of escalating.
- ☐ Keep real-world threats out of game language.
- ☐ Apologize without excuses after harm.
- ☐ Tell an adult when consequences may extend beyond the game.

Chapter 19 Discussion Questions

1. What makes tilt different from normal frustration?
2. Why should stop rules be written early?
3. Where is the line between banter and harassment?
4. What should an apology avoid?

5. When might professional support help?

Make It Stick

MEMORY ANCHOR

WHEN YOUR BODY SAYS STOP, QUEUING AGAIN IS NOT TOUGHNESS.

PRESSURE TEST

You lose a promotion match and feel the urge to threaten the teammate who made the final mistake.

- A. Send the message privately.
- B. Leave the queue and voice channel, use the reset rule, and return only after your body settles.
- C. Post a vague threat without naming anyone.

SAFEST FIRST MOVE

Choose B. The first safety task is interrupting the state that makes harmful communication likely.

60-SECOND DRILL

Write a three-step tilt reset and place it near the device: leave queue, move body, delay chat.

SAY IT OUT LOUD

I am tilted. I am leaving the queue before I make the next decision worse.

CLOSED-BOOK RECALL

1. Name three physical tilt signals.
2. What content crosses the trash-talk line?
3. What are the parts of a real repair?

CHAPTER 20

Sleep, School, Body, Hearing, and Healthy Play

QUICK RECALL BEFORE YOU READ

What part of your current setup or schedule is likely to hurt first: sleep, eyes, hearing, neck, back, hands, school, or meals?

SCENARIO

Sofia practices until 2 a.m. because her team scrimps in another time zone. She wakes exhausted, skips breakfast, and develops wrist pain and ringing in her ears. She hides the symptoms because she fears being replaced.

Performance depends on recovery

Sleep supports attention, reaction time, learning, mood, and impulse control. A schedule that repeatedly removes sleep may improve short-term practice volume while reducing the ability to use that practice. Teenagers should not be expected to carry adult overnight schedules without consequences.

Set an end time, device wind-down, alarm outside the game, and recovery plan after late events. Teams should publish schedules early enough for families to evaluate them.

Pain is information, not weakness

Wrist, hand, shoulder, neck, back, eye, and headache symptoms can result from poor setup, long static posture, repetitive movement, and inadequate breaks. Adjust chair height, screen position, input devices, lighting, and posture. Use short movement and eye breaks.

Persistent pain, numbness, weakness, or vision problems deserve medical evaluation. Do not play through worsening symptoms to protect a roster spot.

Protect hearing before damage is obvious

Headsets can reach unsafe volume, especially when game audio competes with voice chat. Lower the level, use noise isolation instead of volume

when possible, and take quiet breaks. Ringing, muffled hearing, or sound sensitivity are warning signs.

A limiter or parental volume control can help, but the player still needs a habit of checking volume after loud moments.

Build a schedule that includes the rest of life

Gaming should coexist with school, meals, hygiene, movement, responsibilities, family agreements, and offline relationships. The exact balance differs by season and goals. A written weekly plan makes tradeoffs visible.

Parents should evaluate patterns rather than one long tournament day. Concern grows when sleep, school, health, relationships, or basic care repeatedly collapse and the player cannot adjust.

Chapter 20 Summary

- Recovery supports reaction, learning, and emotional control.
- A team schedule should not depend on chronic sleep loss.
- Persistent pain and neurological symptoms need attention.
- Headset volume can damage hearing before the player notices.
- Healthy gaming fits within a visible whole-life schedule.

Chapter 20 Safety Checklist

- ☐ Set a normal stop time.
- ☐ Use movement and eye breaks.
- ☐ Adjust chair, screen, and input position.
- ☐ Lower headset volume.
- ☐ Tell an adult about pain, numbness, ringing, or vision changes.
- ☐ Keep meals, school, and responsibilities visible.
- ☐ Review patterns weekly.

Chapter 20 Discussion Questions

1. How does sleep affect competition?
2. Which symptoms should not be ignored?
3. Why can noise isolation be safer than higher volume?
4. What makes a schedule sustainable?

5. How should parents distinguish an event exception from a harmful pattern?

Make It Stick

MEMORY ANCHOR

THE BODY IS PART OF THE GAMING SETUP. MAINTAIN IT LIKE ONE.

PRESSURE TEST

Your team adds a mandatory midnight practice before a school exam.

- A. Attend and hide the schedule.
- B. Tell the coach and parent that the conflict must be adjusted or excused.
- C. Skip the exam preparation and catch up later.

SAFEST FIRST MOVE

Choose B. A safe team can discuss school conflicts and does not require secrecy or chronic sleep loss.

60-SECOND DRILL

Set a 25-minute timer and inspect posture, jaw, hands, volume, eyes, and breathing when it ends.

SAY IT OUT LOUD

I can compete seriously without sacrificing basic sleep, school, and health.

CLOSED-BOOK RECALL

1. Name two hearing warning signs.
2. What symptoms require medical attention?
3. What makes a long session an exception rather than a pattern?

CHAPTER 21

Rankings, Burnout, Identity, and Knowing When to Stop

QUICK RECALL BEFORE YOU READ

Would losing your rank change what you believe you are worth?

SCENARIO

Jules climbs into the top one percent and receives attention for the first time. Soon every loss feels public. Jules stops playing with friends, avoids unfamiliar games, and spends most of the day checking rank changes and comparing stats. Winning brings relief rather than enjoyment.

Metrics can turn play into surveillance

Rankings, streaks, leaderboards, viewer counts, and performance dashboards provide useful feedback. They also create constant comparison. When every session becomes evidence for worth, experimentation and friendship disappear.

Choose a few metrics that serve the goal. Review them on a schedule rather than after every match. Include process measures such as communication, decision quality, practice completion, sleep, and enjoyment.

Burnout is not laziness

Burnout may appear as dread, irritability, numbness, declining performance, avoidance, sleep disruption, or the need for more hours to achieve less. Rest is part of training, not proof that someone lacks commitment.

A break should reduce pressure rather than become secret guilt. Communicate with the team, preserve account security, and choose a return point based on recovery, not fear of falling behind.

Diversify identity and goals

Maintain roles that do not depend on the same scoreboard: friend, student, sibling, artist, worker, volunteer, musician, athlete, or learner. Within

gaming, diversify too: competitive play, casual play, coaching, analysis, modding, storytelling, or community building.

A broader identity makes a ban, injury, roster change, or game shutdown painful without making it total.

Know the signs that require more help

Concern increases when gaming is the only source of self-worth, the player cannot stop despite serious harm, conflict becomes constant, or depression and anxiety worsen. Parents should avoid diagnosing from a single behavior and instead look at function, flexibility, and distress.

A doctor or mental-health professional can help when gaming and mood are tightly connected, especially when self-harm, hopelessness, severe sleep disruption, or aggression appears.

Chapter 21 Summary

- Metrics are tools, not verdicts.
- Process measures can be healthier than constant rank checking.
- Burnout reduces function and is not laziness.
- A diversified identity improves resilience.
- Severe distress, inflexibility, or self-harm risk requires adult and professional help.

Chapter 21 Safety Checklist

- ☐ Limit how often I check rank and stats.
- ☐ Track one process goal.
- ☐ Schedule real rest.
- ☐ Keep non-gaming roles active.
- ☐ Tell the team before burnout becomes collapse.
- ☐ Notice whether winning brings joy or only relief.
- ☐ Seek help for severe mood or safety changes.

Chapter 21 Discussion Questions

1. When does feedback become surveillance?
2. What are burnout signs?
3. Why should identity be diversified?

4. What is a process metric?
5. Which changes require professional help?

Make It Stick

MEMORY ANCHOR

RANK CAN MEASURE A RESULT. IT CANNOT MEASURE A PERSON.

PRESSURE TEST

You are sick and exhausted, but missing one session may drop you from the leaderboard.

- A. Play through it to protect identity.
- B. Rest, communicate, and accept a temporary metric loss to protect health.
- C. Give the account to a friend.

SAFEST FIRST MOVE

Choose B. A sustainable competitor protects the capacity to return rather than sacrificing it to one update cycle.

60-SECOND DRILL

Write five identities or values that remain true even if every gaming account disappears.

SAY IT OUT LOUD

My rank is feedback about a game, not a verdict about me.

CLOSED-BOOK RECALL

1. Name three burnout signs.
2. What is one useful process metric?
3. When should a family seek professional support?

PART V

RECOVER AND KEEP PLAYING

The incident does not get the final word. Recovery is a skill set,
not a lucky outcome.

CHAPTER 22

Helping a Teammate in Crisis

QUICK RECALL BEFORE YOU READ

What is your job when someone may be in immediate danger: keep it secret, solve it alone, or bring in real-world help?

SCENARIO

During a late match, Rina's teammate says he has a weapon nearby and will not be alive by morning. Another player calls it attention-seeking and tells Rina not to ruin the session. Rina is frightened, does not know the teammate's exact address, and wonders whether reporting will make things worse.

Take direct statements seriously

A message about suicide, self-harm, abuse, or immediate violence deserves action even when you are unsure whether the person will follow through. Do not challenge them to prove it, shame them, or promise secrecy. Stay calm and ask direct questions: "Are you in immediate danger?" "Do you have a plan or means?" "Where are you right now?"

Direct questions do not create the idea. They help determine urgency and what information responders need.

Do not become the only lifeline

Keep the person engaged if doing so is safe, but contact a trusted adult immediately. Use platform emergency-report tools where available. If you know the person's location and danger is immediate, contact emergency services in that location. In the United States, call or text 988 for crisis support and 911 for immediate danger.

A teen teammate should not carry sole responsibility for another person's life. Bring in adults and professionals even if the person asks you not to.

Preserve useful information

Save the username, profile ID, server, timestamp, exact message, known name, phone, school, city, and any location clues. Do not publicly crowdsource the person's identity. Give relevant information to the platform, adult, crisis responder, or law enforcement.

If the person disconnects, continue the report. Silence does not mean the danger ended.

Support yourself afterward

A crisis disclosure can leave the helper shaken, guilty, angry, or afraid to log in. Tell a parent, counselor, coach, or trusted adult what happened. Limit exposure to rumors and do not take responsibility for outcomes you could not control.

The strongest help is not perfect wording. It is refusing secrecy and connecting the person to real-world support.

Chapter 22 Summary

- Take direct danger statements seriously.
- Ask calm, direct questions about immediate safety and location.
- Do not promise secrecy or manage the crisis alone.
- Use adults, platform tools, crisis services, and emergency services.
- Preserve relevant information without public investigation.
- Helpers also need support.

Chapter 22 Safety Checklist

- ☐ Know 988 and the local emergency number.
- ☐ Identify a trusted adult available during gaming hours.
- ☐ Locate platform emergency reporting.
- ☐ Save exact messages and account IDs.
- ☐ Ask for location when danger is immediate.
- ☐ Continue reporting after disconnection.
- ☐ Debrief with a trusted adult.

Chapter 22 Discussion Questions

1. Why should direct statements be taken seriously?
2. What questions help assess urgency?
3. Why should secrecy be refused?
4. Which information helps responders?
5. What support might the helper need?

Make It Stick

MEMORY ANCHOR

CARE ENOUGH TO BRING IN HELP BIGGER THAN THE LOBBY.

PRESSURE TEST

A teammate says, "Do not tell anyone or I will do it right now."

- A. Promise secrecy to keep them talking.
- B. Keep them engaged if safe while immediately contacting an adult and crisis or emergency support.
- C. Block them because the threat is manipulative.

SAFEST FIRST MOVE

Choose B. The threat may be genuine, coercive, or both. Safety requires real-world support, not one teen holding the secret.

60-SECOND DRILL

Save the crisis contacts and platform-report route where you can reach them without searching during panic.

SAY IT OUT LOUD

I care about you too much to keep this secret. I am getting help now.

CLOSED-BOOK RECALL

1. What should you ask during immediate risk?
2. What number provides U.S. crisis support?
3. What should happen if the person disconnects?

CHAPTER 23

RESET: Incident Response for Gamers

QUICK RECALL BEFORE YOU READ

Can you perform RESET in order without inventing the steps during panic?

SCENARIO

In one evening, Cam receives repeated MFA prompts, discovers a trade he did not approve, and sees a threat containing his old address. He starts deleting messages and changing random settings while arguing with the attacker, making it difficult to understand which account was compromised first.

R - Remove yourself

Leave the lobby, server, call, trade, stream, or direct-message thread. Stop giving the attacker new reactions, information, or opportunities. Do not click new links, approve prompts, pay, or continue a trade.

Move to a trusted device and safe physical place. If the incident includes immediate danger, skip directly to emergency help while another person preserves evidence.

E - Evidence

Capture usernames, profile URLs, account IDs, server and channel names, timestamps, exact threats, transactions, email alerts, device logins, and report numbers. Write a simple timeline. Preserve originals when possible.

Do not forward intimate content, download illegal material, or keep interacting to manufacture more evidence. Useful evidence identifies what happened without spreading the harm.

S - Secure

Start with the primary email. Change exposed passwords, revoke sessions, remove unknown recovery methods, enable strong MFA, and review forwarding rules. Then secure launchers, console networks, Discord, payment services, cloud accounts, and linked creator channels.

Scan or isolate devices when malware is possible. Contact the bank or payment provider quickly after fraud.

E and T - Explain and Tell the right system

Tell a usable adult and assign roles: one person secures accounts, one records evidence, one contacts platforms or financial services, and one supports the player. Report through official channels. Contact NCMEC for child sexual exploitation, law enforcement for credible threats and swatting, and crisis services for immediate emotional danger.

Keep a case log with dates, ticket numbers, responses, and next checks. Recovery often requires follow-up rather than one report.

Chapter 23 Summary

- RESET provides an order when panic disrupts judgment.
- Remove yourself before responding further.
- Evidence should identify the incident without redistributing harm.
- Secure email before dependent accounts.
- Adults can divide response roles.
- Keep a report and follow-up log.

Chapter 23 Safety Checklist

- ☐ Memorize RESET.
- ☐ Use a trusted device.
- ☐ Write a timeline.
- ☐ Secure primary email and payment accounts.
- ☐ Revoke sessions and unknown recovery methods.
- ☐ Tell a usable adult.
- ☐ Record every report number.

Chapter 23 Discussion Questions

1. Why does leaving the interaction help?
2. What evidence should not be redistributed?
3. Which account should be secured first?
4. How can adults divide roles?

5. Why is a case log useful?

Make It Stick

MEMORY ANCHOR

REMOVE. EVIDENCE. SECURE. EXPLAIN. TELL.

PRESSURE TEST

You discover an unauthorized login while the attacker is still messaging you.

A. Argue to learn who they are.

B. Stop contact, move to the official account on a trusted device, preserve the trail, and begin RESET.

C. Delete the account immediately.

SAFEST FIRST MOVE

Choose B. Engagement gives the attacker more control. RESET protects evidence, accounts, and decision quality.

60-SECOND DRILL

On paper, perform RESET for a fake stolen-account scenario and assign each step to a person or device.

SAY IT OUT LOUD

Stop. We are using RESET: leave, save, secure, explain, report.

CLOSED-BOOK RECALL

1. What does each RESET letter mean?
2. Which account is first in the secure step?
3. What belongs in a case log?

CHAPTER 24

Stolen Accounts, Lost Inventory, and Payment Fraud

QUICK RECALL BEFORE YOU READ

What must be contained before public explanation: email, sessions, payment methods, linked accounts, and scam messages?

SCENARIO

Avery wakes to find the account email changed, inventory emptied, and a card charged for currency. Friends report that Avery's account is sending links. Avery's first thought is to create a public post naming the suspected thief.

Contain the recovery hub

Use a trusted device to secure the primary email, phone account, and password manager. Change reused credentials, revoke sessions, remove unknown forwarding rules and recovery methods, and turn on strong MFA.

If the email cannot be recovered, begin the provider's official recovery process and secure any accounts that still use it.

Use official ownership evidence

Contact the game or platform through its official support route. Provide account ID, prior email, creation details, legitimate purchase receipts, billing identifiers, linked console accounts, and the approximate takeover time. Do not send full card numbers or government IDs unless the verified process specifically requires them.

Avoid recovery services sold in messages. They often continue the scam.

Stop financial damage

Contact the card issuer, bank, or payment service through an official number. Report unauthorized transactions, ask about freezing or replacing the payment method, and preserve transaction IDs. Discuss chargebacks with the platform and payment provider because automatic disputes may affect the game account.

Remove saved payment methods from other exposed accounts and review family accounts for linked access.

Warn contacts without creating new risk

After securing the account, warn friends not to open recent links or send money. Use a verified alternate channel. Keep the message factual and avoid naming a suspect without evidence.

Document stolen inventory and unauthorized trades. Recovery policies differ, and virtual items may not be restored, but accurate records improve the claim.

Chapter 24 Summary

- Secure email, phone, and the password manager first.
- Official recovery requires ownership evidence.
- Recovery scammers target victims of account theft.
- Financial providers should be contacted quickly.
- Chargebacks may affect account status and should be coordinated.
- Warn contacts after containment.

Chapter 24 Safety Checklist

- ☐ Secure the recovery hub.
- ☐ Change reused credentials.
- ☐ Revoke all sessions.
- ☐ Gather account and purchase records.
- ☐ Contact official platform support.
- ☐ Notify the payment provider.
- ☐ Warn contacts through a verified channel.

Chapter 24 Discussion Questions

1. Why should public accusation wait?
2. Which records prove ownership?
3. What is a recovery scam?
4. Why should chargebacks be coordinated?
5. When should friends be warned?

Make It Stick

MEMORY ANCHOR

RECOVER CONTROL BEFORE YOU TRY TO RECOVER THE STORY.

PRESSURE TEST

A stranger offers to restore the account for cryptocurrency and says official support is too slow.

- A.** Pay because the inventory is valuable.
- B.** Refuse and continue through official recovery and financial channels.
- C.** Give the stranger temporary email access.

SAFEST FIRST MOVE

Choose B. Victims are often targeted again by people promising impossible recovery.

60-SECOND DRILL

Create a secure account record with IDs, creation dates, linked services, receipts, and official support bookmarks.

SAY IT OUT LOUD

I only use official recovery. I do not pay strangers to return an account.

CLOSED-BOOK RECALL

1. What are the first three accounts or services to secure?
2. Name four ownership records.
3. Why should warning contacts wait until containment?

CHAPTER 25

Raids, Reputation Damage, Appeals, and Starting Again

QUICK RECALL BEFORE YOU READ

What protects a damaged reputation better: one documented statement and an appeal, or an uncontrolled evidence dump?

SCENARIO

A rival server coordinates false reports against Leila's community. Her server is disabled, edited screenshots spread, and former members accuse her of conduct she did not commit. Leila wants to post every private message and send her members after the rival group.

Stabilize before defending

Restrict posting, secure moderator accounts, preserve logs, and identify what is verified. A chaotic public response can expose private members, contradict later evidence, and produce new rule violations.

Write a timeline and separate facts, allegations, and unknowns. Let a trusted adult or moderator review the first public statement.

Appeal the decision, not the entire internet

Use the platform's official appeal system. Provide account or server IDs, dates, relevant logs, screenshots, prior reports, and a concise explanation of coordinated abuse. Avoid insults, speculation, and repeated duplicate tickets.

An appeal may take time or fail. Keep copies of content, member contacts, rules, and backups so the community does not depend entirely on one platform.

Protect innocent people

Do not publish private messages, phone numbers, school information, or identities to prove your case. Redact bystanders and minors. Do not send members to retaliate or mass-report. Coordinated counteraction can become harassment and damage the appeal.

Correct important claims with evidence, but do not try to answer every rumor.

A restart can be professional

If access is not restored, rebuild with clearer rules, stronger moderator security, backups, ownership separation, and a smaller trusted core.

Explain what changed without turning the new community into a permanent war room.

Starting again is not admitting every allegation. It is choosing continuity when a platform or community can no longer support safe participation.

Chapter 25 Summary

- Stabilize accounts, logs, and communication before defending publicly.
- Separate facts, allegations, and unknowns.
- Appeals should be concise and evidence-based.
- Protect bystanders and do not organize retaliation.
- Backups reduce dependence on one platform.
- A restart can be a valid recovery strategy.

Chapter 25 Safety Checklist

- ☐ Secure moderators and integrations.
- ☐ Save logs and write a timeline.
- ☐ Use the official appeal route.
- ☐ Redact private information.
- ☐ Post one factual update.
- ☐ Do not mass-report or retaliate.
- ☐ Maintain community backups and alternate contacts.

Chapter 25 Discussion Questions

1. Why can an evidence dump create new harm?
2. What makes an appeal useful?
3. Who should be redacted?
4. Why is counter-reporting risky?
5. What infrastructure supports a safe restart?

Make It Stick

MEMORY ANCHOR

DOCUMENT ONCE. APPEAL CLEARLY. DO NOT TURN RECOVERY INTO A SECOND RAID.

PRESSURE TEST

Members demand that you publish a rival moderator's real name and address to prove who organized the raid.

- A.** Publish it because the accusation is serious.
- B.** Refuse, preserve relevant evidence privately, and use official reporting and appeal channels.
- C.** Hint at the address without posting it fully.

SAFEST FIRST MOVE

Choose B. Doxxing someone else does not repair the original harm and can create new victims and consequences.

60-SECOND DRILL

Draft a six-sentence incident statement: what happened, what is confirmed, what is being secured, where reports were filed, what members should do, and when the next update will occur.

SAY IT OUT LOUD

We are preserving evidence and appealing through official channels. Do not retaliate or share private information.

CLOSED-BOOK RECALL

1. What are the three information categories in a timeline?
2. Why should duplicate tickets be avoided?
3. What makes a restart professional?

PART VI

PARENT FIELD GUIDE

The goal is not to defeat gaming. It is to help a young person build judgment, recovery skills, and growing independence.

CHAPTER 26

Support Without Treating Games as the Enemy

QUICK RECALL BEFORE YOU READ

Would your teen expect help, punishment, surveillance, or disbelief after admitting an online mistake?

SCENARIO

A parent hears shouting from a sixteen-year-old's room, enters without knocking, disconnects the console, reads every message, and announces that online friends are not real. The teen later receives a threatening DM but hides it, expecting that disclosure will end gaming completely.

Learn the function before judging the hours

Gaming may provide friendship, mastery, creativity, competition, recovery, or avoidance. The same number of hours can mean different things depending on sleep, school, health, responsibilities, flexibility, and emotional state. Ask what the game and community provide.

Understanding function does not remove limits. It makes limits accurate.

Become a usable adult

A usable adult responds to disclosure with calm sequencing: safety first, evidence second, consequences later. Begin with, "I am glad you told me. Are you safe right now? Show me what happened."

Automatic humiliation, public confrontation, or total device removal may teach a teenager to hide future incidents. Consequences should target the behavior and risk, not erase every source of connection.

Respect privacy without abandoning supervision

Transparent supervision explains what is reviewed, why, for how long, and what earns more independence. Focus on high-risk areas: unknown adults, private DMs, payments, disappearing messages, location, late-night use, sexual pressure, threats, and sudden behavior changes.

Routine secret surveillance can damage trust and expose peers' private disclosures. Immediate safety concerns may justify closer oversight, but the plan should be named and reviewed.

Enter the gaming world enough to help

Know the game, account stack, friends, team, server, payment system, report controls, and current family settings. Play a match, watch a tournament, or ask the teen to explain the platform. Curiosity should not become an interrogation.

Adults do not need expert mechanics. They need enough context to recognize when a normal loss becomes fraud, grooming, harassment, or physical danger.

Chapter 26 Summary

- Gaming hours must be interpreted in context.
- A calm first response increases future disclosure.
- Consequences should target behavior and risk.
- Supervision should be transparent and proportionate.
- Adults need platform context, not elite gaming skill.

Chapter 26 Safety Checklist

- ☐ Ask what gaming provides.
- ☐ Practice a calm disclosure response.
- ☐ Know the main accounts and communities.
- ☐ Explain monitoring openly.
- ☐ Separate immediate safety from later consequences.
- ☐ Avoid insulting online friendships.
- ☐ Review limits on a schedule.

Chapter 26 Discussion Questions

1. What functions can gaming serve?
2. What makes an adult usable?
3. When is closer supervision justified?
4. Why can secret surveillance backfire?
5. What should a parent learn about the platform?

Make It Stick

MEMORY ANCHOR

THE GOAL IS NOT TO WIN AGAINST THE GAME. IT IS TO STAY ON THE SAME TEAM AS YOUR TEEN.

PRESSURE TEST

Your teen says, "I clicked a tournament link and now my account is gone."

- A.** Begin with a lecture about responsibility.
- B.** Say you are glad they told you, secure the email and payment accounts, preserve evidence, then discuss consequences later.
- C.** Confiscate every device before asking questions.

SAFEST FIRST MOVE

Choose B. Early containment and trust protect more than immediate punishment.

60-SECOND DRILL

Practice the first four sentences you will use after a serious disclosure.

SAY IT OUT LOUD

I am glad you told me. You are not in trouble for asking for help. Are you safe? Let us handle the next step together.

CLOSED-BOOK RECALL

1. What should come before consequences?
2. What high-risk areas deserve supervision?
3. What does a parent need to know about a game community?

CHAPTER 27

Readiness, Supervision, and the Family Gaming Agreement

QUICK RECALL BEFORE YOU READ

What skills should determine access: age alone, or judgment, honesty, boundaries, recovery, and the specific platform risk?

SCENARIO

A thirteen-year-old wants unrestricted voice chat because classmates already use it. The parents respond with a permanent ban. The teen creates a hidden account on a friend's device, leaving the family with less visibility and no practiced safety plan.

Readiness is skill-based and context-specific

Assess whether the teen can protect credentials, use block and report tools, recognize manipulation, follow spending rules, stop when directed, disclose mistakes, and manage sleep and school. A teen may be ready for a friends-only party but not a public server or overnight tournament.

Reassess after platform changes, new games, new teams, or major incidents.

Write the agreement together

A useful family agreement covers accounts, real-name use, voice and video, DMs, friends, purchases, schedules, devices, travel, downloads, reporting, and what happens after a mistake. It should include adult obligations: calm response, respect for ordinary privacy, and no public shaming.

The agreement is strongest when it names the reason behind each rule and includes a review date.

Use graduated independence

Begin with narrower communication, spending approval, known-friend play, and visible schedules. Increase access as the teen demonstrates

judgment and early disclosure. Reduce access temporarily when a specific risk appears, with a clear path to regain it.

Permanent restrictions can encourage workarounds when they do not match development or behavior.

Practice incidents before they happen

Run drills for a stolen account, sexual threat, doxxing post, unknown adult DM, accidental purchase, and crisis message. Ask the teen to perform the first steps while calm.

The purpose is not to frighten. Practice reduces the amount of thinking required under pressure.

Chapter 27 Summary

- Readiness depends on skills and platform context.
- Family agreements should include teen and adult responsibilities.
- Rules need reasons and review dates.
- Independence should grow with demonstrated judgment.
- Incident drills build usable memory.

Chapter 27 Safety Checklist

- ☐ Assess account and reporting skills.
- ☐ Write rules and adult promises together.
- ☐ Set a review date.
- ☐ Use friends-only settings as a starting lane.
- ☐ Define spending and schedule limits.
- ☐ Create a path to more independence.
- ☐ Practice at least three incident drills.

Chapter 27 Discussion Questions

1. Which skills show readiness?
2. What should adults promise in the agreement?
3. Why do permanent bans create workarounds?
4. How can independence be earned?
5. Which incident should the family rehearse first?

Make It Stick

MEMORY ANCHOR

RULES WORK BEST WHEN EVERYONE KNOWS THE REASON, THE REVIEW DATE, AND THE PATH FORWARD.

PRESSURE TEST

Your teen asks to join a public server for a game tournament.

- A.** Allow or deny based only on age.
- B.** Review the server, rules, moderators, DM settings, event need, and the teen's safety skills; then choose a limited plan.
- C.** Allow it secretly so the other parent does not object.

SAFEST FIRST MOVE

Choose B. Specific assessment produces a rule that matches the actual risk.

60-SECOND DRILL

Set a 30-day review date and write three behaviors that would support more independence.

SAY IT OUT LOUD

This limit is not forever. We will review it on this date using these skills and behaviors.

CLOSED-BOOK RECALL

1. What makes readiness context-specific?
2. What belongs in the adult side of the agreement?
3. Why are drills useful?

CHAPTER 28

Platform Controls, Communication, and Privacy

QUICK RECALL BEFORE YOU READ

How many separate systems make up your teen's gaming stack?

SCENARIO

A family enables a console playtime limit but assumes the teenager is protected everywhere. The teen uses Discord on a phone, game voice on a laptop, and a linked publisher account with separate privacy and payment settings. No one realizes that server members can send direct messages.

Controls are layered

A console setting may not control the game publisher, Discord, mobile companion app, launcher, livestream service, browser, or payment wallet. Build an account map. For each layer, review communication, friends, content, spending, playtime, privacy, location, recordings, and recovery.

Use child or teen accounts with accurate ages. False ages may disable protections and complicate recovery.

Use official family tools

Xbox, PlayStation, Nintendo, Roblox, Epic, and Discord provide family or parental tools with different scopes. Official features may manage playtime, communication, content, friend requests, spending, activity insights, and sensitive content. Settings and regional availability change.

Open the official support page together and verify what the control actually does. Do not assume a label such as "safe" blocks every route.

Protect privacy while supervising

Prefer summaries, settings, and high-risk alerts over reading every conversation. Explain which information the adult can see. Avoid demanding shared passwords when family tools and recovery contacts provide safer oversight.

For immediate danger, exploitation, or repeated rule evasion, more direct review may be necessary. Define the scope and exit conditions.

Review after updates and new accounts

Games add voice, cross-play, user-generated content, marketplaces, and external links. A new season or device may introduce separate defaults. Review settings quarterly and whenever the teen joins a new game, server, team, or platform.

Keep the parent-control PIN separate from ordinary device PINs and do not leave unrestricted guest accounts available.

Chapter 28 Summary

- Gaming safety controls exist across multiple account layers.
- Accurate ages help apply appropriate protections.
- Official family tools vary by platform and region.
- Transparent summaries are usually better than total conversation surveillance.
- Settings need review after updates and new services.

Chapter 28 Safety Checklist

- ☐ Create an account and device map.
- ☐ Use accurate-age teen accounts.
- ☐ Review communication and friend settings.
- ☐ Set spending approval and recovery contacts.
- ☐ Disable unrestricted guest paths.
- ☐ Explain what the parent can see.
- ☐ Repeat reviews quarterly.

Chapter 28 Discussion Questions

1. Why is a console limit incomplete?
2. What problems come from false ages?
3. What should transparent supervision reveal?
4. When might closer review be necessary?
5. What events trigger a settings review?

Make It Stick

MEMORY ANCHOR

CONTROL THE WHOLE STACK - NOT JUST THE BOX UNDER THE TELEVISION.

PRESSURE TEST

A parent discovers the teen has a second unrestricted account used only at a friend's house.

- A.** Install secret monitoring on every device.
- B.** Discuss why the workaround exists, secure current risks, revise the agreement, and coordinate with the other household when appropriate.
- C.** Ban the friend permanently.

SAFEST FIRST MOVE

Choose B. The immediate risk and the failed rule both need attention; secrecy alone does not solve either.

60-SECOND DRILL

Draw the gaming stack: device, console account, game account, Discord, email, payment, streaming, and family controls.

SAY IT OUT LOUD

We need one accurate account map so no safety setting depends on a guess.

CLOSED-BOOK RECALL

1. Name four layers beyond the console.
2. Why should ages be accurate?
3. When should settings be reviewed?

CHAPTER 29

Money, Esports, Contracts, Travel, and Workload

QUICK RECALL BEFORE YOU READ

When gaming becomes work, which adult systems must become real: contracts, records, taxes, safeguarding, schedule, travel, and ownership?

SCENARIO

A talented fifteen-year-old receives tournament winnings, a team contract, equipment from a sponsor, and a request to travel. The family celebrates but does not clarify taxes, ownership, practice hours, school absences, hotel supervision, or who controls the player's accounts and content.

Treat money as money

Track prizes, sponsorships, affiliate income, coaching payments, gifted equipment, expenses, fees, and refunds. Keep separate records and, when appropriate, a separate bank account managed according to local law and the teen's age. Consult a qualified tax professional about reporting obligations.

Do not let team staff route a minor's money through personal payment accounts without transparent documentation.

Read every contract

Contracts may address exclusivity, content rights, name and likeness, prize splits, termination, behavior, confidentiality, equipment, travel, dispute resolution, and account access. A parent or guardian should review minor agreements, and meaningful deals deserve independent legal advice.

Do not sign blank pages, accept verbal changes, or let urgency replace review.

Protect school and workload

Practice, content, travel, media, sponsor obligations, and recovery can become a job. Set maximum weekly hours, school protections, off-days, sleep minimums, and a process for exam or illness conflicts.

A young person's excitement does not eliminate the adult duty to prevent exploitative schedules.

Travel needs safeguarding

Identify adult supervisors, background or safeguarding policies where applicable, transport, lodging, room assignments, medical information, emergency contacts, and how a minor reports concerns away from the coach.

Parents should know where the teen is, who is responsible, and how the teen can leave without depending on the person who controls selection or payment.

Chapter 29 Summary

- Gaming income requires records and tax review.
- Minor contracts deserve parent and often professional review.
- Ownership and termination terms matter.
- Workload must protect school, sleep, and health.
- Travel safety needs a reporting path outside the coach.

Chapter 29 Safety Checklist

- ☐ Track all income, gifts, and expenses.
- ☐ Keep copies of contracts and changes.
- ☐ Use independent professional review for significant deals.
- ☐ Define maximum hours and school protections.
- ☐ Clarify account and content ownership.
- ☐ Create a written travel plan.
- ☐ Provide a separate safeguarding contact.

Chapter 29 Discussion Questions

1. What income should be recorded?

2. Which contract terms deserve special attention?
3. Why should deal review be independent?
4. What limits belong in a workload plan?
5. Why should travel reporting be separate from the coach?

Make It Stick

MEMORY ANCHOR

WHEN PLAY BECOMES WORK, PROTECTION MUST BECOME PROFESSIONAL TOO.

PRESSURE TEST

A team offers a contract that transfers all content rights and allows termination without paying earned prizes.

- A. Sign because the opportunity may not return.
- B. Pause and obtain parent and independent professional review.
- C. Cross out the terms and sign without telling the team.

SAFEST FIRST MOVE

Choose B. Rights and payment terms can affect years of work and should not be accepted under urgency.

60-SECOND DRILL

Create folders for contracts, receipts, travel plans, tax records, and account ownership information.

SAY IT OUT LOUD

We are interested, but a minor does not sign until the agreement is independently reviewed.

CLOSED-BOOK RECALL

1. Name five contract topics.
2. What workload limits should be written?
3. What makes travel supervision safer?

CHAPTER 30

Crisis Response, Growing Independence, and the Long-Term Plan

QUICK RECALL BEFORE YOU READ

Does the family's safety plan create more judgment over time, or only more control?

SCENARIO

At seventeen, Morgan has handled accounts and team communication responsibly for a year. After one serious harassment incident, the parents restore childhood-level restrictions indefinitely. Morgan stops sharing concerns and prepares to move every account at eighteen without family recovery support.

Respond to crisis in phases

First stabilize safety, evidence, accounts, money, and emotional state. Second, investigate what happened and which systems failed. Third, choose proportional temporary controls. Fourth, restore independence according to written conditions.

Do not make permanent rules during the first hour of panic unless immediate safety requires them.

Use after-action reviews

Within a few days, ask: What happened? What worked? What delayed help? Which account, rule, or relationship increased risk? What should change? Keep the review focused on systems and choices rather than character judgments.

Document updates to passwords, settings, contacts, spending, moderators, travel, and team rules.

Transfer responsibility deliberately

As teens mature, teach them to own the password manager, recovery records, budgets, support tickets, travel planning, and professional communication. Parents can remain backup contacts without holding every password.

Before adulthood, clarify account ownership, payment methods, tax records, contracts, domain names, channels, equipment, and data backups.

Define the long-term success standard

Success is not zero incidents. It is early disclosure, thoughtful decisions, proportional recovery, healthy routines, respect for others, and the ability to leave unsafe people or systems. Review the plan every three months and after major changes.

The best family safety system becomes less visible as judgment grows, but remains easy to activate during crisis.

Chapter 30 Summary

- Crisis response should move from stabilization to restoration.
- Permanent rules should not be improvised during panic.
- After-action reviews focus on systems and choices.
- Responsibility should transfer before adulthood.
- Account, money, contract, and data ownership need clarity.
- Success is measured by judgment and recovery, not perfection.

Chapter 30 Safety Checklist

- ☐ Use phased crisis response.
- ☐ Schedule an after-action review.
- ☐ Write conditions for restoring independence.
- ☐ Teach the teen to manage recovery and records.
- ☐ Clarify ownership before age eighteen.
- ☐ Review the safety plan quarterly.
- ☐ Keep emergency contacts current.

Chapter 30 Discussion Questions

1. What are the four crisis phases?
2. Why should restrictions include restoration conditions?
3. What belongs in an after-action review?
4. Which responsibilities should transfer before adulthood?
5. How should family success be measured?

Make It Stick

MEMORY ANCHOR

THE SAFETY PLAN SHOULD GROW A CAPABLE ADULT - NOT A PERMANENTLY MANAGED CHILD.

PRESSURE TEST

After an incident, a parent wants every password forever despite the teen's strong recovery behavior.

- A. Keep the rule because fear justifies permanent control.
- B. Use temporary safeguards with a review date and move toward recovery contacts, family tools, and demonstrated independence.
- C. Tell the teen to create secret accounts.

SAFEST FIRST MOVE

Choose B. Proportional, reviewable safeguards protect safety while preserving the relationship and long-term skill development.

60-SECOND DRILL

Set the next quarterly review and list three responsibilities the teen will own before that date.

SAY IT OUT LOUD

Our goal is more judgment and independence. This safeguard has a review date and a clear path forward.

CLOSED-BOOK RECALL

1. What should happen before permanent rule changes?
2. Name three responsibilities to transfer.
3. What defines success besides zero incidents?

TOOLS AND RESOURCES

Copy, print, or adapt these tools. A completed one-page plan is more useful during panic than a perfect policy no one can find.

Ten-Minute Gamer Safety Setup

- ☐ Secure the primary email with a unique credential and strong MFA.
- ☐ Turn on MFA for game launchers, console networks, Discord, streaming, and payment accounts.
- ☐ Review active sessions, recovery methods, and linked apps.
- ☐ Limit direct messages and friend requests from unknown people.
- ☐ Turn off unnecessary activity, location, and notification previews.
- ☐ Remove saved payment methods or require a purchase PIN.
- ☐ Locate block, report, emergency-report, trade-history, and account-recovery tools.
- ☐ Write three usable adults and crisis contacts.
- ☐ Create a panic scene or blank screen for streaming and screen sharing.
- ☐ Say RESET aloud once.

Family Gaming Agreement

PURPOSE

We agree that gaming can be meaningful recreation, friendship, competition, creativity, and work. Our rules exist to protect safety, health, money, responsibilities, and trust - not to humiliate or control.

Accounts and identity

- ☐ Real names and school information allowed in these spaces: _____
- ☐ Parent recovery contact or family tool: _____
- ☐ Passwords are not shared with friends, partners, teammates, or coaches.

Communication

- ☐ Voice/video allowed with: _____
- ☐ Unknown DMs are handled by: _____

- ☐ At least one adult knows important servers, teams, and online friendships.

Money

- ☐ Monthly budget: _____
- ☐ Purchase approval threshold: _____
- ☐ Saved payment and refund rules: _____

Time and health

- ☐ Normal stop time: _____
- ☐ School-night and tournament exceptions: _____
- ☐ Break, pain, hearing, meal, and sleep rules: _____

Safety response

- ☐ RESET contacts: _____
- ☐ No automatic punishment for asking for urgent help.
- ☐ Review date and path to more independence: _____

Incident Log

- ☐ Date and time
- ☐ Platform, game, server, lobby, channel, or event
- ☐ Account IDs and profile links
- ☐ What happened in chronological order
- ☐ Exact threat or request
- ☐ Evidence saved and location
- ☐ Accounts secured
- ☐ Money or items affected
- ☐ Adults and organizations contacted
- ☐ Report or ticket numbers
- ☐ Next follow-up date
- ☐ Emotional and physical safety check

Tournament and Meetup Safety Plan

- ☐ Verified organizer and venue
- ☐ Adult responsible for minor safeguarding
- ☐ Transport to and from venue

- ☐ Lodging and room assignments
- ☐ Check-in schedule
- ☐ Medical needs and emergency contacts
- ☐ Independent exit and return plan
- ☐ Public meeting location for online friends
- ☐ Device, equipment, and account security
- ☐ Changes require parent or guardian approval

RESET Pocket Card

R - REMOVE

Leave the lobby, call, server, trade, stream, or argument. Move to safety.

E - EVIDENCE

Save account IDs, links, timestamps, exact messages, transactions, and report numbers.

S - SECURE

Protect email, accounts, devices, payment methods, sessions, and recovery information.

E - EXPLAIN

Tell a calm adult or official who can help coordinate the response.

T - TELL

Report to the platform and the correct real-world system: bank, school, NCMEC, crisis service, or law enforcement.

30-Day Gamer Safety Challenge

- ☐ Day 1: Search your main gamer tag while logged out.
- ☐ Day 2: Secure the primary email.
- ☐ Day 3: Replace one reused password.
- ☐ Day 4: Enable MFA on one major gaming account.
- ☐ Day 5: Review Discord or community DM settings.

- ☐ Day 6: Remove one unnecessary linked app.
- ☐ Day 7: Convert three virtual prices to dollars.
- ☐ Day 8: Set a purchase PIN or approval.
- ☐ Day 9: Locate trade and payment history.
- ☐ Day 10: Audit a gamer profile for identity clues.
- ☐ Day 11: Practice mute, block, leave, and report.
- ☐ Day 12: Review screen-share notifications.
- ☐ Day 13: Create a clean gaming browser or user profile.
- ☐ Day 14: Check headset volume and setup.
- ☐ Day 15: Write a tilt stop rule.
- ☐ Day 16: Schedule one sleep-protecting stop time.
- ☐ Day 17: List three usable adults.
- ☐ Day 18: Save crisis and CyberTipline resources.
- ☐ Day 19: Practice RESET for a fake account theft.
- ☐ Day 20: Review one server's moderation structure.
- ☐ Day 21: Check game and tournament rules on mods and boosting.
- ☐ Day 22: Back up saves or important content.
- ☐ Day 23: Create an account ownership record.
- ☐ Day 24: Review family controls across the full account stack.
- ☐ Day 25: Write a meetup or event plan.
- ☐ Day 26: Track one week of gaming spending.
- ☐ Day 27: Track one week of sleep and playtime.
- ☐ Day 28: Choose one non-gaming identity to strengthen.
- ☐ Day 29: Complete a family agreement review.
- ☐ Day 30: Teach RESET to another player.

Emergency and Reporting Resources

Immediate danger in the United States: 911

Mental-health crisis in the United States: Call or text 988; use the 988 Lifeline official service.

Suspected child sexual exploitation: NCMEC CyberTipline; 1-800-THE-LOST in the United States.

Eligible intimate images created before age eighteen: NCMEC Take It Down.

Fraud and identity theft: Contact the bank or payment provider; use IdentityTheft.gov and ReportFraud.ftc.gov in the United States.

Federal crime tips in the United States: FBI electronic tip form or local FBI field office.

Platform harm: Use the official in-app report, safety center, and support process; preserve ticket numbers.

Glossary

Account stack — The connected email, launcher, console, game, chat, payment, streaming, and recovery accounts that support gaming.

Boosting — Using another person or prohibited method to raise rank or progress, often in violation of rules.

Credential stuffing — Testing credentials exposed from one service against other accounts.

Doxxing — Publishing or threatening to publish identifying information to intimidate or enable harm.

Gacha — A randomized reward system in which players spend currency for a chance at characters or items.

Grooming — A process of building access, trust, secrecy, and control to exploit a young person.

MFA — Multifactor authentication, requiring more than one type of proof to log in.

Parasocial relationship — A one-sided sense of closeness between an audience member and a public person or player.

Phishing — A deceptive message or page designed to steal credentials, money, or access.

RESET — Remove, Evidence, Secure, Explain, Tell - the gamer incident-response framework.

Sextortion — Threatening to share sexual material or claims in order to demand money, more material, or control.

Smurfing — Using a secondary account to play below a player's usual level; rules and effects vary by game.

Swatting — Making a false emergency report intended to trigger an armed law-enforcement response.

Tilt — An emotional state that narrows judgment and harms decision-making and performance.

Virtual currency — Game-specific units bought or earned and used for items, entries, or progress.

Living Platform Safety Matrix

Platform controls change too quickly for a printed menu path to remain reliable. This snapshot was verified in July 2026. Use the official support page and the series update center before acting.

Platform	Age / eligibility	Communication controls	Parent / family tools	Last verified
Discord	Service is not available under 13; older local minimum ages can apply.	Teen-by-default safety settings, message-request screening, sensitive-media filters, age-restricted spaces, reporting.	Family Center shows activity summaries and selected safety settings without exposing message content.	July 2026
Roblox	Age checks are required for communication features; voice chat is 13+ after age check.	Similar-age chat groups, parent-managed communication settings, private-server controls, block/report tools.	Linked parent controls, communication permissions, content restrictions, spending limits and notifications.	July 2026
Twitch	At least 13 and any older minimum age required	Chat moderation, block/report, AutoMod and channel roles; rules	Parent/guardian agreement for minor use and consent/sup	July 2026

Platform	Age / eligibility	Communication controls	Parent / family tools	Last verified
	locally; minors need parent or guardian supervision.	vary by channel.	ervision for Affiliate onboarding.	
Xbox / Microsoft	Account age and family settings depend on region and family account configuration.	Privacy, communication, multiplayer and cross-network controls.	Microsoft Family Safety and Xbox family settings.	Verify current official page
PlayStation	Age and child-account rules depend on country and family setup.	Communication, user-generated content, spending and play-time controls.	Family Management and PlayStation family tools.	Verify current official page
Nintendo	Child-account rules and features depend on product and region.	Friend, communication, restriction and play-time settings vary by system and game.	Nintendo Switch Parental Controls and account-family settings.	Verify current official page
Epic Games	Cabined-account and age rules depend on declared age and region.	Voice/text chat permissions, friend requests, mature language	Epic parental controls and PIN-protected settings.	Verify current official page

Platform	Age / eligibility	Communication controls	Parent / family tools	Last verified
		and purchases.		
Steam	Account and purchase rules apply; family eligibility varies by feature and region.	Profile, chat, community, trade and inventory privacy controls.	Steam Families, Steam Guard and account recovery tools.	Verify current official page

Proof-of-Ownership Account Recovery Checklist

Before an account is stolen, record enough information to prove ownership without publishing it or storing it in the same account:

- ☐ Original account email and approximate creation date.
- ☐ Previous usernames, linked console IDs, and authorized devices.
- ☐ Purchase receipts, order numbers, gift-card records, and subscription dates.
- ☐ Recovery codes and backup authentication methods stored separately.
- ☐ Screenshots or records of high-value inventory, where permitted.
- ☐ Parent or guardian contact information used for a minor account.
- ☐ Official support case numbers and the dates of prior ownership changes.

Never pay an unofficial "recovery expert," share one-time login codes, or download remote-control software because a stranger claims they can restore the account.

Sources and Further Reading

The following official sources were reviewed for this July 2026 educational edition. Platform settings and rules change; readers should use current official support pages before relying on a specific feature or age requirement.

2026 platform verification sources:

- Discord, "Discord Launches Teen Default Experience Globally" and "A Safer Discord by Default: New Teen Safety Updates," February 2026; Discord Family Center and reporting guidance.
- Roblox Support, "How to chat on Roblox," "Understanding Age Checks on Roblox," "Parental Controls Overview," and Voice Chat guidance, reviewed July 2026.
- Twitch Terms of Service, effective April 13, 2026; Twitch Affiliate onboarding and minor-consent guidance.
- NCMEC Take It Down FAQ and participating-platform list, reviewed July 2026.
- CISA: More Than a Password; phishing and phishing-resistant multifactor authentication guidance.
- Discord Safety Center, Teen Safety Assist, Family Center, teen-default safety updates, child-safety policy explainers, and parent guidance.
- Twitch Safety Center, Community Guidelines, and Guide for Parents & Educators.
- Roblox Safety Center, Parental Controls, communication controls, and content maturity guidance.
- Xbox Family Safety and privacy controls; Xbox Family Settings app.
- PlayStation Safety, Family Management, parental controls, and PlayStation Family app guidance.
- Nintendo online safety and Nintendo Switch Parental Controls, including communication restrictions.
- Epic Games Safety and Security Center, Parental Controls, and Cabined Accounts guidance.
- Steam Support: Steam Guard, Mobile Authenticator, account security recommendations, stolen-account recovery, and trading restrictions.
- NCMEC: Online Enticement, CyberTipline, NetSmartz, Take It Down, and generative-AI exploitation resources.
- FTC: video-game consumer protection, loot boxes, in-game purchase guidance, fraud reporting, and enforcement involving deceptive randomized rewards.
- FBI: swatting guidance, hoax threats, electronic tips, and 2025-2026 warnings about violent online networks targeting minors.
- 988 Lifeline and local emergency services for crisis response.

FINAL MESSAGE TO TEEN GAMERS

You can play seriously without surrendering your privacy, money, body, relationships, or judgment. You can leave a lobby, reject a trade, report a coach, block a friend, take a break, ask for help, and start again. The strongest player is not the person who never faces pressure. It is the person who can recognize pressure and still choose the next safe move.

FINAL MESSAGE TO ADULTS

Stay usable. Learn the platform. Protect the person before the account. Preserve evidence before deleting. Separate safety from punishment. Build rules that grow judgment, and let independence expand when the young person demonstrates it. The relationship is part of the safety system.

For corrections and platform updates, use the Connected Without Compromise update center.