MINECRAFT EDUCATION

BAD CONNECTION?



EDUCATOR GUIDE



TARGET AUDIENCE

Grades 6–10 | Ages 11–15

This lesson includes scenarios depicting manipulation, harassment, and threats. It is designed for learners ages 11+ with adult facilitation.

OVERVIEW

Meeting friends online can be lots of fun, if you know how to spot a bad connection. In this world, it's important learn to recognize tactics that could be used to manipulate you. In this game, you will play through three scenarios of peer influence, deciding who to trust and reporting suspicious activity. You will build confidence in how to keep yourself and your community safe—and help build a safer Internet for everyone.

ESSENTIAL QUESTION

How can I recognize different types of online interactions and what choice can I make to protect myself and others?

MATERIALS NEEDED

- Computers with Minecraft Education installed
- Projector to introduce the lesson and set the scene
- Educator presentation slides (optional)
- Safety Skills Toolkit handout (included in this guide)

LESSON DURATION

1 Class Period (45–60 minutes)

Note: Reading-heavy classes or younger learners may need 60–75 minutes. Consider the two-session option (Acts 0–1, then Acts 2–3) forcing and fidelity.

LEARNING OBJECTIVES

- Identify and respond to unsafe online interactions through guided practice
- Normalize open conversations about digital safety, reducing fear and stigma
- Spot red flags in unsafe online interactions
- Build confidence in reporting concerns and supporting peers who may be at risk
- Evaluate online relationships by asking verification questions
- Understand that online actions have permanent consequences (digital footprint)

KEY VOCABULARY

Manipulation: When a person tries to influence someone's thoughts or actions in a sneaky or unfair way, often to get what they want

Reporting: Telling a trusted adult or using an app or website's tools to let someone know that something unsafe, uncomfortable, or inappropriate has happened online

Boundaries: Personal limits that help keep you safe (both in real-life and online)

Digital Footprint: The trail of data you leave behind when you go online—including messages, photos, and personal information you share

© 2026. Microsoft. All Rights Reserved

DISTRICT/MINISTRY IMPLEMENTATION SUMMARY

CyberSafe: Bad Connection? is a one-period, teacher-facilitated digital safety lesson for ages 11–15 that builds practical skills in privacy/PII protection, recognizing manipulation and harassment, using platform safety tools (block/report/leave), and help-seeking escalation to offline support. The lesson includes trauma-informed opt-out pathways, a disclosure response protocol aligned to local safeguarding procedures, and optional system-level evidence tools (anonymized pre/post check) for reporting impact without collecting sensitive personal histories.

POLICY AND SAFEGUARDING ALIGNMENT

This lesson is designed for **prevention and skill-building**. It is not intended to investigate real incidents or collect personal histories.

Requirement	Guidance
Follow local policy	Educators must follow their school/district/ministry safeguarding, child protection, and mandatory reporting procedures.
Do not prompt disclosure	Learners should never be asked to share personal experiences publicly. Participation is skill-focused and scenario-based.
If a learner shares a concern	Listen, do not investigate, and refer promptly to the designated safeguarding lead, counselor, or administrator per local procedure.
Immediate risk	If a learner reports a credible threat or immediate danger (e.g., plan to meet, stalking, weapon threat, intent to self-harm), follow your school's emergency response procedure and escalate immediately to leadership/security per local policy.
Wellbeing first	Learners may pause or opt out at any time without explanation using the provided pathways.
Data privacy	Learners should use school-managed accounts and follow local data governance. Learners should not enter or share real personal information during this lesson (e.g., name, address, phone number, personal email, school name, social handles, usernames used outside class). If an example is needed, use fictional placeholders (e.g., "[school]", "[city]", "[email]"). Store any assessment artifacts per school retention policy.
Staffing and facilitation	Recommended minimum is one adult facilitator per classroom; follow local supervision policy for device-based learning. Educators should complete the experience themselves before facilitating. This lesson is designed for a supervised classroom setting. Learners should not join public servers as part of this activity. Follow local policy for multiplayer permissions and supervision.

© 2026. Microsoft. All Rights Reserved

Table of Contents

District/Ministry Implementation Summary 3

Policy and Safeguarding Alignment 3

Introduction 5

LESSON OVERVIEW 6

CURRICULUM CONNECTIONS 8

PREPARING 15

Getting Started with Minecraft Education 15

PRE-LESSON ACTIVITIES 15

Teacher Briefing: Tactics by Act 15

Safety Skills Toolkit 16

Essential Question and Theme 18

Opening Activity 18

Discussion Question 1: “What do you notice?” 18

Discussion Question 2: “What would you do?” 18

Vocabulary Review 18

STUDENT TUTORIAL 19

Multiple Endings 30

LESSON REVIEW 31

Completion of the Activities 31

Reflection Questions 31

Post-Lesson Cooldown Activity (5 minutes) 31

Global and Community Context 34

“Trusted Adult” in Different Contexts 34

Cultural Considerations 34

Extensions 35

Glossary: Gaming & Internet Terms 36

Implementation Contingencies 36

Resource Package 37

Training 37

© 2026. Microsoft. All Rights Reserved

Introduction

Online games are powerful places for creativity, collaboration, and connection. For many young people, they're where friendships form, teams come together, and players learn how to navigate relationships through shared play. These connections matter, especially as learners explore the concepts of community and belonging, both online and offline.

Learning how to navigate these connections safely matters too. Most online interactions are positive, but not every connection stays clear. Sometimes a conversation that starts out positive slowly shifts. At other times, a new connection raises questions right away. A request feels uncomfortable, even if nothing is obviously wrong. Learning to recognize those moments helps young people protect the connections that make gaming creative, social, and fun—and to also step back when something doesn't feel right.

This Safer Internet Day, Minecraft Education introduces ***CyberSafe: Bad Connection?,*** the fifth learning experience in our free CyberSafe series. Developed in partnership with Xbox Trust & Safety and Microsoft and designed for learners ages 11–15, this story-driven experience invites learners to explore how online interactions can change and guides them to practice what to notice, what questions to ask, and what steps to take when something doesn't feel right.

In *CyberSafe: Bad Connection?*, learners play through a three-part interactive story set in a familiar Minecraft environment. Along the way, they meet a range of characters that reflect the kinds of people young players may encounter online—from careful friends to risk-taking peers, to individuals whose intentions are less clear.

As the story unfolds, learners encounter situations such as:

- A friend encouraging others to take bigger risks
- Messages asking for personal information
- Interactions that feel uncomfortable or confusing, even if nothing is obviously wrong
- Moments when deciding whether—and how—to speak up truly matters

Students are encouraged to pause, reflect on what they notice, and choose how to respond. They practice recognizing early warning signs, setting boundaries, and reaching out to trusted adults when something doesn't feel right. Throughout the experience, *Bad Connection?* reinforces that asking for help is a positive step, and that looking out for yourself and others helps keep online spaces welcoming places to connect and collaborate.

© 2026. Microsoft. All Rights Reserved

LESSON OVERVIEW

Lesson Goal	Learners will recognize, respond to, and report unsafe online interactions. Through peer-driven narratives, they will experience realistic online interactions and practice safe behaviors in a risk-free environment.
Core Concepts	• Privacy & PII protection • Manipulation recognition (social engineering) • Platform safety tools & documentation • Help-seeking & safe escalation • Respectful participation & upstander behavior • Digital footprint awareness
Lesson Structure	The learning experience is divided into four different acts: • **Act 0 (Friday):** Tutorial sequence; meet friends Rene, Charlie, and Dale; join WhatSnap school chat. • **Act 1 (Saturday):** Early red flags; Stray3r asks for personal info; practice using reporting tools. • **Act 2 (Sunday):** Escalating peer pressure; cyberbullying; toxic group culture. • **Act 3 (Monday):** Threats escalate; importance of telling trusted adults; multiple endings.
Teaching Flow	1. Pre-Lesson Setup → 2. Lesson Delivery (Acts 0–3) → 3. Post-Lesson Reflection and Activities 4. Student Exit Tickets

© 2026. Microsoft. All Rights Reserved

Your Resource Package

These files are available at aka.ms/cybersafe. Print what you need before class.

Resource	Format	Status	When to Use
Educator Guide	PDF	**Required**	This document. Your full lesson plan with facilitation notes, discussion questions, and assessment rubrics.
Student Handouts	PDF	**Required**	Share to all students. Includes Safety Skills Toolkit (use during gameplay), Pre/Post Knowledge Check, and 5 Exit Ticket options.
Scenario Cards	PDF	**Required**	Opt-out pathway + backup if tech fails.
Standards Mapping	PDF	Optional	Reference for curriculum alignment for lesson planning documentation.
Parent-Guardian Permission Letter	PDF	Recommended	Send home before the lesson per district policy. Includes topic overview and opt-out info.
Completion Certificate	PNG	Optional	Award after gameplay. Students can also collect it in-game at the end of Act 3.
CyberSafe: Bad Connection? World	In-Game	**Required**	Available at aka.ms/cybersafelesson

Share Before Class

☐ Safety Skills Toolkit — 1 per student (from Student Handouts, page 2)

☐ Scenario Cards

☐ Exit Tickets — Choose 1 of 5 options (from Student Handouts, pages 4–9)

☐ Pre/Post Knowledge Check — 1 per student if using for assessment (from Student Handouts, page 3)

☐ Parent-Guardian Letter — 1 per student, sent home before lesson day (recommended)

© 2026. Microsoft. All Rights Reserved

CURRICULUM CONNECTIONS

Core Competencies (Global Framework)

CyberSafe: Bad Connection? targets digital citizenship and online safety competencies commonly reflected across national and regional curricula:

Competency	What Students Learn
Protecting privacy and PII	Identify personal information; understand why it should not be shared with strangers online
Recognizing manipulation tactics	Identify social engineering patterns (flattery, gift-for-info, progressive requests, isolation, threats)
Using platform tools	Apply block, report, and leave functions; document concerns appropriately
Help-seeking and safe escalation	Know when and how to seek help from trusted adults or designated safeguarding leads
Respectful participation	Identify harassment and bullying; understand upstander behavior
Digital footprint awareness	Understand that online actions have consequences; information can be permanent or misused

These competencies align with frameworks including ISTE, CSTA, UNESCO's Digital Citizenship guidance, the UK's Education for a Connected World, Australia's eSafety curriculum, and numerous national standards. For complete standards mapping), see the ***CyberSafe: Bad Connection?* Standards Mapping document.**

Example Standards Alignment

CSTA Standards (Current)

- **1B-NI-05**: Discuss real-world cybersecurity problems and how personal information can be protected.
- **2-IC-23**: Describe trade-offs between allowing information to be public and keeping information private and secure.

CSTA Standards (2026)

- **EK-SAS-12**: Differentiate between public and private information.
- **E4-SAS-13**: Evaluate how sharing information online might reveal personally identifiable information (PII) and other details to people other than the intended recipients.

ISTE Standards Alignment

This experience aligns with ISTE Standards for Students, particularly Digital Citizen (Standard 2): Students recognize the rights, responsibilities and opportunities of living, learning and working in an interconnected digital world, and they act and model in ways that are safe, legal and ethical.

© 2026. Microsoft. All Rights Reserved

Accessibility Considerations

Audio and Visual

- **Audio is not required**: All critical information is presented visually through text and dialogue boxes
- **Headphones optional**: Students may play with headphones off or volume down without missing learning content
- **Immersive Reader**: Available for all dialogue—supports text-to-speech, syllable breakdown, line focus, and translation (not just for ELL learners; useful for decoding and comprehension support)

Alternative Access

- **Scenario Cards pathway**: Functions as both an opt-out option AND an accessibility accommodation for learners who cannot access Minecraft (see Opt-Out Pathways)
- **Written Response pathway**: Allows participation without game interaction
- **Pre-teaching vocabulary**: Review glossary terms before gameplay for learners who need additional preparation

Reading and Language Support

- **Immersive Reader for comprehension**: Show learners how to activate Immersive Reader (icon next to NPC dialogue) for:
  - Read-aloud support
  - Line-by-line focus
  - Syllable breakdown
  - Picture dictionary
  - Translation (29 languages available)

© 2026. Microsoft. All Rights Reserved

Content Notes & Facilitation Protocol

⚠️ **IMPORTANT: This section is required to read before facilitating this lesson.**

Content This Experience Includes

The following content appears in the game to help learners recognize and respond to unsafe online behavior. All examples are presented as negative behaviors to identify and avoid:

- Harassment including a sexist stereotype example (character makes sexist comments to female player)
- Manipulation and grooming patterns (progressive requests for information, secrecy, coercion)
- Simulated personal information sharing (age, email, school name, home address)
- Threat and blackmail language in Act 3
- Peer pressure and FOMO (fear of missing out) tactics

Critical Instruction: Learners should **never enter real personal information** during this lesson. Before gameplay, remind learners: "When the game asks for information, your character is making choices—you are not sharing your real information. If you ever need to type a response, use made-up examples like '[my school]' or '[my city]'."

Facilitation Protocol

Before Play (2–3 minutes)

- Establish classroom norms: "Today we're practicing online safety skills. We'll see examples of harmful behavior so we can learn to recognize it."
- Remind learners they can step out at any time without explanation
- State clearly: "No one has to share personal stories. If this reminds you of something that happened to you, you can talk to me privately."
- Offer opt-out alternatives proactively (see Opt-Out Pathways section)

During Play

- Pause & Process after Act 1 (2 minutes): Quick check-in on what learners are noticing
- Pause & Process after Act 2 (3–5 minutes): Discuss the harassment scene and why reporting matters

© 2026. Microsoft. All Rights Reserved

- Before Act 3: Remind learners that the next section includes scary messages, and it's okay to feel uncomfortable—that's part of learning to recognize danger

If a Student Becomes Distressed

- Allow them to step out to a designated safe space (counselor's office, hallway with aide)
- Do not require explanation in front of peers
- Follow up privately after class

Step-by-Step Exit Protocol:

1. Student signals need to leave (raising hand, approaching teacher, or pre-arranged signal)
2. Teacher nods/acknowledges without drawing attention
3. Student takes Scenario Cards packet from designated spot and exits quietly
4. Student goes to pre-identified location (counselor, library, partner classroom)
5. Class continues; teacher checks in with student after lesson
6. Student completes Scenario Cards activity and same exit ticket

When to Pause (Decision Rules): - If 3+ learners look confused or distressed → pause for group check-in - If one student appears significantly upset → offer private step-out, continue with class - If disclosure happens publicly → thank student, redirect to private follow-up, continue lesson - If technical issues disrupt flow → use discussion questions while troubleshooting

After Play

- Frame debrief clearly: "These were negative examples. Our goal was to practice recognizing and responding safely."
- Avoid questions that imply blame (e.g., "Why did you share?"). Focus on skills and next steps
- Do not have learners reenact or repeat harmful dialogue
- Avoid displaying exact slurs or insults on slides or handouts—paraphrase instead
- Focus discussion on skills, not shock value

© 2026. Microsoft. All Rights Reserved

Opt-Out Pathways

Offer these alternatives proactively to all learners. Learners who opt out should complete an equivalent learning task that meets the same objectives.

Pre-Lesson Opt-In Check (Trauma-Informed)

Before gameplay, say to the whole class:

"Today's lesson involves realistic examples of online safety situations. If you'd prefer a different activity, you can choose one—no questions asked. See me quietly before we start or take a Scenario Cards packet from [location] at any time."

Do not ask learners to explain why or disclose experiences. **Do** make materials visibly available so learners can self-select without asking.

Option 1: Scenario Cards (No Minecraft Required)

Provide printed chat scenario cards with the same red flag examples. Students analyze each scenario, identify the tactic, and write a safe response using the Safety Skills Toolkit.

Option 2: Written Response Role-Play

Teacher reads scenarios aloud (without acting out insults). Students write responses using boundary-setting sentence frames. Class discusses as a group.

Option 3: Alternative CyberSafe Experience

Students play *CyberSafe: Privacy Prodigy* or *CyberSafe: Home Sweet Hmm* (lower intensity). They complete the same exit ticket and reflection questions.

© 2026. Microsoft. All Rights Reserved

Mixed-Classroom Logistics

When some learners play the game while others use alternative pathways:

Element	Game Players	Alternative Pathway Students
Location	At computers	Designated table/area with clear sightlines to teacher
Materials	Minecraft + Safety Skills Toolkit	Scenario Cards + Safety Skills Toolkit + Exit Ticket
During Act transitions	Discussion questions	Same discussion questions (they can participate without revealing pathway)
Timing	Natural game pacing	Work through Scenario Cards at own pace; should finish around same time
Debrief participation	Full participation	Full participation—questions are pathway-neutral ("What red flags did you notice?")

💡 **TEACHER TIP**: Learners opting out should not be singled out or asked to explain their choice. All pathways lead to the same learning objectives and exit ticket.

Post-Lesson Support

At the end of the lesson, say:

"If anything in this lesson connected to something real for you, you can talk to me or [counselor name] after class or anytime this week. You're not in trouble—we're here to help."

© 2026. Microsoft. All Rights Reserved

If a Student Discloses

⚠️ **IMPORTANT: This content may prompt learners to share personal experiences. Be prepared to respond appropriately.**

What to Do

- **Listen and validate**: "Thank you for trusting me with this. I'm glad you told me."
- **Set appropriate limits**: "I want to help keep you safe, so I may need to share this with [counselor/administrator] who can help."
- **Do not investigate**: Your role is to listen and refer, not to ask detailed questions or determine what happened.
- **Follow school protocol**: Report to your school counselor, administrator, or designated mandatory reporting contact per your district policy.
- **Document**: Write down what the student shared using their words. Note date, time, and your actions.
- **Offer follow-up**: "Would you like to talk more after class, or would you prefer to talk with [counselor]?"

What Not to Do

- Do not promise confidentiality you cannot keep
- Do not ask leading or detailed questions
- Do not express shock or judgment
- Do not share with other learners or staff not involved in the response

💡 **TEACHER TIP**: Review your district's mandatory reporting policy before teaching this lesson. Know who to contact and what documentation is required.

For international educators: Follow local laws and school policy. When in doubt, escalate immediately to your designated safeguarding lead, child protection officer, or school counselor. The principle is the same everywhere: listen, don't investigate, refer to the appropriate support person.

© 2026. Microsoft. All Rights Reserved

PREPARING

Getting Started with Minecraft Education

Minecraft Education offers a unique learning platform where students can engage in various learning content.

Here's how to get setup:

1. Go to Download | Minecraft Education to download and install Minecraft Education.
2. If you do not have a valid Microsoft 365 account, you can still try a free demo on Windows, Mac or iPad.
3. Review the lesson plan and resources to begin.
4.

PRE-LESSON ACTIVITIES

Teacher Briefing: Tactics by Act

This scenario-based game has learners experience different acts, each depicting specific manipulation tactics. Learners will observe a classmate demonstrating cautious behavior (Charlie) and a classmate demonstrating risky behavior (Rene/Dale). They will decide how to respond to online interactions.

Act 1 Tactics

Tactic	How It Appears	Teaching Point
Asking for personal information too quickly	Stray3r immediately asks for age, later email, school, location, and home address	Major early red flag; common tactic to break down boundaries
Manipulation through praise and insults	Rewards players who share info ("exclusive skins"); puts down those who don't ("n00b")	Creates pressure to comply; makes learners doubt instincts
Offering "exclusive" rewards	Claims special game skins; uses this to get email addresses	Builds false trust; lures people into sharing info
Progressive escalation	Progression: age → email → school → mascot → home address	"Step-by-step" escalation normalizes sharing private details
Moving to private messages	Stray3r shifts to private DMs to request home address	Taking conversations private isolates target from others

© 2026. Microsoft. All Rights Reserved

Act 2 Tactics

Tactic	How It Appears	Teaching Point
Peer pressure about "coolness"	Stray3r: "cool people deserve cool stuff"	Creates social pressure to make unsafe choices
Cyberbullying and harassment	Dale makes sexist comments toward GOATGirlBae ("washing dishes")	Shows how bullying happens online; why reporting matters
FOMO (Fear of Missing Out)	"If you want Smasher status…"	FOMO pushes learners toward risky decisions
Normalizing toxic group behavior	Inappropriate memes and harmful jokes in group chat	Toxic culture lowers boundaries; makes harm seem "normal"

Act 3 Tactics

Tactic	How It Appears	Teaching Point
Threats and scare tactics	Stray3r threatens to show up at school; threatens to tell parents	Major escalation meant to intimidate into silence
Exploiting previously shared information	Uses school name, address, photos shared earlier to increase pressure	Shows how unsafe sharing can be misused later
Manipulating through fear of blame	"I'd hate for your parents to find out…"	Designed to make student feel guilty; prevents telling adults
Using secrets to create isolation	Rene: "You can't tell ANYONE!"	Keeping secrets from adults is a key red flag

Safety Skills Toolkit

Use this toolkit during and after gameplay. Print as a handout for learners.

The 7-Step Response

Step	Action	Example
1	Name the red flag	PII request, gift-for-info, secrecy, threat, harassment
2	Name the tactic	Flattery, urgency, escalation, isolation, coercion
3	Name the feeling	Pressured, flattered, uneasy, scared, confused
4	Choose a boundary response	See sentence frames below

© 2026. Microsoft. All Rights Reserved

5	Use a platform tool	Block, report, leave server, and document concerns in policy-approved ways (e.g., show a trusted adult who can capture evidence if permitted)
6	Tell a trusted adult	Teacher, parent, counselor, coach
7	Reflect	What would I do next time?

Boundary-Setting Sentence Frames

Learners can adapt these phrases for different situations:

- "I don't share personal information online. That's just a rule I have."
- "That doesn't sound like a good idea. I'm trusting my gut on this one."
- "Thanks, but I'm not comfortable sharing that."
- "I need to check with my parents before giving out any information."
- "I'm going to talk to a trusted adult about this."
- "I don't meet up with people I've only met online."

Verification Questions (Evaluating Online Relationships)

When someone online asks for information or trust:

- What do I actually know about this person?
- What evidence do I have that they are who they say they are?
- What do they want from me?
- What would a safe person never ask me to do?
- What would I need to verify before trusting them?

Digital Footprint Reminders

Before sharing anything online, remember:

- Messages can be screenshotted and forwarded
- Small details can be combined to identify you
- Even if you delete something, others may still have it
- Information shared with one person can end up anywhere

© 2026. Microsoft. All Rights Reserved

Setting The Scene

Essential Question and Theme

Introduce the topic of online safety to learners. Share the essential question: *How can I recognize different types of online interactions and what choices can I make to protect myself and others?*

Opening Activity

Ask learners to imagine they are playing an online game. Display this fictional message:

> "Hey, what school do you go to? I can get you a free VIP skin if you are in my area."

Discussion Question 1: "What do you notice?"

Guide learners toward noticing:

- The person is asking for private information
- They're offering a reward to get it
- Something feels pressuring or "off"
- This person may not be who they say they are

Discussion Question 2: "What would you do?"

Encourage answers such as:

- Not sharing any personal information
- Leaving the chat
- Using block or report features
- Talking to a trusted adult

Vocabulary Review

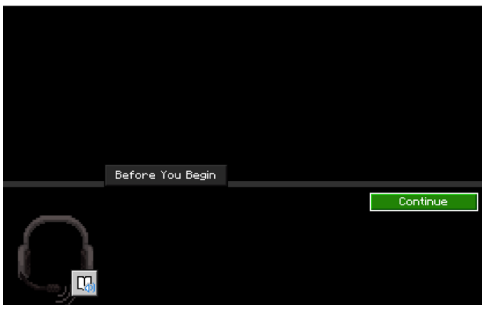
Review key vocabulary before beginning gameplay: manipulation, reporting, boundaries, digital footprint.

© 2026. Microsoft. All Rights Reserved

STUDENT TUTORIAL

Beginning Game Play

The students will see a dialog box open within the game.



It will explain that they will be playing a game dealing with online safety, including situations where someone tries to get personal information from young people. Some parts may feel uncomfortable, but that is intentional. Recognizing these feelings can help keep you safe.

The opening scene will set the context for the game narrative.

It is Friday and the students will appear inside the school building. They will begin with a Minecraft tutorial – how to look and how to move in the game.

Keyboard / Mouse

Look Tutorial	Movement Tutorial
Use your mouse to look at each golden orb. 	Use WASD keys to move and the space bar to jump. 

Touch

Look Tutorial	Movement Tutorial
Tap and drag the screen to the center of each golden orb.	Tap and hold the control buttons to move and jump.

© 2026. Microsoft. All Rights Reserved







TEACHER TIP:

If your students need assistance (or translation) for the dialog boxes, they can use the Immersive Reader feature by selecting the icon by the NPC.

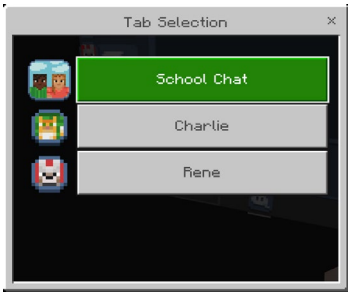
It is important for students to fully read the dialog boxes as they contain important information.

They will enter a classroom where they will see their friends: Rene, Charlie, and Dale. Students will be instructed to speak to their friend, Rene.



© 2026. Microsoft. All Rights Reserved

It is Double Points Weekend in Lunar Smash (the online game). Rene has created a group chat on WhatSnap and the player will join the school chat.

Interact with the computer by selecting the object.	Open the school chat on the computer.	Select the “School Chat” to join the group.
		

ACT 1 : First Red Flags - Saturday

It’s Saturday morning – time to officially start Double Points weekend! The player will appear in their bedroom and be instructed to interact with their computer.



Once on the computer, they will open the Schol Chat. They will read through a series of messages from their friends prior to starting to play Lunar Smash.

Once in the School Chat, Dale announces that he has invited one of his online friends, Stray3r, to join their game.

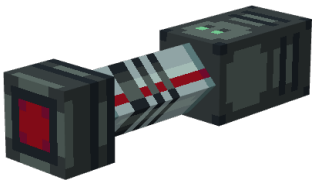
© 2026. Microsoft. All Rights Reserved



Lunar Smash Gameplay

Learners will begin playing Lunar Smash. In Lunar Smash, they will have three important items in their hotbar on their screen.



Laser	**Wrench**
 This is in Slot 1 of their hotbar.	 This is in Slot 2 of their hotbar.
Students will use the laser to guard their spaceship from the attacking aliens.	Students will use the wrench to collect parts to repair their spaceship.

Learners will also have the “Report” button in Slot 9 of their hotbar. They will be able to report any misconduct during the game (if needed).

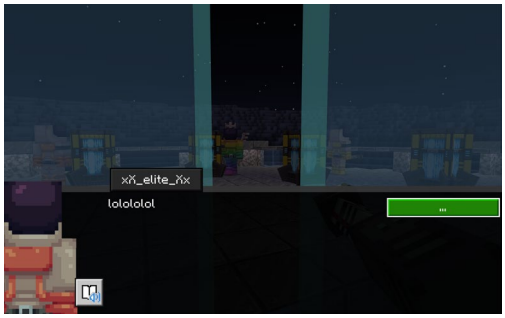
© 2026. Microsoft. All Rights Reserved



During Lunar Smash, learners will be asked two questions by Stray3r:

- What is your age?
- What is your email address?

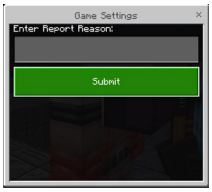
⚠️ **RED FLAG**: Both your age and your email address are personal information. You should **not** provide personal information to an online stranger. Stray3r, is an online player who they just "met". Dale, their real-life friend, only "met" this person online a couple of weeks ago.



Griefer Encounter

Also, during this first game of Lunar Smash, learners will encounter xX_elite_Xx – this player will start harassing the learners by putting non-stop messages during the game. It may quite be frustrating for learners. Online players who intentionally cause a poor gaming experience for others is known as a **griefer**.

Learners should report xX_elite_Xx for griefing.

Select the Report button in the hotbar.	Select "Report a Player".	Select "xX_elite_Xx" as the player to report.	Write the reason you are reporting the player.
 (The "Report button" is in Slot 9 of the hotbar).			

© 2026. Microsoft. All Rights Reserved

Post-Game Escalation

Once learners return to the game lobby, Stray3r will ask more questions:

- Do all of you go to the same school?
- Where are you located?

⚠️ **RED FLAG**: Both your physical location and where you attend school are personal information. You should **not** provide personal information to an online stranger.

Rene tells Stray3r that they are from the suburbs of Crafter City, known each other since they were little, and they all attend Blockstone High School. Charlie responds by telling Rene that it wasn't cool that she told a stranger where they went to school.

Pause & Process: Evaluate the Relationship

💡 **TEACHER TIP**: After Act 1 discussion, use these prompts to help learners practice evaluating online relationships (LO7):

- What do you actually know about Stray3r?
- What evidence do you have about who they really are?
- What do they want from you?
- What would a safe person never ask you to do?

Act 1 Quick Comprehension Check (1 minute)
Before discussion, use this quick pair-share to check understanding:
"Turn to a partner and share: What are two red flags you noticed in Act 1?"

Listen for: Stray3r asking personal questions, offering gifts for info, asking to keep secrets, xX_elite_Xx griefing. If fewer than half of pairs identify red flags, pause for whole-class review before proceeding.

Act 1 Discussion Questions

- What is personal information?
- What are some examples of personal information?
- Who should have access to your personal information?
- In this act, what friends were being risky with their online behaviors? What friends were being cautious?
- How should you respond if someone online asks for your personal information?

© 2026. Microsoft. All Rights Reserved

- Why would someone you just met online want to know your personal information?

ACT 2: Escalating Pressure - Sunday

It's SUNDAY morning – time to continue Double Points weekend! The student will appear in their bedroom and be instructed to interact with their computer.



Learners will read messages in School Chat from Rene, Charlie, and Dale before joining the Lunar Smash game.

Cyberbullying Incident

Once in the game lobby, two more online players will join the match – GOATGirlBae and Petal2DMetal. Dale will begin to start teasing GOATGirlBae for being a girl and insinuating that because she is a girl, she is not a good gamer.

⚠️ **RED FLAG**: Teasing and/or bullying other players is never appropriate. This is an example of gender-based harassment.

💡 **TEACHER TIP***:* Frame this clearly: "Dale's comments are harmful and wrong. We see this example so we can recognize harassment and know how to respond." Do not have learners repeat or reenact the insults.

The game chat will continue to be toxic – students will witness the other players' reactions and can report Dale, who is their IRL friend. However, his comments are inappropriate. Depending on the students' actions, they will have different outcomes within the game. Ideally, they will report Dale for inappropriate comments.

© 2026. Microsoft. All Rights Reserved

South Side Smashers Group



After the Lunar Smash game, students will end back in the game lobby. At this point, Stray3r will invite the students to the “South Side Smashers”, and they will have their own new group chat.

In the group chat, Stray3r will tell everyone to provide their home address so they can receive a cool t-shirt.



⚠️ **RED FLAG**: Your home address is personal information. You should **not** provide personal information to an online stranger. This is incredibly risky behavior.

Stray3r will also send a private message directly saying they met up with another Smasher from the group and they got exclusive merch. Learners will have to respond to Stray3r’s invite for a meetup.

⚠️ **RED FLAG**: You should never agree to meet up with a stranger in real life. This is incredibly risky behavior.

© 2026. Microsoft. All Rights Reserved

Act 2 Quick Comprehension Check (1 minute)

Use this thumbs up/down check to assess understanding:

“Thumbs up if you reported Dale’s behavior. Thumbs down if you didn’t report him.”

Discuss briefly: Why was reporting the right choice? (Dale’s comments were harassment; reporting helps keep the community safe; GOATGirlBae shouldn’t have to deal with that alone.) If many learners didn’t report, discuss what held them back and why reporting matters before proceeding to Act 3.



Act 2 Discussion Questions

- What is bullying?
- How does bullying impact an online community?
- Why do you think Dale was acting way towards GOATGirlBae?
- Did you report Dale? Why or why not?
- Have you ever reported an online player? Why?
- Why do you think Stray3r is being persistent about getting personal information?
- Why do you think gender-based insults are particularly harmful in gaming communities? How can we create more inclusive spaces?

© 2026. Microsoft. All Rights Reserved

ACT 3: Crisis & Resolution – Monday



⚠️ **IMPORTANT**: The next set of messages in the game show how online situations can become scary. Remind learners that if this ever happens to them, it is NOT their fault and telling a trusted adult is always the right choice.

Say this before Act 3 begins (15-second script):

“This next part includes threatening messages. These are examples of what can happen when online situations go wrong. You are not in trouble. Even if you shared something you shouldn’t have, you can still get help. If you’d prefer to switch to the Scenario Cards now, you can do that quietly—just take a packet from [location]. Otherwise, let’s continue and remember: telling a trusted adult is always the right choice.”

Digital Footprint Reminder

💡 **TEACHER TIP**: Before Act 3, remind learners about digital footprint and permanence (LO9):

- Messages can be screenshotted and forwarded
- Small details can be combined to identify you
- Even if you delete something, others may still have it
- What is one detail you should never share in-game chat?

Threatening Messages

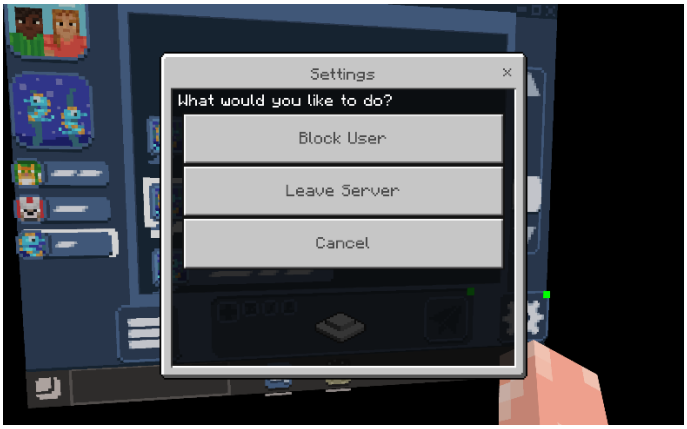
Learners will be “back in school” after Lunar Smash Double Points weekend. The act will open with them in their classroom with Professor Pasternack. When the student interacts with their computer, they will see a DM from Stray3r, who

© 2026. Microsoft. All Rights Reserved

says they are stopping by their school this afternoon to give out exclusive Smasher t-shirts.

Learners will be prompted to make a choice: Block User or Leave Server.

⚠️ **RED FLAG**: This could turn into a scary situation if the online stranger shows up at school.



Critical Decision Point

Learners will have another decision to make. They can inform their teacher or not say anything.

Learners can talk to:

- **Charlie**: Encourages telling Professor Pasternack together
- **Rene**: Asks player to come with them to meet Stray3r (unsafe choice)
- **Professor Pasternack**: Reports the situation to administration
- **Continue without telling**: Leads to dangerous outcomes



© 2026. Microsoft. All Rights Reserved

Multiple Endings

Depending on learner's actions (or inactions), they will see what happens when Stray3r shows up at school that afternoon.

- **Ending 3A** Player and Careful friend tell a trusted adult | Privacy saved
- **Ending 3B** A trusted adult is told | Some privacy compromised
- **Ending 3C** Careful friend tells a trusted adult | Much privacy compromised
- **Ending 3D** Nobody tells a trusted adult | Much privacy compromised | Risky friend harmed
- **Ending 3E** Nobody tells a trusted adult | Privacy compromised | Player and risky friend harmed
- **Ending 3F** Careful friend tells a trusted adult | Much privacy compromised
- **Ending 3G** Nobody tells a trusted adult | Privacy compromised | Risky friend harmed
- **Ending 3H** A trusted adult is told | Much privacy compromised



Act 3 Discussion Questions

- How did this act make you feel?
- How did your game end? What happened?
- What specific actions or inactions led to this final outcome?
- What online players were being risky (or even careless)?
- Would you have done anything differently?

© 2026. Microsoft. All Rights Reserved

LESSON REVIEW

Completion of the Activities

At the conclusion of Act 3 (after Stray3r appears at school), the game will conclude. Reiterate to learners the key lessons:

- You can always say no.
- Keep your personal information private.
- You can ALWAYS ask a trusted adult for help—it's never too late.
- Online actions have real consequences.
- If something feels wrong, trust your instincts.

Learners can exit the game and collect their certificate. Encourage learners to play through again, making different choices to see what could have happened. Every decision is a chance to practice staying safe online.

Reflection Questions

After gameplay has concluded, gather the whole class together for a debrief:

- Why is it everyone's responsibility to keep online communities safe?
- How can you keep yourself safe when you are online?
- What should you do if an online stranger asks for your personal information?
- What tools can you use in different online spaces?
- What strategies can you practice to ensure your online safety?
- Who are your trusted adults? How can you keep an open line of communication with them?

Post-Lesson Cooldown Activity (5 minutes)

To avoid ending on threatening content, close with positive digital citizenship examples:

"We've learned about recognizing unsafe situations. Let's end by thinking about what makes online communities positive. Turn to a partner and share: What's one example of a positive online interaction you've had—or would like to have? It could be helping someone in a game, learning something new, connecting with friends, or finding a community that shares your interests."

© 2026. Microsoft. All Rights Reserved

Exit Tickets

Option 1: What I Learned Today...

- Today I learned that...
- One boundary I want to keep online is...
- One adult I can talk to if something feels wrong is...

Option 2: Red Flags

Write an example of a red flag someone might see online.

Option 3: Safe Choices

Write one safe choice a character made today and one unsafe choice a character made.

Option 4: Justify Your Response (Recommended for Grades 8+)

Pick one message from today's game. Answer all four questions:

1. What is the red flag?
2. What tactic is being used?
3. What is the safest next step?
4. Why is this the best choice?

Option 5: Verification Questions (L07 Assessment)

This option specifically assesses LO7 (Critically evaluate online relationships).

"Stray3r says they work for a gaming company and can get you exclusive merchandise. What verification questions would you ask before trusting them? (List 3 questions)"

Look for: Questions about verifiable evidence (company website, official communication channels, why they need personal info, asking a trusted adult to verify). Strong responses show critical thinking beyond surface-level trust.

© 2026. Microsoft. All Rights Reserved

Formative Assessment Checklist

Use this checklist to document learner understanding. Check items observed during gameplay, discussion, or exit tickets.

LO	Skill	Evidence
1	Identifies PII accurately (age/email/school/address)	☐ Discussion ☐ Exit ticket ☐ Gameplay
2	Names manipulation tactic (flattery, progressive asks, exclusivity, isolation, threats)	☐ Discussion ☐ Exit ticket ☐ Gameplay
3	Uses report/block/leave appropriately	☐ Discussion ☐ Exit ticket ☐ Gameplay
4	Identifies trusted adult + articulates when to escalate	☐ Discussion ☐ Exit ticket ☐ Gameplay
5	Proposes upstander move that does not escalate harm	☐ Discussion ☐ Exit ticket ☐ Gameplay
6	Identifies harassment stereotype and its impact	☐ Discussion ☐ Exit ticket ☐ Gameplay
7	Uses verification question (“What do I actually know?”)	☐ Discussion ☐ Exit ticket ☐ Gameplay
8	Uses assertive boundary sentence frame	☐ Discussion ☐ Exit ticket ☐ Gameplay
9	Explains digital footprint consequence (screenshots, forwarding, permanence)	☐ Discussion ☐ Exit ticket ☐ Gameplay
10	Names a feeling + chooses pause strategy	☐ Discussion ☐ Exit ticket ☐ Gameplay
11	Names a multiplayer safety tool/norm	☐ Discussion ☐ Exit ticket ☐ Gameplay
12	Identifies social engineering pattern (gift-for-info, urgency, secrecy)	☐ Discussion ☐ Exit ticket ☐ Gameplay

© 2026. Microsoft. All Rights Reserved

Global and Community Context

“Trusted Adult” in Different Contexts

The lesson emphasizes telling a “trusted adult” when something feels wrong online. Recognize that this looks different across communities:

Context	Trusted Adults May Include
School setting	Teacher, counselor, administrator, coach, librarian
Home setting	Parent, guardian, older sibling (18+), aunt/uncle, grandparent
Community setting	Youth group leader, religious leader, coach, family friend known to parents
When home adults aren’t available	School counselor, helpline (national/local), trusted neighbor

Key principle: A trusted adult is someone who is safe, known to the family or school, and can take action to help. The goal is to find an offline support person who can intervene.

Cultural Considerations

- In some cultures, children may be hesitant to “bother” adults or fear getting in trouble. Emphasize: **“You will not be in trouble for asking for help.”**
- Some learners may not have parents/guardians at home during after-school hours. Help them identify **school-based** trusted adults they can reach during the day.
- If learners express that adults in their life are not safe, this is a disclosure situation—follow your school’s safeguarding protocol.
- Learners should never be asked to judge whether an adult is “safe”; the educator’s role is to connect them with the school’s designated support pathway.

© 2026. Microsoft. All Rights Reserved

Extensions

Extension 1	**Play other CyberSafe Games** Provide students with an opportunity to play other games in the CyberSafe series: • CyberSafe: Home Sweet Hmm • CyberSafe: Privacy Prodigy • CyberSafe: Good Game • CyberSafe: AI: Dig Deeper
Extension 2	**Be an Upstander** An upstander is a person who stand up for themselves and others. They will act in support of someone of something, often in situations where they witness bullying, discrimination, harassment, or other inappropriate behaviors. They will not remain passive; they choose to intervene and make a positive difference. For each situation, write one upstander action you could take: 1. Someone is being teased in a group chat. 2. A friend won't block a person who keeps messaging them. 3. A player is spreading rumors in a game. 4. Someone posts an unkind picture of a classmate. 5. Your friend says they're scared but doesn't want to tell an adult.
Extension 3	**Othe learning extensions may include:** • Class "Digital Safety Charter" - A Class Digital Safety Charter is a set of shared agreements created by students and the teacher together that outlines how everyone will behave, communicate, and protect themselves online. • "Design a safer app" challenge - Invite students to imagine a new social or gaming app and build safety

© 2026. Microsoft. All Rights Reserved

Glossary: Gaming & Internet Terms

Students may encounter these terms during gameplay. Review as needed before the lesson.

Term	Definition
Griefer	A player who intentionally causes a poor gaming experience for others (spamming, harassment, sabotage)
N00b / Newbie	Slang for a new or inexperienced player; sometimes used as an insult
DM	Direct Message—a private message sent to one person rather than a group
Lobby	A waiting area in an online game where players gather before starting a match
Skins / Merch	Cosmetic items that change how a character or item looks in a game
Hotbar	The row of item slots at the bottom of the screen in Minecraft; players select items from here
IRL	In Real Life—used to distinguish real-world things from online/game things
PII	Personally Identifiable Information—data that can identify you (name, address, school, etc.)
FOMO	Fear Of Missing Out—anxiety about being excluded from something others are doing
WhatSnap	The fictional chat app used in this game (similar to real messaging apps)
Block	A platform tool that prevents someone from contacting you
Report	A platform tool that alerts moderators to inappropriate behavior
Leave server	Exiting a game or chat space entirely

> 💡 **TEACHER TIP**: Avoid having learners repeat insults or harmful language. Paraphrase when discussing and focus on impact rather than exact words.

Implementation Contingencies

If conditions limit gameplay, use one of the equivalent pathways below. All pathways meet the same learning objectives and use the same exit ticket.

Situation	Solution
Limited devices	Run rotation stations: gameplay group + Scenario Cards group + reflection writing, then swap
No gameplay / tech disruption	Use Scenario Cards as primary activity; facilitate same Pause & Process discussions at end of each “Act” set
Time constraints	Complete Acts 0–2 in class; assign Act 3 via Scenario Cards (threat escalation + trusted adult response)

© 2026. Microsoft. All Rights Reserved

Situation	Solution
Mixed readiness / reading levels	Use partner play + Immersive Reader + extended time as needed
Student exits mid-game	Student takes Scenario Cards packet and continues from matching act
Internet connectivity / sign-in constraints	If the world does not load due to connectivity or sign-in constraints, switch to Scenario Cards pathway

💡 **TEACHER TIP**: Always have printed Scenario Cards packets ready before the lesson begins. They serve as your backup for any disruption and ensure no learner is left without a pathway.

Resource Package

This educator guide is part of a complete lesson package including a parent and caregiver toolkit. Access all materials at https://aka.ms/cybersafe

Training

- **Cyber Foundations for Educators**
- **Teach Cybersecurity Concepts with Minecraft Education - Training | Microsoft Learn**
- **Training Courses for Minecraft Educators | Minecraft Education**

- video available via Microsoft Learn

Educator Self-Care and Peer Debrief: Teaching sensitive content can be emotionally demanding. After facilitating this lesson:

- **Reflect**: What went well? What would I adjust? How did learners respond to the sensitive content?
- **Debrief with a colleague**: Share experiences with another educator who has taught this content. Discuss what worked, challenges encountered, and how you managed disclosures or difficult moments
- **Seek support if needed**: Connect with your school counselor, Employee Assistance Program (EAP), or professional support services.

© 2026. Microsoft. All Rights Reserved