CYBERSAFE: BAD CONNECTION?
COMPREHENSIVE LEARNING STANDARDS

Executive Summary

The design brief identifies three categories of learning outcomes:

Knowledge Objectives (What Students Will Know):

- Personal information should not be shared with people met online
- Red flags in online interactions (requests for info, pressure tactics, gifts, isolation)
- Reporting tools exist in platforms to address harassment and predatory behavior
- Trusted adults are resources when situations feel uncomfortable

Skill Objectives (What Students Will Do):

- Recognize manipulation tactics including flattery, exclusivity, progressive requests
- Respond with boundary-setting language
- Report inappropriate behavior using in-game tools
- Seek help from trusted adults when situations escalate
- Understand that online actions have permanent consequences and that shared information can be used in ways not originally intended
- Critically evaluate online relationships and understand that people may misrepresent themselves online; recognize risks of meeting people known only through digital communication

Behavioral Objectives (What Students Will Practice):

- Pausing before sharing information online
- Trusting instincts when something feels wrong
- Supporting peers who are being targeted
- Documenting concerning interactions for reporting
- Reporting to trusted adults

Expanded Learning Objectives Framework

CyberSafe: Bad Connection? aligns to **12 comprehensive learning objectives**

ID	Category	Learning Objective
LO1	Digital Privacy & Identity Protection	Understand what constitutes personal information and why it should not be shared with strangers online
LO2	Online Manipulation Recognition	Identify grooming tactics including flattery, gift-giving, exclusivity, progressive information requests, and isolation strategies
LO3	Digital Citizenship & Reporting	Use platform-specific reporting tools to address harassment, bullying, and predatory behavior
LO4	Help-Seeking & Trust	Recognize when to seek help from trusted adults and understand it's never too late to report concerning interactions
LO5	Peer Support & Upstander Behavior	Support peers experiencing online harassment or manipulation and recognize collective responsibility for online safety
LO6	Cyberbullying Recognition & Response	Identify cyberbullying behaviors (including gender-based harassment) and understand appropriate responses including reporting
LO7	Critical Evaluation of Online Relationships	Distinguish between appropriate and inappropriate online relationships and understand risks of meeting people known only online
LO8	Boundary Setting & Communication	Practice using assertive language to set boundaries and refuse inappropriate requests without escalating conflict
LO9	Digital Footprint & Consequences	Understand that online actions have consequences and that shared information can be permanent or misused
LO10	Emotional Awareness & Self-Regulation	Recognize emotional responses to online pressure (FOMO, guilt, fear) and practice pausing before responding
LO11	Online Gaming Safety	Apply safety principles specifically to multiplayer gaming environments including chat moderation and stranger danger
LO12	Social Engineering & Phishing Recognition	Recognize social engineering tactics designed to extract personal information through deception

Complete Standards Mapping

ISTE Standards for Students (2016)

The ISTE Standards provide a framework for leveraging technology for learning. CyberSafe: Bad Connection? aligns primarily with **Standard 2: Digital Citizen**.

Primary Alignments:

Learning Objective	ISTE Standard	Alignment Details
LO1, LO7, LO9, LO12	**2.2 Digital Citizen**	"Manage their personal data to maintain digital privacy and security and are aware of data-collection technology"
LO2, LO3, LO6, LO8	**2.2 Digital Citizen**	"Engage in positive, safe, legal and ethical behavior when using technology, including social interactions online"
LO2, LO7, LO9	**2.1 Digital Citizen**	"Cultivate and manage their digital identity and reputation and are aware of the permanence of their actions in the digital world"
LO4, LO12	**3.2 Knowledge Constructor**	"Evaluate the accuracy, perspective, credibility and relevance of information, media, data or other resources"
LO5, LO8	**7.2 Global Collaborator**	"Use collaborative technologies to work with others…to examine issues and problems from multiple viewpoints"
LO10	**1.1 Empowered Learner**	"Articulate and set personal learning goals, develop strategies leveraging technology to achieve them and reflect on the learning process"
LO8	**6.1 Creative Communicator**	"Choose the appropriate platforms and tools for meeting the desired objectives of their creation or communication"

CSTA K-12 Computer Science Standards (2017)

The CSTA Standards emphasize **Impacts of Computing** and **Networks and the Internet** concepts relevant to online safety. Target grade bands are **Level 2 (Grades 6-8)** and **Level 3A (Grades 9-10)**.

Primary Alignments:

Learning Objective	CSTA 2017 Standards
LO1 (Privacy & Identity)	2-NI-05 (security measures); 2-IC-23 (public vs. private information tradeoffs)
LO2 (Manipulation Recognition)	2-IC-20 (technology tradeoffs); 2-IC-21 (bias in technologies)

LO3 (Reporting Tools)	2-IC-22 (collaborate to address cyberbullying); Practice 1 (Inclusive Culture)
LO4 (Help-Seeking)	2-IC-20 (technology tradeoffs); Practice 2 (Collaborating)
LO5 (Peer Support)	2-IC-22 (address cyberbullying); Practice 1.2 (diverse users)
LO6 (Cyberbullying)	2-IC-22 (cyberbullying and harassment); 2-IC-23 (privacy implications)
LO7 (Online Relationships)	2-IC-20 (technology tradeoffs); 2-IC-23 (public vs. private)
LO8 (Boundary Setting)	Practice 7 (Communicating effectively); Practice 2 (Collaborating)
LO9 (Digital Footprint)	2-IC-23 (public/private tradeoffs); 2-NI-05 (security measures)
LO10 (Emotional Awareness)	Practice 1 (Inclusive Culture); Practice 2 (Collaborating)
LO11 (Gaming Safety)	2-IC-20 (technology impacts); 2-IC-22 (address harassment)
LO12 (Social Engineering)	2-NI-05 (security measures); 2-IC-23 (information privacy)

Regional Standards Alignments

AU New South Wales, Australia

Framework: Australian Curriculum - Digital Technologies (v9.0) + PDHPE (Personal Development, Health and Physical Education)

Key Alignments:

- **Years 5-6 Digital Technologies**: "Plan, create and communicate ideas and information, including collaboratively online, applying agreed ethical, social and technical protocols (ACTDIP024)" → **LO1, LO3**
- **Years 7-8 Digital Technologies**: "Acquire, manage, analyse and represent data to create information and address problems (ACTDIP025)" → **LO11, LO12**
- **Years 7-8 PDHPE**: "Examines and evaluates strategies to manage current and future challenges; demonstrates self-management skills to act responsibly and promote health, safety and wellbeing" → **LO4, LO6, LO10**
- **Online Safety Connection**: All objectives align with eSafety Commissioner's classroom resources focusing on recognizing online risks, unsafe situations, and seeking help

GB United Kingdom

Framework: Computing Curriculum (National Curriculum) + PSHE (Personal, Social, Health and Economic Education) + RSE (Relationships and Sex Education)

Key Alignments:

- **KS2 Computing** (Ages 7-11): "Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns" → **LO1, LO3, LO4**
- **KS3 Computing** (Ages 11-14): "Understand the opportunities networks offer for communication and collaboration; understand computer networks including risks such as phishing and social engineering" → **LO2, LO12**
- **KS2/KS3 PSHE**: "Internet safety and harms, including being subject to inappropriate online requests; how to recognize online grooming; how to ask for help and advice; respecting equality" → **LO2, LO4, LO5, LO6, LO7**
- **KS3 RSHE**: "The law relating to sexual consent, sexual exploitation, abuse, grooming, coercion, harassment, rape, domestic abuse, forced marriage, honour-based violence and FGM" → **LO2, LO7**

Note: BBC Teach provides specific resources on "Online Grooming" for KS3/KS4 Computing curriculum.

CA Ontario, Canada

Framework: Health and Physical Education Curriculum + Digital Literacy (integrated across subjects)

Key Alignments:

- **Grades 5-8 Health Education**: "Demonstrate the ability to apply health knowledge and living skills to make reasoned decisions and take appropriate actions relating to personal safety and injury prevention" → **LO1, LO4, LO7**
- **Grades 6-8 Health - Personal Safety**: "Distinguish between positive and negative relationships; describe characteristics of healthy relationships; demonstrate understanding of consent; identify factors influencing decision making" → **LO7, LO8, LO10**
- **Grades 6-8 Health - Communication**: "Demonstrate communication skills including refusal skills; apply decision-making strategies; demonstrate skills that help develop self-awareness and self-confidence" → **LO8, LO10**
- **Digital Literacy Integration**: Safe and responsible use of technology; recognizing exploitative relationships and knowing where to get help

🇺🇸 United States - State-Specific Alignments

Florida (CPALMS Standards)

Framework: Florida Computer Science Standards (2024) + Health Education Standards

Key Alignments:

- **SC.68.CS-PC.1.2**: "Describe the social and economic implications of privacy in the context of safety, law, or ethics" → **LO1, LO7, LO9, LO12**
- **SC.68.CS-PC.1.3**: "Describe appropriate and inappropriate online behavior" → **LO3, LO6**
- **SC.68.CS-PC.1.4**: "Describe social interactions in online environments" → **LO5, LO6, LO11**
- **SC.68.CS-CS.1.6**: "Explain safe computing practices for protecting personal identity online" → **LO1, LO12**
- **HE.6.C.2.4**: "Demonstrate effective communication when confronted with uncomfortable situations" → **LO8**
- **HE.7.B.5.2**: "Discuss ways to prevent and stop bullying" → **LO6**
- **HE.7.B.5.4**: "Examine barriers that prevent reporting of crimes, abuse or neglect" → **LO3, LO4**

Texas (TEKS - Texas Essential Knowledge and Skills)

Framework: Technology Applications TEKS (2024-25 implementation)

Key Alignments:

- **TA.6.10.A**: "Identify real-world cybersecurity problems such as phishing, malware, password attacks, identity theft, and hacking" → **LO12**
- **TA.6.10.C**: "Explain security impacts of phishing and social engineering" → **LO2, LO12**
- **TA.6.10.E**: "Discuss the impact of cyberbullying" → **LO6**
- **TA.7.10.B**: "Identify the impacts of choosing to share or not share information about oneself online" → **LO1, LO7, LO9**
- **TA.7.10.C**: "Demonstrate appropriate practices in digital communications" → **LO8**
- **TA.7.10.D**: "Practice responsible digital citizenship" → **LO3, LO5, LO10**
- **TA.8.10.B**: "Understand permanence of digital footprint" → **LO9**
- **TA.8.10.D**: "Understand risks of communicating personal information to unknown persons" → **LO2, LO7**

New York (NYSED Computer Science & Digital Fluency Standards)

Framework: NYS K-12 Computer Science and Digital Fluency Learning Standards (2020)

Key Alignments:

- **5-6.IC.3**: "Describe the positive and negative impacts of technology on personal and societal well-being" → **LO1, LO9**
- **5-6.IC.4**: "Identify and discuss problems that may emerge from use of computing devices" → **LO4**
- **5-6.IC.5**: "Describe how fake or misleading information is spread" → **LO3, LO12**
- **5-6.NSD.3**: "Explain potential security threats and security measures" → **LO2, LO12**
- **7-8.IC.1**: "Describe how others may have different perspectives based on individual or group needs" → **LO5, LO10**
- **7-8.IC.2**: "Describe impacts of sharing information about oneself and others online" → **LO1, LO7, LO9**
- **7-8.IC.3**: "Develop and promote guidelines for respecting rights and needs of others" → **LO3, LO5, LO6, LO8**
- **7-8.IC.4**: "Describe need for developers to consider cultural perspectives" → **LO4**
- **7-8.NSD.3**: "Explain potential security threats and security measures to address them" → **LO12**

California (Computer Science Standards)

Framework: California Computer Science Standards K-12 (2018)

Key Alignments:

- **6-8.IC.20**: "Compare tradeoffs between allowing information to be public versus keeping it private and secure" → **LO1, LO7, LO9, LO12**
- **6-8.IC.21**: "Discuss ways computing technologies can be used to connect to individuals who share interests or provide support" → **LO3, LO5, LO11**
- **6-8.IC.22**: "Describe how computing technologies have changed the way people live, work, communicate, and interact" → **LO2, LO9, LO11**
- **6-8.IC.24**: "Identify and describe equity issues caused by computing innovations" → **LO4**
- **6-8.IC.25**: "Discuss real-world computing technologies that raise legal and ethical concerns" → **LO6, LO10**
- **6-8.IC.27**: "Identify and discuss potential impacts of biased technologies" → **LO6**

- **6-8.NI.5**: "Explain potential security threats and measures to protect information" → **LO12**

Georgia (Standards of Excellence)

Framework: Georgia Standards of Excellence - Computer Science K-8 (2016)

Key Alignments:

- **CSS.EL.6-8.1**: "Use technology resources to increase self-direction and self-regulation in learning" → **LO10**
- **CSS.IC.6-8.1**: "Discuss the social impacts of computing innovations" → **LO9**
- **CSS.IC.6-8.3**: "Demonstrate respect for the rights and privacy of others when using technology" → **LO5, LO11**
- **CSS.IC.6-8.4**: "Examine appropriate and inappropriate uses of technology, including copyright, privacy, and security" → **LO1, LO6, LO7**
- **CSS.DC.6-8.1**: "Demonstrate knowledge of acceptable use policies regarding technology" → **LO7**
- **CSS.DC.6-8.2**: "Model the importance of asking permission before using resources created by others" → **LO3, LO8**
- **CSS.DC.6-8.3**: "Model respect for intellectual property and privacy of others" → **LO5**
- **CSS.DC.6-8.4**: "Identify and describe roles and responsibilities in computing community" → **LO4, LO10**
- **CSS.DC.6-8.5**: "Identify strategies to prevent and address cyberbullying" → **LO5, LO6**
- **CSS.DC.6-8.6**: "Report inappropriate behavior in digital communications" → **LO3**
- **CSS.NI.6-8.1**: "Identify types of network vulnerabilities and security threats" → **LO12**

Comprehensive Standards Mapping Table

The following table shows how each of the 12 learning objectives maps across all 12 standards frameworks:

Learning Objective	ISTE 2016	CSTA 2017	Regional Standards Summary
LO1: Personal Information & Privacy Protection	2.2, 2.4 Digital Citizen	2-NI-05, 2-IC-23	Strong alignment across all regions; cybersecurity and privacy core to all CS curricula
LO2: Manipulation & Grooming Recognition	2.1, 2.2 Digital Citizen	2-IC-20, 2-IC-21	UK PSHE explicit on grooming; Ontario Health Ed addresses exploitative relationships; all regions address social engineering
LO3: Platform Reporting Tools	2.2 Digital Citizen; 7.2 Global Collaborator	2-IC-22; Practice 1	Strong alignment; Georgia, Virginia, Maryland explicitly require "reporting inappropriate behavior"
LO4: Help-Seeking from Trusted Adults	2.2 Digital Citizen; 3.2 Knowledge Constructor	2-IC-20; Practice 2	Strong alignment especially UK PSHE, Ontario Health, Florida Health Ed, Maryland SI.3
LO5: Peer Support & Upstander Behavior	2.1 Digital Citizen; 7.1, 7.3 Global Collaborator	2-IC-22; Practice 1.2	Strong alignment; Georgia DC.6-8.5 explicit on cyberbullying prevention strategies
LO6: Cyberbullying Recognition & Response	2.1, 2.2 Digital Citizen	2-IC-22, 2-IC-23	Universal coverage; Texas, Florida, Georgia, Maryland explicitly address cyberbullying
LO7: Evaluating Online Relationships	2.1, 2.2 Digital Citizen	2-IC-20, 2-IC-23	Strong UK RSHE/PSHE alignment; Ontario consent education; partial coverage in some US state CS standards
LO8: Boundary Setting & Communication	2.2 Digital Citizen; 6.4 Creative Communicator	Practice 7; Practice 2	Ontario Health (refusal skills); UK PSHE (assertiveness); Florida Health (negotiation skills)
LO9: Digital Footprint & Consequences	2.1, 2.4 Digital Citizen	2-IC-23, 2-NI-05	Strong alignment; Texas TA.8.10.B explicitly addresses "permanence of digital footprint"
LO10: Emotional Awareness & Self-Regulation	1.1 Empowered Learner; 2.2 Digital Citizen	Practice 1; Practice 2	NSW/AU PDHPE, UK PSHE mental health, Ontario Health (stress/emotions); Georgia EL.6-8.1 self-regulation

LO11: Multiplayer Gaming Safety	2.2 Digital Citizen	2-IC-20, 2-IC-22	Moderate alignment; Florida SC.68.CS-PC.1.4 explicit on "online gaming environments"
LO12: Social Engineering & Phishing	2.2, 2.4 Digital Citizen; 3.2 Knowledge Constructor	2-NI-05, 2-IC-23	Strong cybersecurity alignment; Texas TA.6.10.A explicit on phishing; NY, CA, MD, VA strong NI standards

References & Standards Documentation

International Frameworks:

- ISTE Standards for Students (2016): https://iste.org/standards/students[^2]
- CSTA K-12 Computer Science Standards, Revised 2017: https://csteachers.org/k12standards[^3]

Regional Frameworks Researched:

- Australia: Australian Curriculum v9.0 Digital Technologies, PDHPE; eSafety Commissioner resources
- United Kingdom: National Curriculum Computing, PSHE Education, RSE statutory guidance
- Canada (Ontario): Health and Physical Education Curriculum, Digital Literacy frameworks
- USA - Florida: CPALMS Computer Science Standards (2024), Health Education Standards
- USA - Texas: TEKS Technology Applications (2024-25)
- USA - New York: NYSED Computer Science & Digital Fluency Standards (2020)
- USA - California: Computer Science Standards K-12 (2018)
- USA - Georgia: Georgia Standards of Excellence - Computer Science