Full Ethics Role-Play Pack

All educators | Reference

Ethics activities should assess reasoning, stakeholder awareness, evidence, and professional responsibility rather than reward one predetermined opinion. Each numbered H.x section is a separate prompt set, role-play tool, or debrief resource; bold labels beneath it belong to that resource. Explain the boundaries of the discussion, distinguish legal requirements from ethical judgments, and protect learners from pressure to disclose personal experiences.

H.1 K-6 Discussion Prompts

1. A classmate shares a photo of another student without asking. What should happen next, and why?
2. A game offers a reward for entering a parent's email address. What questions should the player ask before continuing?
3. Someone discovers a friend's password written where others can see it. What is the kind and safe response?
4. A student receives an unkind message and wants to repost it so everyone can see what happened. What are safer choices?
5. An app asks to use the camera even though the activity does not need it. What should the learner do?
6. A student accidentally clicks something suspicious and is afraid of getting in trouble. How should adults and classmates respond?

K-6 Debrief Questions

- Who could be helped or harmed by each choice?
- What information is private or sensitive?
- Which trusted adult or reporting path should be used?
- How can the problem be addressed without blaming the person who asks for help?

H.2 Grades 7-12 Discussion Prompts

1. A student finds a weakness in a school-approved practice site. May the student test it further without asking?
2. A friend sends screenshots of a private conversation as evidence of bullying. How should the evidence be protected and reported?
3. A popular account posts a dramatic security claim without a source. Is sharing it “just in case” responsible?
4. A team member wants to use an AI tool to complete a security report but does not plan to disclose the assistance. What are the concerns?
5. A school proposes extensive monitoring of student devices to improve security. What benefits, risks, and safeguards should be considered?
6. A competition rewards the fastest team, but one member completed nearly all the work. What would fair recognition and assessment look like?
7. A student receives access to information that was not intended for that student. What should the student do before viewing, copying, or sharing it?
8. A club wants to demonstrate phishing by sending an unexpected fake message to students. What approvals, protections, and alternatives are needed?

Grades 7-12 Reasoning Frame

Learners should identify:

- The authorized purpose and scope
- Affected people and organizations
- Information that is known, assumed, or missing
- Relevant duties, rules, or policies
- Reasonable alternatives

- Likely benefits and harms
- A decision and the conditions that could change it

H.3 Postsecondary and Professional Dilemmas

1. Responsible disclosure: A researcher identifies a serious vulnerability in a widely used product. The vendor does not respond. What disclosure path is proportionate, and what evidence should be preserved?
2. Ransomware decision: A public-service organization faces prolonged disruption. Leaders are considering payment. What technical, legal, ethical, operational, and societal factors belong in the decision?
3. Insider monitoring: An organization proposes expanded behavior analytics after a suspected insider incident. How should need, privacy, transparency, bias, retention, and oversight be balanced?
4. AI-generated security advice: A team uses a generative system to recommend cloud controls. The recommendations appear plausible but cite nonexistent sources. Who is accountable for verification and approval?
5. Student research data: A class project uses security telemetry that may contain personal information. What minimization, consent, access, retention, and publication controls are required?
6. Supply-chain warning: A component has a severe vulnerability, but immediate replacement could interrupt a critical service. How should temporary controls, communication, acceptance, and retirement be handled?
7. Conflict of interest: An advisory partner donates a platform and asks that the curriculum emphasize that product. What boundaries preserve academic independence?
8. Public incident communication: Investigators have incomplete evidence, but customers demand immediate certainty. How should leaders communicate what is known, unknown, and changing?
9. Accessibility versus speed: A time-critical security training rollout is not usable by several employees with disabilities. Is partial deployment acceptable, and under what conditions?
10. Portfolio confidentiality: A learner wants to include internship work in a public portfolio. What evidence can be shown without exposing organizational information?

H.4 Stakeholder Role Cards

Incident Coordinator

Primary responsibility: Coordinate priorities, decisions, owners, and update rhythm. Information needed: Scope, mission impact, current actions, dependencies, and unresolved decisions. Common tension: Acting quickly without allowing urgency to erase documentation or consultation.

Security Analyst

Primary responsibility: Interpret technical evidence and propose testable hypotheses. Information needed: Logs, configurations, timelines, system context, and known-good baselines. Common tension: Communicating uncertainty without making the analysis sound unhelpful.

IT or Service Owner

Primary responsibility: Maintain and restore reliable operations. Information needed: Dependencies, change history, recovery options, user impact, and support capacity. Common tension: Restoring service quickly while preserving evidence and avoiding reinfection or recurrence.

Privacy or Records Lead

Primary responsibility: Protect information about people and manage collection, use, disclosure, retention, and notification concerns. Information needed: Data types, affected populations, jurisdiction, access, and evidence of exposure. Common tension: Supporting investigation without unnecessary collection or indefinite retention.

Legal or Compliance Advisor

Primary responsibility: Explain applicable duties, contractual commitments, and legal risk. Information needed: Jurisdiction, data, sector, timeline, contracts, and confirmed facts. Common tension: Providing actionable guidance while facts and law may still be uncertain.

Communications Lead

Primary responsibility: Deliver accurate, timely, audience-appropriate information. Information needed: Confirmed facts, user impact, approved actions, next update, and contact path. Common tension: Pressure for certainty, reassurance, or blame before evidence supports it.

Executive Sponsor

Primary responsibility: Make mission, resource, risk, and stakeholder decisions. Information needed: Consequence, options, tradeoffs, cost, obligations, and recommendation. Common tension: Avoiding both technical micromanagement and uninformed decision-making.

Affected User or Community Representative

Primary responsibility: Surface practical harm, access needs, trust concerns, and communication gaps. Information needed: What happened, what actions are required, available support, and how information will be used. Common tension: The organization may focus on systems while people experience financial, emotional, educational, or professional consequences.

External Partner or Regulator

Primary responsibility: Protect shared interests and verify that obligations are met. Information needed: Scope, impact, evidence, controls, notification, and remediation. Common tension: The organization may fear reputational damage while the partner requires transparency.

H.5 Role-Play Procedure

1. Provide a short scenario and a common evidence packet.
2. Assign roles and allow learners to identify missing information.
3. Require each role to state its priority, concern, and requested action.
4. Introduce one new fact that changes the decision environment.
5. Require a documented decision and dissent or unresolved issue.
6. Rotate roles in a second round so learners experience a different perspective.

H.6 Debrief Guide

- Which facts were most important, and which assumptions were treated as facts?
- Which stakeholder was easiest to ignore?
- Where did legal permission, policy, ethics, and operational need point in different directions?
- What alternative caused less harm while still meeting the purpose?
- How did uncertainty affect communication?
- What evidence would have changed the decision?
- What should be documented for accountability and future learning?

Ethical Reasoning Rubric

Criterion	Strong evidence	Developing evidence	Weak evidence
Stakeholder awareness	Identifies affected groups, unequal impacts, and duties	Identifies obvious stakeholders	Focuses only on the decision-maker
Facts and uncertainty	Separates facts, inference, and missing information	Notes some uncertainty	Treats assumptions as facts

Criterion	Strong evidence	Developing evidence	Weak evidence
Principles and obligations	Applies relevant ethical principles, authorization, policy, and law appropriately	Names rules without integrating them	Uses personal preference as the only basis
Alternatives	Compares feasible options and safeguards	Provides more than one option	Presents a false binary or no alternative
Justification	Gives a clear decision, reasoning, limitations, and review conditions	Gives a decision with partial reasoning	Gives an answer without defensible reasoning

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. Online public appendices - Appendix H.

Sharing and reuse: Please do not resell this resource. You may repost or share it with other educators. Please leave the Bare Metal Cyber Educators Hub URL below intact. Use fictional or appropriately authorized data where applicable.

Read online: https://educate.baremetalcyber.com/resources/ethics/