BỘ GIÁO DỤC VÀ ĐÀO TẠO	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: /QĐ-BGDĐT	*Hà Nội, ngày tháng năm 2026*

QUYẾT ĐỊNH
Phê duyệt Tài liệu và Infographic hướng dẫn triển khai, tuyên truyền khai thác, sử dụng mạng an toàn cho học sinh

BỘ TRƯỞNG BỘ GIÁO DỤC VÀ ĐÀO TẠO

Căn cứ Nghị định số 279/2026/NĐ-CP ngày 12/7/2026 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Giáo dục và Đào tạo;

Căn cứ Quyết định số 2936/QĐ-BGDĐT ngày 22/10/2025 của Bộ trưởng Bộ Giáo dục và Đào tạo ban hành hướng dẫn hoạt động giáo dục kỹ năng cho học sinh, sinh viên trong và ngoài nhà trường;

Căn cứ Kế hoạch số 246/KH-BGDĐT ngày 10/02/2026 của Bộ Giáo dục và Đào tạo hướng dẫn công tác khai thác, sử dụng môi trường mạng an toàn, lành mạnh cho học sinh, sinh viên năm 2026;

Căn cứ Quyết định số 865/QĐ-BGDĐT ngày 13/4/2026 của Bộ trưởng Bộ Giáo dục và Đào tạo về việc thành lập Ban biên soạn tài liệu và Infographic hướng dẫn triển khai, tuyên truyền khai thác, sử dụng mạng an toàn cho học sinh;

Căn cứ Quyết định số 2736/QĐ-BGDĐT ngày 17/9/2026 của Bộ trưởng Bộ Giáo dục và Đào tạo về việc thành lập Hội đồng thẩm định dự thảo tài liệu và Infographic hướng dẫn triển khai, tuyên truyền khai thác, sử dụng mạng an toàn cho học sinh;

Căn cứ Biên bản họp Hội đồng thẩm định tài liệu ngày 24/9/2026;

Theo đề nghị của Vụ trưởng Vụ Học sinh, sinh viên.

QUYẾT ĐỊNH:

Điều 1. Phê duyệt Tài liệu và Infographic hướng dẫn triển khai, tuyên truyền khai thác, sử dụng mạng an toàn cho học sinh *(Tài liệu kèm theo)*.

Điều 2. Quyết định có hiệu lực kể từ ngày ký.

Điều 3. Chánh Văn phòng, Vụ trưởng Vụ Học sinh, sinh viên, Thủ trưởng các đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này./.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nơi nhận:
- Như Điều 3 (để thực hiện);
- Bộ trưởng (để báo cáo);
- Các sở giáo dục và đào tạo;
- Cổng thông tin điện tử Bộ GDĐT;
- Lưu: VT, Vụ HSSV.

Nguyễn Thị Quyên Thanh

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TÀI LIỆU VÀ INFOGRAPHIC

HƯỚNG DẪN TRIỂN KHAI, TUYÊN TRUYỀN KHAI THÁC, SỬ DỤNG MẠNG AN TOÀN CHO HỌC SINH

Hà Nội, năm 2026

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TÀI LIỆU VÀ INFOGRAPHIC

HƯỚNG DẪN TRIỂN KHAI, TUYÊN TRUYỀN KHAI THÁC, SỬ DỤNG MẠNG AN TOÀN CHO HỌC SINH

Ban biên soạn:

Nguyễn Thị Nhung

Lê Hoàn

Nguyễn Thị Thanh Huyền

Nguyễn Thế Lộc

Nguyễn Văn Tuấn

Hà Nội, năm 2026

LỜI NÓI ĐẦU

Các em học sinh thân mến,

Internet và công nghệ số ngày càng trở thành một phần quen thuộc trong học tập và đời sống. Thông qua máy tính, điện thoại thông minh và các thiết bị có kết nối mạng, các em có thể tìm kiếm thông tin, tiếp cận nhiều nguồn học liệu, học tập trực tuyến, trao đổi với thầy cô và bạn bè, tham gia các hoạt động sáng tạo và sử dụng nhiều dịch vụ số. Sự phát triển nhanh chóng của trí tuệ nhân tạo (AI) cũng mở ra những cách thức mới để khám phá kiến thức, phát triển ý tưởng và giải quyết vấn đề.

Bên cạnh những lợi ích đó, môi trường mạng cũng tiềm ẩn nhiều nguy cơ. Các em có thể gặp thông tin sai lệch, nội dung không phù hợp, lừa đảo trực tuyến, giả mạo danh tính, mất tài khoản, lộ dữ liệu cá nhân, bắt nạt trên mạng hoặc những hành vi xâm phạm quyền riêng tư, danh dự và hình ảnh. Sự phát triển của AI còn khiến việc giả mạo hình ảnh, giọng nói, video và thông tin ngày càng tinh vi, khó nhận biết. Đôi khi, chỉ một thao tác như nhấp vào đường liên kết không an toàn, cung cấp thông tin cá nhân hay chia sẻ nội dung chưa được kiểm chứng cũng có thể dẫn đến những hậu quả không mong muốn.

Vì vậy, sử dụng Internet an toàn không có nghĩa là hạn chế tiếp cận công nghệ, mà là biết khai thác công nghệ chủ động, an toàn, hiệu quả và có trách nhiệm. Các em cần biết bảo vệ tài khoản và dữ liệu cá nhân; nhận diện nguy cơ; đánh giá và kiểm chứng thông tin; giao tiếp, ứng xử phù hợp; sử dụng mạng xã hội, các công cụ số và AI có trách nhiệm; đồng thời biết cách xử lý và tìm kiếm sự hỗ trợ khi gặp sự cố.

Xuất phát từ yêu cầu đó, *Tài liệu và Infographic hướng dẫn triển khai, tuyên truyền, khai thác, sử dụng mạng an toàn cho học sinh* được xây dựng nhằm cung cấp những kiến thức pháp luật cơ bản, nguyên tắc và kỹ năng thiết thực để các em vận dụng trong học tập, giao tiếp và sử dụng Internet hằng ngày. Tài liệu tập trung vào những vấn đề gần gũi như quyền và trách nhiệm trên môi trường mạng; bảo vệ thông tin, dữ liệu cá nhân, tài khoản và thiết bị; nhận diện lừa đảo, giả mạo, thông tin sai lệch; phòng tránh nội dung độc hại và bắt nạt trên mạng; tìm kiếm, đánh giá và sử dụng thông tin; giao tiếp, chia sẻ, hợp tác trực tuyến và sử dụng AI an toàn, hiệu quả.

Đối tượng sử dụng chính của tài liệu là học sinh phổ thông ở các cấp tiểu học, trung học cơ sở và trung học phổ thông. Nội dung được trình bày theo hướng dễ hiểu, gần gũi với những tình huống thực tế và có thể vận dụng phù hợp với từng độ tuổi. Với học sinh nhỏ tuổi, sự hướng dẫn và đồng hành của thầy cô, cha mẹ có vai trò đặc biệt

quan trọng. Ở các cấp học cao hơn, các em cần từng bước hình thành khả năng tự nhận diện nguy cơ, đánh giá tình huống, lựa chọn cách ứng xử và chịu trách nhiệm đối với hành vi của mình trên môi trường mạng.

Tài liệu kết hợp giữa nội dung hướng dẫn và hệ thống infographic. Phần nội dung bao gồm 5 chương giúp các em hiểu vấn đề, nhận biết nguy cơ và biết cách phòng tránh, xử lý; chương 6 tập hợp hệ thống infographic, hình ảnh minh họa cô đọng những kiến thức quan trọng thành các nguyên tắc, dấu hiệu nhận biết, quy trình và thông điệp trực quan, dễ nhớ. Các infographic cũng có thể được sử dụng trong hoạt động truyền thông và giáo dục tại nhà trường.

Đồng thời, tài liệu được thiết kế như một cẩm nang về sử dụng mạng an toàn để các em có thể tra cứu khi cần. Khi gặp một tình huống trên Internet, các em có thể tìm đến chủ đề tương ứng để nhận biết dấu hiệu, xem những việc nên làm và cách tìm kiếm sự hỗ trợ. Khi gặp lừa đảo, giả mạo, mất tài khoản, xâm phạm quyền riêng tư, đe dọa, bắt nạt hoặc tình huống gây mất an toàn, các em cần bình tĩnh, thực hiện những biện pháp phù hợp và chủ động tìm kiếm sự hỗ trợ từ cha mẹ, thầy cô hoặc người lớn tin cậy.

Cán bộ quản lý giáo dục, cha mẹ và người chăm sóc trẻ em sử dụng tài liệu để tham khảo, hướng dẫn và đồng hành cùng các em, nhất là đối với học sinh tiểu học. Giáo viên và nhà trường có thể khai thác nội dung, tình huống và infographic trong dạy học, sinh hoạt lớp, hoạt động trải nghiệm, sinh hoạt chuyên đề và tuyên truyền. Cha mẹ có thể sử dụng tài liệu để trao đổi với con, hướng dẫn các em hình thành thói quen sử dụng Internet an toàn và hỗ trợ khi xảy ra sự cố. Sự phối hợp giữa học sinh, gia đình và nhà trường sẽ góp phần tạo dựng môi trường số an toàn, lành mạnh và tích cực.

Thông qua tài liệu này, chúng tôi mong muốn các em không chỉ biết tự bảo vệ mình, mà còn biết tôn trọng và bảo vệ người khác, tận dụng những lợi ích của Internet cho học tập, sáng tạo và phát triển bản thân, đồng thời có trách nhiệm với mỗi hành động và nội dung mình chia sẻ trên mạng.

MỤC LỤC

LỜI NÓI ĐẦU 1
MỤC LỤC 3
DANH MỤC HÌNH ẢNH 8
DANH MỤC BẢNG BIỂU 10
CHƯƠNG 1. KIẾN THỨC PHÁP LUẬT CƠ BẢN VỀ AN NINH, AN TOÀN MẠNG 11
1.1. Cơ sở pháp lý 11
1.1.1. Các văn bản pháp luật và văn bản chỉ đạo, hướng dẫn của Việt Nam 11
1.1.2. Các công ước và văn kiện quốc tế có liên quan 13
1.2. Một số quy định pháp luật liên quan đến học sinh trên môi trường mạng 13
1.2.1. Quyền và bảo vệ trẻ em trên môi trường mạng 13
1.2.2. Quyền và nghĩa vụ bảo vệ dữ liệu cá nhân 14
1.2.3. An ninh mạng, sử dụng Internet và thông tin trên mạng 16
1.2.4. Sử dụng công cụ số và AI an toàn và có trách nhiệm 19
1.3. Kết luận chương 20
CHƯƠNG 2. NGUYÊN TẮC, KỸ NĂNG SỬ DỤNG MẠNG AN TOÀN 22
2.1. Nguyên tắc cốt lõi 23
2.1.1. Suy nghĩ trước khi đăng và chia sẻ 24
2.1.2. Bảo vệ thông tin cá nhân, tài khoản và quyền riêng tư 25
a. Infographic minh họa: “Những gì KHÔNG nên đăng” 27
b. Tình huống thực tế 27
2.1.3. Cảnh giác và kiểm chứng trước khi tin hoặc hành động 28
2.1.4. Tôn trọng bản thân và người khác trên môi trường mạng 30
2.1.5. Chủ động lên tiếng và tìm kiếm sự hỗ trợ khi cần thiết 31
2.1.6. Sử dụng Internet cân bằng, lành mạnh và có mục đích 32
a. Sử dụng Internet cân bằng 32

b. Sử dụng Internet lành mạnh 34
c. Sử dụng Internet có mục đích 34
2.2. Kỹ năng sử dụng mạng an toàn 35
2.2.1. Xây dựng và quản lý mật khẩu mạnh 35
a. Công thức "Câu chuyện + số + ký tự đặc biệt" 36
b. Các mức bảo vệ tài khoản 36
c. Kích hoạt xác thực 2 lớp (2FA) 37
d. Sử dụng trình quản lý mật khẩu 38
2.2.2. Giao tiếp an toàn với người lạ 39
a. Nhận diện dấu hiệu bất thường 39
b. Hành vi trên mạng và vi phạm pháp luật 40
c. Tình huống thực tế liên quan 40
d. Sử dụng chức năng Báo cáo và Chặn 41
2.2.3. Cập nhật phần mềm và nhận diện lừa đảo 41
a. Luôn cập nhật hệ điều hành và ứng dụng 41
b. Nhận diện tin nhắn, cuộc gọi lừa đảo 42
2.3. Trách nhiệm phối hợp Gia đình – Nhà trường – Học sinh 43
2.4. Bảng tự đánh giá kỹ năng sử dụng mạng an toàn 45
2.5. Kết luận chương 46
CHƯƠNG 3. CÁC RỦI RO PHỔ BIẾN KHI THAM GIA MÔI TRƯỜNG MẠNG 48
3.1. Rủi ro kỹ thuật và phần mềm độc hại 48
3.1.1. Phishing và Smishing tinh vi 49
3.1.2. Malware từ game và ứng dụng crack 51
3.1.3. Deepfake và AI lừa đảo 53
3.2. Rủi ro xã hội và tâm lý 56
3.2.1. Bắt nạt mạng (Cyberbullying) 57
a. Chế giễu và xúc phạm: 57
b. Công kích tập thể: 57

c. Lan truyền tin đồn: 57
d. Chia sẻ hình ảnh hoặc thông tin riêng tư: 57
e. Mạo danh: 57
f. Cô lập trên mạng: 57
g. Chỉnh sửa hoặc tạo nội dung giả: 57
3.2.2. Tin giả và thao túng thông tin 59
3.2.3. Dụ dỗ (Grooming) và ép buộc trên mạng (Sextortion) 60
3.3. Rủi ro sức khỏe và phát triển 63
3.3.1. Nghiện mạng xã hội và giảm tập trung 64
3.3.2. Tiếp xúc nội dung độc hại không phù hợp 64
3.4. Phân tích tổng hợp: Ma trận rủi ro 66
3.5. Kết luận chương 67
CHƯƠNG 4. CÁC BIỆN PHÁP PHÒNG TRÁNH, ỨNG PHÓ KHI GẶP SỰ CỐ TRÊN KHÔNG GIAN MẠNG 69
4.1. Các biện pháp phòng tránh chủ động 70
4.1.1. Cài đặt công cụ bảo mật thiết bị 70
4.1.2. Thiết lập kiểm soát phụ huynh thông minh 72
4.1.3. Giáo dục kỹ năng số tại trường học 75
4.1.4. Xây dựng cơ chế tiếp nhận và xử lý phản ánh trong nhà trường 77
a. Kênh phản ánh trong trường 80
b. Nguyên tắc bảo mật cho các tình huống nhạy cảm 80
4.2. Quy trình ứng phó khẩn cấp khi gặp sự cố 81
4.2.1. Bước 1–3: Phản ứng ngay lập tức 82
4.2.2. Bước 4–5: Báo cáo và phối hợp 83
4.2.3. Bước 6–7: Phục hồi và phòng ngừa lâu dài 84
4.2.4. Minh họa: áp dụng quy trình 7 bước vào một tình huống cụ thể 85
4.2.5. Bài học kinh nghiệm sau khi giải quyết sự cố 87
4.3. Kết luận chương 88

CHƯƠNG 5. MỘT SỐ KỸ NĂNG KHAI THÁC MẠNG AN TOÀN, HIỆU QUẢ PHỤC VỤ HỌC TẬP 89
5.1. Kỹ năng tìm kiếm, đánh giá và sử dụng thông tin 90
5.1.1. Nhận diện và lựa chọn nguồn thông tin đáng tin cậy 91
a. Ai cung cấp thông tin? 91
b. Thông tin được đăng khi nào? 91
c. Thông tin có căn cứ không? 91
d. Có thể kiểm tra lại ở nguồn khác không? 92
e. Nên ưu tiên nguồn nào? 92
f. Phù hợp với từng cấp học 92
5.1.2. Sử dụng từ khóa và các kỹ thuật tìm kiếm nâng cao 93
a. Bắt đầu bằng những từ quan trọng 93
b. Thu hẹp kết quả khi cần 94
c. Tìm kiếm với sự hỗ trợ của AI 94
d. Cách tìm kiếm phù hợp với từng cấp học 95
e. Điều cần nhớ 95
5.1.3. Đánh giá độ tin cậy của nguồn 98
5.1.4. Ghi nguồn và trích dẫn đúng cách 101
5.2. Hợp tác học tập an toàn và công cụ AI 102
5.2.1. Làm việc nhóm an toàn trên nền tảng số 103
5.2.2. Sử dụng AI học tập có kiểm soát 105
5.2.3. Đạo đức học thuật và tính trung thực khi sử dụng AI 109
5.2.4. Quản lý thời gian học online hiệu quả 110
5.3. Kỹ thuật soạn thảo câu lệnh khi sử dụng AI (Prompt engineering) 112
5.3.1. Prompt là gì? 112
5.3.2. Đối với cấp Tiểu học 113
a. Chữ R thứ nhất – RÕ: Nói rõ em muốn gì 113
b. Chữ R thứ hai – RIÊNG: Cho AI biết em là ai 113
c. Chữ R thứ ba – RÀ LẠI: Hỏi thêm nếu chưa hiểu 113

d. Mẫu câu "điền vào chỗ trống" 113
e. Những điều em cần nhớ 114
5.3.3. Cấp trung học cơ sở 114
a. Công thức bốn phần 114
b. Năm kỹ thuật hữu ích 114
c. Cảnh giác với AI 115
5.3.4. Cấp trung học phổ thông 115
a. Khung prompt nâng cao C.R.E.A.T.E 115
b. Bảy kỹ thuật chuyên sâu 115
c. Ví dụ: Từ prompt yếu đến prompt mạnh 116
5.3.5. Đạo đức và tư duy phản biện 116
5.4. Minh họa: một tuần tự học tích hợp cả 8 kỹ năng 117
5.5. Kết luận chương 121
CHƯƠNG 6. INFOGRAPHIC VÀ HÌNH ẢNH MINH HỌA 122
6.1. Giáo dục về đạo đức và pháp luật 122
6.2. Kiến thức về tin học và an toàn thông tin 123
6.3. Nguy cơ về nội dung xấu trên mạng, bảo vệ thông tin cá nhân 124
6.4. Nguy cơ về tương tác có hại với người khác 125
6.5. Nguy cơ về quảng cáo và tiêu dùng 126
6.6. Nguy cơ về an toàn thông tin 127
6.7. Sử dụng mạng xã hội an toàn 128
6.8. Sử dụng an toàn thiết bị 129
TÀI LIỆU THAM KHẢO 130
PHỤ LỤC 133
Các kênh hỗ trợ khi gặp sự cố 133
Giải thích một số thuật ngữ 134

DANH MỤC HÌNH ẢNH

Hình 1.1. Một số hành vi bị nghiêm cấm theo Điều 7 Luật An ninh mạng 2025 19

Hình 2.1. Những gì KHÔNG nên đăng/chia sẻ trên mạng xã hội 27

Hình 2.2. Cách ứng phó với tình huống thực tế cho các cấp độ trường học 28

Hình 2.3. Trách nhiệm giữa gia đình, nhà trường và học sinh 45

Hình 3.1. Sơ đồ kịch bản giả mạo "kết quả thi học kỳ" lan truyền qua Zalo/Facebook 50

Hình 3.2. Minh họa lừa đảo/phishing và cách đối phó 51

Hình 3.3. Kịch bản cuộc gọi deepfake giả giọng người thân, bạn bè để vay tiền gấp 54

Hình 3.4. 5 dấu hiệu nhận diện một cuộc gọi/video giả mạo bằng công nghệ deepfake 55

Hình 3.5. Giả giọng nói sử dụng AI để lừa đảo 56

Hình 3.6. Mô hình khái quát các giai đoạn hành vi grooming trên mạng 61

Hình 3.7. Các giai đoạn của hành vi Sextortion 62

Hình 4.1. Bốn nhóm tính năng chính của Google Family Link 73

Hình 4.2. Các hình thức cha mẹ đồng hành khi học sinh sử dụng Internet 74

Hình 4.3. Bốn cách cha mẹ hỗ trợ học sinh sử dụng Internet an toàn 75

Hình 4.4. Ba trụ cột giáo dục kỹ năng số tại trường học 77

Hình 4.5. Quy trình tiếp nhận và xử lý phản ánh sự cố trên không gian mạng 78

Hình 4.6. Hướng dẫn xử lý sau sự cố cho từng cấp độ trường học 79

Hình 4.7. Quy trình 7 bước ứng phó khi gặp sự cố trên không gian mạng 82

Hình 4.8. Các kênh trình báo chính thức khi gặp sự cố trên không gian mạng ...84

Hình 4.9. Bài học kinh nghiệm sau khi tư vấn giải quyết sự cố 87

Hình 5.1. Tổng quan 8 kỹ năng khai thác mạng an toàn, hiệu quả phục vụ học tập 90

Hình 5.2. Bốn toán tử Boolean cơ bản và cách áp dụng vào tìm kiếm học thuật 96

Hình 5.3. Quy trình thu thập và trích dẫn tài liệu tự động bằng Zotero 99

Hình 5.4. Khung CRAAP: năm tiêu chí đánh giá độ tin cậy của một nguồn thông tin 102
Hình 5.5. Quy trình 6 bước sử dụng AI trong học tập 107
Hình 5.6. Ba công cụ AI học tập phổ biến hiện nay 108
Hình 5.7. Một chu kỳ Pomodoro điển hình 111
Hình 6.1. Giáo dục về đạo đức và pháp luật 122
Hình 6.2. Kiến thức về tin học và an toàn thông tin 123
Hình 6.3. Nguy cơ về nội dung xấu trên mạng, bảo vệ thông tin cá nhân 124
Hình 6.4. Nguy cơ về tương tác có hại với người khác 125
Hình 6.5. Nguy cơ về quảng cáo và tiêu dùng 126
Hình 6.6. Nguy cơ về an toàn thông tin 127
Hình 6.7. Sử dụng mạng xã hội an toàn 128
Hình 6.8. Sử dụng an toàn thiết bị 129

DANH MỤC BẢNG BIỂU

Bảng 1.1. Bảng tự đánh giá nhận thức pháp luật.....20
Bảng 2.1. Tổng hợp 12 nguyên tắc vàng giúp nhận thức và bảo vệ thông tin 22
Bảng 2.2. Phân loại mức độ rủi ro của loại thông tin cá nhân.....25
Bảng 2.3. Khuyến nghị thời gian sử dụng theo độ tuổi.....33
Bảng 2.4. Các mức độ bảo vệ tài khoản 36
Bảng 2.5. Trách nhiệm của các chủ thể.....43
Bảng 2.6. Bảng đánh giá kỹ năng sử dụng mạng an toàn.....45
Bảng 3.1. Phân loại các chế độ trong khi cài đặt trò chơi 52
Bảng 3.2. Ma trận phân tích các rủi ro 66
Bảng 4.1. Bảng tổng hợp các công cụ hỗ trợ theo hệ điều hành 72
Bảng 5.1. Bảng dữ liệu nguồn và mức độ tin cậy.....93
Bảng 5.2. Bảng mở rộng các toán tử tìm kiếm nâng cao khác 97
Bảng 5.3. Các yếu tố của chuẩn APA và chuẩn MLA 99
Bảng 5.4. Bảng hướng dẫn sử dụng AI phù hợp với từng cấp học 105
Bảng 5.5. Ví dụ về cách sử dụng Prompt cho học sinh Tiểu học.....113
Bảng 5.6. Ví dụ sử dụng công thức bốn phần cho THCS 114
Bảng 5.7. Công thức sử dụng Prompt cho học sinh THPT 115
Bảng 5.8. Bảng tổng hợp 8 kỹ năng và công cụ tương ứng 119
Bảng 5.9. Bảng tự đánh giá kỹ năng khai thác mạng phục vụ học tập.....120

CHƯƠNG 1. KIẾN THỨC PHÁP LUẬT CƠ BẢN VỀ AN NINH, AN TOÀN MẠNG

Các quy định pháp luật liên quan đến an ninh, an toàn mạng đối với học sinh được quy định trong nhiều văn bản khác nhau, tương ứng với từng nhóm vấn đề như quyền và bảo vệ trẻ em, bảo vệ thông tin và dữ liệu cá nhân, an ninh mạng, quản lý và sử dụng Internet, trách nhiệm đối với hành vi vi phạm trên môi trường mạng. Bên cạnh đó, Bộ Giáo dục và Đào tạo cũng đã ban hành các quy định và hướng dẫn cụ thể về năng lực số, an toàn số và sử dụng trí tuệ nhân tạo đối với học sinh, trong đó có một số nội dung liên quan đến con người và đạo đức trên môi trường số. Đồng thời, một số công ước và văn kiện quốc tế mà Việt Nam tham gia hoặc sử dụng làm cơ sở tham chiếu cũng đặt ra các nguyên tắc về quyền trẻ em và bảo vệ trẻ em trong môi trường số. Vì vậy, để xác định đầy đủ cơ sở pháp lý cho việc hướng dẫn học sinh sử dụng mạng an toàn, tài liệu này căn cứ vào các văn bản chính được trình bày sau đây.

1.1. Cơ sở pháp lý

1.1.1. Các văn bản pháp luật và văn bản chỉ đạo, hướng dẫn của Việt Nam

- Luật Trẻ em số 102/2016/QH13 ngày 05/4/2016 của Quốc hội.

- Nghị định số 56/2017/NĐ-CP ngày 09/5/2017 của Chính phủ quy định chi tiết một số điều của Luật Trẻ em.

- Thông tư số 09/2017/TT-BTTTT ngày 23/6/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về tỷ lệ nội dung, thời điểm, thời lượng dành cho trẻ em và cảnh báo nội dung không phù hợp với trẻ em trên báo nói, báo hình, báo in, báo điện tử và xuất bản phẩm.

- Quyết định số 468/QĐ-TTg ngày 23/03/2026 của Thủ tướng Chính phủ phê duyệt Chương trình "Bảo vệ và hỗ trợ trẻ em phát triển trên môi trường mạng giai đoạn 2026–2030".

- Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 ngày 26/6/2025 của Quốc hội.

- Nghị định số 356/2025/NĐ-CP ngày 31/12/2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân.

- Luật An ninh mạng số 116/2025/QH15 ngày 10/12/2025 của Quốc hội.

- Nghị định số 333/2026/NĐ-CP ngày 19/8/2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật An ninh mạng.

- Nghị định số 147/2024/NĐ-CP ngày 09/11/2024 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng.

- Nghị định số 327/2026/NĐ-CP ngày 19/8/2026 của Chính phủ quy định về phòng ngừa, xử lý thông tin và hành vi sử dụng công nghệ thông tin, mạng máy tính, mạng viễn thông, phương tiện điện tử xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên không gian mạng.

- Nghị định số 328/2026/NĐ-CP ngày 19/8/2026 của Chính phủ quy định về phòng, chống tin giả, tin sai sự thật trên không gian mạng.

- Nghị định số 330/2026/NĐ-CP ngày 19/8/2026 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng và bảo vệ dữ liệu cá nhân.

- Thông tư số 02/2025/TT-BGDĐT ngày 24/01/2025 của Bộ trưởng Bộ Giáo dục và Đào tạo quy định Khung năng lực số cho người học.

- Công văn số 3456/BGDĐT-GDPT ngày 27/6/2025 của Bộ Giáo dục và Đào tạo về việc hướng dẫn triển khai thực hiện Khung năng lực số cho học sinh phổ thông và học viên giáo dục thường xuyên.

- Quyết định số 2422/QĐ-BGDĐT ngày 18/8/2026 của Bộ trưởng Bộ Giáo dục và Đào tạo ban hành Khung nội dung giáo dục trí tuệ nhân tạo cho học sinh phổ thông.

- Công văn số 5588/BGDĐT-GDPT ngày 19/8/2026 của Bộ Giáo dục và Đào tạo về việc hướng dẫn triển khai thực hiện nội dung giáo dục trí tuệ nhân tạo cho học sinh phổ thông.

- Luật Trí tuệ nhân tạo số 134/2025/QH15 ngày 10/12/2025 của Quốc hội.

- Thông tư số 19/2025/TT-BGDĐT ngày 15/09/2025 của Bộ Giáo dục và Đào tạo về Quy định về khen thưởng và kỷ luật học sinh.

- Quyết định số 447/QĐ-BGDĐT ngày 31 tháng 01 năm 2024 của Bộ Giáo dục và Đào tạo về việc phê duyệt "Hướng dẫn bảo đảm an toàn thông tin, tham gia môi trường mạng an toàn đối với hoạt động giảng dạy, quản lý giáo dục".

- Quyết định số 88/QĐ-BTTTT ngày 21/01/2025 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) ban hành Bộ Quy tắc ứng xử về bảo vệ trẻ em trên môi trường mạng.

- Công văn số 3147/BGDĐT-HSSV ngày 29/5/2026 được Bộ Giáo dục và Đào tạo ban hành về việc tăng cường chấn chỉnh, xử lý, ngăn chặn và đẩy lùi bạo lực học đường

trong các cơ sở giáo dục, nhằm triển khai thực hiện Chỉ thị số 03/CT-TTg ngày 30/01/2026 của Thủ tướng Chính phủ.

1.1.2. Các công ước và văn kiện quốc tế có liên quan

- Công ước của Liên hợp quốc về Quyền trẻ em (Convention on the Rights of the Child – CRC), được Đại hội đồng Liên hợp quốc thông qua ngày 20/11/1989.

- Bình luận chung số 25 (2021) của Ủy ban Quyền trẻ em Liên hợp quốc về quyền trẻ em trong môi trường số (General Comment No. 25 on Children's Rights in Relation to the Digital Environment), ngày 02/3/2021.

- Công ước của Liên hợp quốc về chống tội phạm mạng (United Nations Convention against Cybercrime), được Đại hội đồng Liên hợp quốc thông qua ngày 24/12/2024, và mở ký ngày 25/10/2025. Sau đó vào ngày 07/04/2026 đã ký Quyết định phê chuẩn Công ước của Liên hợp quốc về chống tội phạm mạng (hay còn gọi là Công ước Hà Nội). Việt Nam trở thành quốc gia đầu tiên ở Đông Nam Á và thứ hai trên thế giới phê chuẩn Công ước Hà Nội.

Các văn bản trên tạo thành cơ sở pháp lý và định hướng quan trọng cho việc bảo vệ quyền và lợi ích của trẻ em trên môi trường mạng, bảo vệ thông tin và dữ liệu cá nhân, bảo đảm an ninh, an toàn số, phòng ngừa các hành vi gây hại, đồng thời định hướng hình thành năng lực số và sử dụng trí tuệ nhân tạo an toàn, có đạo đức và trách nhiệm cho học sinh.

1.2. Một số quy định pháp luật liên quan đến học sinh trên môi trường mạng

1.2.1. Quyền và bảo vệ trẻ em trên môi trường mạng

Quyền của trẻ em trên môi trường mạng trước hết được đặt trên nền tảng các quyền cơ bản đã được ghi nhận trong Công ước của Liên hợp quốc về Quyền trẻ em (CRC). Công ước khẳng định trẻ em có quyền được bảo vệ đời sống riêng tư, được tiếp cận thông tin, được bày tỏ ý kiến và được bảo vệ trước các hình thức bạo lực, bóc lột và xâm hại. Những quyền này không chỉ được bảo đảm trong đời sống trực tiếp mà còn phải được tôn trọng khi trẻ em tham gia môi trường số.

Bình luận chung số 25 (2021) của Ủy ban Quyền trẻ em Liên hợp quốc tiếp tục làm rõ việc thực hiện các quyền của trẻ em trong môi trường số. Theo đó, công nghệ số vừa tạo thêm cơ hội để trẻ em học tập, tiếp cận thông tin và tham gia các hoạt động xã hội, vừa có thể làm phát sinh những nguy cơ mới đối với quyền riêng tư, danh dự, sự an toàn và sự phát triển của trẻ em. Vì vậy, quyền và lợi ích tốt nhất của trẻ em cần được

ưu tiên xem xét trong quá trình thiết kế, cung cấp, vận hành và sử dụng các sản phẩm, dịch vụ số.

Ở Việt Nam, các nguyên tắc này được thể hiện trong Luật Trẻ em số 102/2016/QH13 và được cụ thể hóa tại Nghị định số 56/2017/NĐ-CP. Trẻ em có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân và bí mật gia đình; được bảo vệ danh dự, nhân phẩm, uy tín và các hình thức trao đổi thông tin riêng tư. Nghị định số 56/2017/NĐ-CP đồng thời quy định trách nhiệm bảo vệ thông tin bí mật đời sống riêng tư của trẻ em, bảo đảm an toàn khi trẻ em trao đổi và cung cấp thông tin trên môi trường mạng, cũng như hỗ trợ và can thiệp khi trẻ em bị xâm hại hoặc có nguy cơ bị xâm hại.

Khi cần hỗ trợ liên quan đến bảo vệ trẻ em, học sinh hoặc gia đình có thể gọi Tổng đài quốc gia bảo vệ trẻ em 111. Nếu có nguy hiểm khẩn cấp liên quan đến tính mạng hoặc an ninh, trật tự, cần gọi số 113. Việc báo cho người lớn và cơ quan có trách nhiệm giúp vụ việc được xem xét chính thức, đồng thời tạo căn cứ để yêu cầu nền tảng ngăn chặn nội dung gây hại.

Như vậy, khi tham gia môi trường mạng, học sinh vừa có quyền tiếp cận và sử dụng công nghệ số, vừa có quyền được bảo vệ thông tin cá nhân, đời sống riêng tư, danh dự, nhân phẩm và sự an toàn của mình.

1.2.2. Quyền và nghĩa vụ bảo vệ dữ liệu cá nhân

Thông tin và dữ liệu cá nhân gắn với mỗi người trong quá trình học tập, giao tiếp và sử dụng các dịch vụ số. Đối với học sinh, dữ liệu cá nhân có thể bao gồm họ tên, ngày sinh, hình ảnh, thông tin liên hệ, tài khoản trực tuyến, thông tin học tập và nhiều loại dữ liệu khác có thể giúp xác định hoặc liên hệ tới một học sinh. Học sinh cũng là chủ thể của dữ liệu cá nhân và có các quyền đối với dữ liệu của mình.

Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 cùng Nghị định số 356/2025/NĐ-CP tạo thành cơ sở pháp lý trực tiếp cho việc bảo vệ dữ liệu cá nhân. Luật quy định dữ liệu cá nhân chỉ được thu thập, xử lý trong phạm vi và vì mục đích cụ thể, rõ ràng; dữ liệu phải được bảo đảm tính chính xác, được bảo vệ bằng các biện pháp phù hợp và chỉ lưu trữ trong khoảng thời gian phù hợp với mục đích xử lý.

Theo quy định, là chủ thể dữ liệu, học sinh có năm quyền cơ bản và gần gũi nhất với học sinh gồm:

- *Quyền được biết:* Học sinh có quyền biết ứng dụng, nền tảng học tập hoặc mạng xã hội đang thu thập những dữ liệu nào về mình, sử dụng vào mục đích gì, lưu trữ trong bao lâu và có chia sẻ cho bên khác hay không. Vì vậy, trước khi đăng ký hoặc sử dụng

một dịch vụ số, học sinh cần đọc những nội dung chính về việc bảo vệ dữ liệu cá nhân, không nên đồng ý khi chưa hiểu rõ.

- *Quyền đồng ý hoặc không đồng ý:* Học sinh có quyền đồng ý hoặc không đồng ý cho phép xử lý dữ liệu cá nhân của mình, trừ những trường hợp pháp luật có quy định khác. Đối với trẻ em, một số quyền có thể do cha mẹ hoặc người đại diện theo pháp luật thực hiện. Đặc biệt, khi dữ liệu được xử lý nhằm công bố hoặc tiết lộ thông tin về đời sống riêng tư, bí mật cá nhân của trẻ em từ đủ 7 tuổi trở lên, phải có sự đồng ý của cả trẻ em và người đại diện theo pháp luật.

- *Quyền truy cập dữ liệu:* Học sinh có quyền yêu cầu xem hoặc được cung cấp dữ liệu cá nhân mà một ứng dụng hay nền tảng đang lưu trữ về mình. Những dữ liệu này có thể bao gồm thông tin tài khoản, lịch sử hoạt động, hình ảnh, video, vị trí hoặc nội dung đã đăng tải.

- *Quyền chỉnh sửa dữ liệu:* Khi phát hiện dữ liệu cá nhân bị sai, thiếu hoặc không còn chính xác, học sinh có quyền yêu cầu chỉnh sửa. Chẳng hạn, nếu ngày sinh bị ghi nhận sai, học sinh có thể đề nghị cập nhật để nền tảng xác định đúng độ tuổi và áp dụng các biện pháp bảo vệ phù hợp.

- *Quyền yêu cầu xóa dữ liệu:* Học sinh có quyền yêu cầu xóa dữ liệu cá nhân trong những trường hợp pháp luật cho phép, chẳng hạn khi không còn sử dụng ứng dụng hoặc khi mục đích thu thập dữ liệu đã hoàn thành. Khi chưa thể tự thực hiện quyền này, học sinh có thể đề nghị cha mẹ hoặc người đại diện theo pháp luật hỗ trợ.

Bên cạnh các quyền được bảo vệ, học sinh cũng có trách nhiệm tự bảo vệ dữ liệu của mình và tôn trọng dữ liệu của người khác. Các em cần thận trọng khi cung cấp thông tin trên Internet; tìm hiểu thông tin được thu thập để làm gì; không tùy tiện đăng, chuyển tiếp hoặc chia sẻ hình ảnh, thông tin riêng tư của người khác; đồng thời tìm kiếm sự hỗ trợ của cha mẹ, thầy cô hoặc người có trách nhiệm khi phát hiện dữ liệu cá nhân bị sử dụng không phù hợp.

Bên cạnh các quyền được pháp luật bảo đảm, học sinh, với tư cách là chủ thể dữ liệu cá nhân, cũng có trách nhiệm bảo vệ dữ liệu của mình và tôn trọng dữ liệu của người khác theo Điều 4 Luật Bảo vệ dữ liệu cá nhân năm 2025 số 91/2025/QH15. Những trách nhiệm đối với học sinh như sau:

- *Tự bảo vệ dữ liệu cá nhân của mình:* Học sinh cần chủ động bảo vệ thông tin cá nhân trong quá trình học tập, giao tiếp và sử dụng các dịch vụ số. Các em không nên tùy tiện công khai địa chỉ, số điện thoại, thông tin tài khoản, hình ảnh riêng tư hoặc dữ liệu

nhạy cảm; đồng thời cần sử dụng mật khẩu an toàn, kiểm tra quyền truy cập của ứng dụng và thông báo cho cha mẹ, giáo viên hoặc người có trách nhiệm khi phát hiện nguy cơ lộ, mất dữ liệu.

- *Tôn trọng và bảo vệ dữ liệu cá nhân của người khác:* Học sinh không được tự ý thu thập, sử dụng hoặc chia sẻ thông tin, hình ảnh, video, đoạn trò chuyện hay tài liệu cá nhân của người khác khi chưa được đồng ý. Khi thực hiện bài tập nhóm, tham gia mạng xã hội hoặc sử dụng công cụ số, học sinh cần tôn trọng quyền riêng tư của bạn bè, giáo viên và những người có liên quan.

- *Cung cấp dữ liệu đầy đủ và chính xác:* Khi cần cung cấp dữ liệu cá nhân theo quy định, theo thỏa thuận hoặc khi đồng ý cho phép xử lý dữ liệu, học sinh có trách nhiệm cung cấp thông tin đầy đủ và chính xác. Việc sử dụng thông tin sai lệch, giả mạo danh tính hoặc cung cấp dữ liệu của người khác có thể ảnh hưởng đến quyền lợi của chính học sinh và gây tổn hại cho người liên quan.

- *Tuân thủ pháp luật và tham gia phòng, chống hành vi xâm phạm dữ liệu cá nhân:* Học sinh cần thực hiện đúng các quy định về bảo vệ dữ liệu cá nhân; không mua bán, chiếm đoạt, tiết lộ hoặc sử dụng trái phép dữ liệu của người khác. Khi phát hiện hành vi xâm phạm dữ liệu cá nhân, học sinh không nên tiếp tục chia sẻ thông tin đó mà cần báo cho cha mẹ, giáo viên, nhà trường, nền tảng cung cấp dịch vụ hoặc cơ quan có thẩm quyền để được hỗ trợ xử lý.

Đối với học sinh chưa đủ khả năng tự thực hiện đầy đủ các quyền và trách nhiệm này, cha mẹ hoặc người đại diện theo pháp luật có vai trò hướng dẫn, hỗ trợ và thực hiện một số quyền thay cho các em.

Các quy định về quyền và nghĩa vụ của học sinh trong việc bảo vệ dữ liệu cá nhân cũng đặt ra yêu cầu đối với cơ quan, tổ chức và đơn vị cung cấp dịch vụ trong việc áp dụng các biện pháp bảo vệ, kiểm soát quyền truy cập và hạn chế nguy cơ dữ liệu bị truy cập, sử dụng, tiết lộ hoặc xử lý trái phép dữ liệu con người nói chung và của học sinh nói riêng.

1.2.3. An ninh mạng, sử dụng Internet và thông tin trên mạng

Luật An ninh mạng số 116/2025/QH15 và các nghị định hướng dẫn tạo thành khung pháp lý quan trọng điều chỉnh hoạt động trên không gian mạng. An ninh mạng không chỉ liên quan đến việc bảo vệ hệ thống kỹ thuật mà còn bao gồm việc bảo đảm thông tin, dữ liệu và hoạt động trên không gian mạng không gây phương hại đến quyền và lợi ích hợp pháp của tổ chức, cá nhân.

Đối với học sinh, những quy định này gắn trực tiếp với các hoạt động quen thuộc hằng ngày như sử dụng mạng xã hội, trò chuyện trực tuyến, đăng bài, bình luận, chia sẻ thông tin và sử dụng các tài khoản, dịch vụ trên Internet. Khi tham gia môi trường mạng, học sinh cần sử dụng tài khoản và thông tin đúng mục đích; không truy cập trái phép tài khoản, hệ thống hoặc dữ liệu của người khác; không chiếm đoạt, sử dụng trái phép hoặc phát tán thông tin; không mạo danh, xúc phạm, đe dọa hoặc thực hiện các hành vi xâm phạm quyền và lợi ích hợp pháp của người khác. Việc thực hiện những hành vi này thông qua mạng xã hội, ứng dụng nhắn tin hay các phương tiện điện tử vẫn có thể bị xem xét, xử lý theo quy định của pháp luật. Nghị định số 327/2026/NĐ-CP quy định cụ thể việc phòng ngừa và xử lý thông tin, hành vi vi phạm trên không gian mạng.

Học sinh cũng cần có trách nhiệm với thông tin mình đăng tải và chia sẻ. Không nên tạo, đăng lại hoặc tiếp tục phát tán thông tin khi chưa xác định được tính chính xác, đặc biệt là những thông tin có thể gây ảnh hưởng đến cá nhân, nhà trường hoặc cộng đồng. Nghị định số 328/2026/NĐ-CP quy định riêng về phòng, chống tin giả, tin sai sự thật trên không gian mạng.

Học sinh cần chú ý tới trách nhiệm của nền tảng mạng xã hội đối với nội dung vi phạm, cụ thể như:

Khi tham gia mạng xã hội, không chỉ người đăng, bình luận hoặc chia sẻ nội dung phải chịu trách nhiệm về hành vi của mình, mà nền tảng mạng xã hội và đơn vị cung cấp dịch vụ trên Internet cũng có trách nhiệm tham gia xử lý nội dung vi phạm pháp luật. Nghị định số 147/2024/NĐ-CP của Chính phủ quy định về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng là một trong những văn bản quy định các trách nhiệm này.

Nội dung vi phạm có thể bao gồm những thông tin, hình ảnh, video hoặc hoạt động trên mạng xâm phạm quyền và lợi ích hợp pháp của người khác, ảnh hưởng đến trẻ em hoặc thuộc những trường hợp bị pháp luật cấm. Khi phát hiện nội dung như vậy, cơ quan có thẩm quyền có thể yêu cầu đơn vị cung cấp dịch vụ ngăn chặn hoặc gỡ bỏ nội dung vi phạm. Theo Nghị định số 147/2024/NĐ-CP, đối với những trường hợp thuộc phạm vi quy định, việc kiểm tra, giám sát và loại bỏ nội dung vi phạm phải được thực hiện chậm nhất trong 24 giờ kể từ khi có yêu cầu của cơ quan có thẩm quyền.

Các em có thể hiểu đơn giản như sau: mạng xã hội không phải là nơi ai muốn đăng gì cũng được. Nếu một nội dung vi phạm pháp luật, nền tảng có trách nhiệm phối hợp để xử lý. Vì vậy, khi gặp một bài đăng, hình ảnh, video hoặc tài khoản có dấu hiệu giả mạo, lừa đảo, xúc phạm người khác, xâm phạm quyền riêng tư hoặc gây ảnh hưởng đến

trẻ em, học sinh không nên tiếp tục chia sẻ. Các em có thể sử dụng chức năng báo cáo của nền tảng và nói với cha mẹ, thầy cô hoặc người lớn tin cậy. Đối với những vụ việc nghiêm trọng, cơ quan có thẩm quyền có thể yêu cầu nền tảng thực hiện các biện pháp xử lý theo quy định.

Ví dụ: Một tài khoản đăng hình ảnh của một học sinh kèm thông tin giả mạo nhằm xúc phạm hoặc gây ảnh hưởng đến bạn đó. Học sinh không nên bình luận để chế giễu hoặc tiếp tục chia sẻ. Thay vào đó, các em có thể báo cáo nội dung, lưu lại thông tin cần thiết và nói với cha mẹ hoặc giáo viên. Nếu vụ việc có dấu hiệu vi phạm pháp luật, người lớn hoặc cơ quan có thẩm quyền có thể thực hiện các bước cần thiết để yêu cầu nền tảng xử lý.

Vì vậy, tuân thủ pháp luật về an ninh mạng đối với học sinh không phải là những yêu cầu xa lạ, mà bắt đầu từ cách ứng xử hằng ngày trên Internet: bảo vệ tài khoản, tôn trọng người khác, không xâm nhập hoặc sử dụng trái phép thông tin, kiểm tra thông tin trước khi chia sẻ và chịu trách nhiệm về những nội dung mình đăng tải, bình luận hoặc phát tán.

Tùy theo tính chất và mức độ của hành vi, vi phạm trên môi trường mạng có thể dẫn đến các trách nhiệm pháp lý khác nhau. Các quy định về xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng và bảo vệ dữ liệu cá nhân là căn cứ để xử lý những hành vi vi phạm tương ứng; đối với những hành vi nghiêm trọng, các quy định pháp luật khác về dân sự hoặc hình sự có thể được áp dụng.



Hình 1.1. Một số hành vi bị nghiêm cấm theo Điều 7 Luật An ninh mạng 2025

1.2.4. Sử dụng công cụ số và AI an toàn và có trách nhiệm

Đối với học sinh, các quy định chung về an ninh mạng và bảo vệ dữ liệu cá nhân được gắn với hoạt động giáo dục thông qua Khung năng lực số cho người học và các hướng dẫn triển khai của Bộ Giáo dục và Đào tạo. Thông tư số 02/2025/TT-BGDĐT ngày 24 tháng 01 năm 2025 của Bộ Giáo dục và Đào tạo quy định Khung năng lực số cho người học và Công văn số 3456/BGDĐT-GDPT ngày 27 tháng 6 năm 2025 của Bộ Giáo dục và Đào tạo về việc hướng dẫn triển khai thực hiện Khung năng lực số cho học sinh phổ thông và học viên giáo dục thường xuyên xác định những năng lực số cần hình thành và phát triển cho người học theo mức độ phù hợp với từng nhóm lớp. Trong đó, an toàn là một nội dung quan trọng của năng lực số. Học sinh từng bước được hình thành kiến thức và kỹ năng bảo vệ thiết bị, bảo vệ dữ liệu cá nhân và quyền riêng tư, bảo vệ sức khỏe và an sinh trong môi trường số, đồng thời nhận biết và xử lý các nguy cơ có thể gặp phải khi sử dụng công nghệ.

Cùng với năng lực số, sự phát triển nhanh chóng của trí tuệ nhân tạo đặt ra yêu cầu hướng dẫn học sinh sử dụng AI đúng mục đích, an toàn và có trách nhiệm. Quyết định số 2422/QĐ-BGDĐT ngày 18 tháng 8 năm 2026 của Bộ Giáo dục và Đào tạo ban hành Khung nội dung giáo dục trí tuệ nhân tạo cho học sinh phổ thông và Công văn số 5588/BGDĐT-GDPT ngày 19 tháng 8 năm 2026 của Bộ Giáo dục và Đào tạo về việc hướng dẫn triển khai thực hiện nội dung giáo dục trí tuệ nhân tạo cho học sinh phổ thông

từ năm học 2026–2027 cụ thể hóa nội dung giáo dục AI cho học sinh phổ thông theo từng cấp học. Các nội dung không chỉ hướng tới việc giúp học sinh hiểu về AI, biết sử dụng công cụ AI mà còn chú trọng nhận thức và đạo đức AI, tư duy phản biện, kiểm chứng kết quả do AI tạo ra, bảo vệ dữ liệu và quyền riêng tư.

Theo khung nội dung giáo dục AI, yêu cầu về năng lực trí tuệ nhân tạo đối với học sinh được phát triển theo mức độ phù hợp với từng cấp học. Ở những lớp đầu, học sinh chủ yếu hình thành nhận biết và các thói quen sử dụng công nghệ an toàn. Ở các lớp cao hơn, yêu cầu được mở rộng sang khả năng nhận biết rủi ro, lựa chọn biện pháp bảo vệ phù hợp, đánh giá thông tin và sử dụng các công cụ số, AI một cách chủ động, có trách nhiệm.

1.3. Kết luận chương

Chương 1 đã giúp học sinh làm quen với những quy định pháp luật cơ bản liên quan đến việc sử dụng Internet và tham gia môi trường số. Các quy định của Việt Nam và các văn kiện quốc tế đều hướng tới bảo vệ quyền, lợi ích và sự an toàn của trẻ em, đồng thời xác định trách nhiệm của mỗi người đối với hành vi của mình trên mạng.

Khi tham gia môi trường mạng, học sinh có quyền được bảo vệ đời sống riêng tư, thông tin và dữ liệu cá nhân, hình ảnh, danh dự và nhân phẩm. Các em cũng cần tôn trọng những quyền đó của người khác: không tự ý lấy, sử dụng hoặc chia sẻ thông tin, hình ảnh của bạn bè; không mạo danh, xâm nhập tài khoản, phát tán thông tin sai sự thật hoặc sử dụng Internet để xúc phạm, lừa đảo hay gây ảnh hưởng đến người khác.

Học sinh không cần ghi nhớ tất cả số hiệu văn bản hay điều khoản pháp luật. Điều quan trọng là hiểu mình có những quyền gì, cần tôn trọng quyền của người khác như thế nào, những hành vi nào không nên thực hiện và tìm sự giúp đỡ ở đâu khi gặp vấn đề. Đây cũng là nền tảng để các em tiếp tục tìm hiểu các nguy cơ, nguyên tắc và kỹ năng sử dụng mạng an toàn được trình bày trong những chương tiếp theo.

Bảng 1.1. Bảng tự đánh giá nhận thức pháp luật

Nội dung tự đánh giá	Có	Chưa
Em biết tên và số hiệu chính xác của luật hiện đang điều chỉnh an ninh mạng tại Việt Nam (Luật An ninh mạng 2025, số 116/2025/QH15)	☐	☐

Nội dung tự đánh giá	Có	Chưa
Em biết hành vi dùng AI để giả mạo hình ảnh, giọng nói người khác là hành vi bị pháp luật nghiêm cấm cụ thể (Điều 7 Luật ANM 2025)	☐	☐
Em biết nền tảng mạng xã hội có nghĩa vụ gỡ nội dung vi phạm trong 24 giờ khi có yêu cầu của cơ quan chức năng	☐	☐
Em biết cá nhân (không chỉ tổ chức, doanh nghiệp) cũng có thể bị xử phạt hành chính nếu phát tán trái phép dữ liệu cá nhân của người khác	☐	☐
Em biết trẻ em từ 7 tuổi trở lên có quyền được hỏi ý kiến trước khi thông tin đời sống riêng tư của mình bị công bố	☐	☐
Em biết ít nhất một văn bản hướng dẫn riêng của Bộ Giáo dục và Đào tạo về an toàn thông tin trong nhà trường (Quyết định số 447/QĐ-BGDĐT ngày 31 tháng 01 năm 2024 của Bộ Giáo dục và Đào tạo về việc phê duyệt Hướng dẫn bảo đảm an toàn thông tin, tham gia môi trường mạng an toàn đối với hoạt động giảng dạy, quản lý giáo dục)	☐	☐
Em biết Việt Nam là quốc gia đầu tiên trong ASEAN phê chuẩn một điều ước quốc tế mới về chống tội phạm mạng	☐	☐
Em hiểu vì sao tội phạm mạng xuyên biên giới (như lừa đảo game online) cần đến hợp tác quốc tế để xử lý, không thể chỉ dựa vào luật trong nước	☐	☐
Em biết các kênh hỗ trợ phù hợp khi gặp sự cố trên mạng, như Tổng đài 111, số khẩn cấp 113, cơ quan Công an nơi gần nhất và Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT) thuộc Cục An ninh mạng, Bộ Công an	☐	☐
Em hiểu rằng cùng một hành vi vi phạm có thể đồng thời chịu điều chỉnh bởi nhiều văn bản pháp luật khác nhau (an ninh mạng, dữ liệu cá nhân, dân sự)	☐	☐

CHƯƠNG 2. NGUYÊN TẮC, KỸ NĂNG SỬ DỤNG MẠNG AN TOÀN

Chương này trình bày các nguyên tắc và kỹ năng cơ bản giúp học sinh sử dụng Internet an toàn, có trách nhiệm và văn minh. Nội dung được tham khảo, chọn lọc và điều chỉnh cho phù hợp với bối cảnh giáo dục Việt Nam từ ba nguồn chính: chương trình Be Internet Awesome của Google với năm trụ cột Thông minh (Smart) – Cảnh giác (Alert) – Vững vàng (Strong) – Tử tế (Kind) – Dũng cảm (Brave) [1]; Bộ Quy tắc ứng xử về bảo vệ trẻ em trên môi trường mạng [2], ban hành kèm theo Quyết định số 88/QĐ-BTTTT ngày 21/01/2025 của Bộ Thông tin và Truyền thông (nay thuộc Bộ Khoa học và Công nghệ); và Cẩm nang bảo vệ trẻ em trên môi trường mạng năm 2024 của Cục An toàn thông tin.

Mỗi nguyên tắc không chỉ nêu những việc học sinh nên làm hoặc cần tránh, mà còn được giải thích thông qua quy định pháp luật, nguy cơ thường gặp và các tình huống thực tế. Cách trình bày này giúp học sinh hiểu rõ vì sao cần tuân thủ các nguyên tắc an toàn, đồng thời cung cấp cho giáo viên và cha mẹ những nội dung cần thiết để hướng dẫn, trao đổi và hỗ trợ các em trong quá trình sử dụng Internet.

Bảng 2.1 dưới đây tổng hợp thành 12 nguyên tắc "vàng" dễ nhớ, dễ áp dụng cho học sinh phổ thông Việt Nam làm khung nội dung xuyên suốt cho tài liệu và bộ infographic tuyên truyền:

Bảng 2.1. Tổng hợp 12 nguyên tắc vàng giúp nhận thức và bảo vệ thông tin

STT	Nguyên tắc "vàng"	Nội dung thực hành
01	Suy nghĩ kỹ trước khi đăng	Nội dung đã đăng lên mạng có thể bị người khác lưu lại, sao chép hoặc chia sẻ tiếp, nên đôi khi khó thu hồi hoàn toàn. Hãy suy nghĩ kỹ trước khi đăng hoặc chia sẻ. Nếu lỡ đăng nội dung không phù hợp, hãy xóa, báo cáo và nhờ người lớn hỗ trợ khi cần.
02	Giữ kín thông tin định danh	Không công khai họ tên đầy đủ kèm trường lớp, địa chỉ nhà, số điện thoại, lịch trình di chuyển hằng ngày.

STT	Nguyên tắc "vàng"	Nội dung thực hành
03	Đặt mật khẩu mạnh, bật xác thực 2 yếu tố	Sử dụng mật khẩu riêng cho từng tài khoản và luôn bật xác thực 2 yếu tố (2FA) cho email, mạng xã hội.
04	Cảnh giác với người lạ	Không kết bạn, nhắn tin riêng hay hẹn gặp người chỉ quen qua mạng nếu chưa có sự đồng ý, giám sát của cha mẹ.
05	Không chia sẻ hình ảnh nhạy cảm	Tuyệt đối không gửi, đăng ảnh/video riêng tư của bản thân hoặc người khác, kể cả trong nhóm chat kín.
06	Dừng – Nghĩ – Kiểm tra trước khi tin	Xác minh nguồn, tác giả, thời điểm đăng trước khi tin và chia sẻ bất kỳ thông tin nào.
07	Tôn trọng, không bắt nạt trên mạng	Không dùng lời lẽ miệt thị, chế giễu, cô lập bạn bè trong nhóm chat hay bình luận công khai.
08	Biết sử dụng nút Report/Block	Báo cáo và chặn ngay tài khoản, nội dung độc hại, quấy rối thay vì tranh cãi hoặc im lặng chịu đựng.
09	Cân bằng thời gian thực – ảo	Giới hạn thời gian giải trí trên màn hình, ưu tiên vận động, giao tiếp trực tiếp và giấc ngủ đủ.
10	Luôn cập nhật phần mềm, thiết bị	Cập nhật hệ điều hành, ứng dụng thường xuyên để vá các lỗ hổng bảo mật mới bị phát hiện.
11	Nói với người lớn tin cậy khi có vấn đề	Chủ động chia sẻ với cha mẹ, thầy cô ngay khi gặp nội dung xấu, bị đe dọa hoặc cảm thấy bất an.
12	Bật chế độ riêng tư trên từng nền tảng	Chủ động thiết lập tài khoản ở chế độ riêng tư, giới hạn người xem trên Zalo, TikTok, Facebook.

2.1. Nguyên tắc cốt lõi

Mỗi hoạt động trên Internet, từ tìm kiếm thông tin, trao đổi tin nhắn đến đăng tải hình ảnh và sử dụng mạng xã hội, đều có thể ảnh hưởng đến sự an toàn của bản thân và

người khác. Vì vậy, học sinh cần hình thành những nguyên tắc chung để định hướng cách suy nghĩ và hành động trong các tình huống khác nhau. Sáu nguyên tắc dưới đây tập trung vào việc chia sẻ có trách nhiệm, bảo vệ thông tin cá nhân, kiểm chứng thông tin, tôn trọng người khác, tìm kiếm sự hỗ trợ và duy trì sự cân bằng khi sử dụng Internet.

2.1.1. Suy nghĩ trước khi đăng và chia sẻ

Mỗi nội dung được đăng tải hoặc chia sẻ trên Internet đều có thể để lại dấu vết. Một bức ảnh, đoạn video, bình luận hoặc tin nhắn sau khi gửi đi có thể bị người khác chụp lại, sao chép và chuyển tiếp, kể cả khi người đăng đã xóa nội dung ban đầu. Vì vậy, trước khi đăng tải hoặc chia sẻ, học sinh cần suy nghĩ về nội dung, đối tượng tiếp nhận và những ảnh hưởng có thể xảy ra.

Suy nghĩ trước khi chia sẻ không có nghĩa là học sinh phải lo sợ hoặc ngừng thể hiện bản thân trên môi trường mạng. Điều quan trọng là biết cân nhắc để những nội dung được chia sẻ không làm lộ thông tin riêng tư, gây hiểu lầm, ảnh hưởng đến người khác hoặc tạo ra hậu quả mà bản thân không mong muốn.

Trước khi nhấn nút đăng, gửi hoặc chia sẻ, học sinh nên tự hỏi:

- Nội dung này có làm lộ thông tin cá nhân của mình hoặc người khác không?
- Thông tin trong nội dung có chính xác không?
- Việc chia sẻ có thể làm ai đó buồn, xấu hổ hoặc bị tổn thương không?
- Nếu cha mẹ, thầy cô hoặc bạn bè nhìn thấy, mình có cảm thấy thoải mái không?
- Nội dung này có thể gây ảnh hưởng đến mình trong tương lai không?

Ví dụ, một học sinh chụp ảnh cả lớp trong giờ nghỉ và muốn đăng lên mạng xã hội. Trước khi đăng, em cần kiểm tra xem trong ảnh có bạn nào đang ở tư thế không phù hợp, có thông tin trên bảng, điểm số, số điện thoại hoặc dữ liệu cá nhân nào bị lộ hay không. Em cũng cần hỏi ý kiến những người xuất hiện trong ảnh, thay vì cho rằng mình có quyền đăng chỉ vì mình là người chụp.

Học sinh cũng cần thận trọng khi chuyển tiếp nội dung do người khác gửi. Việc "chỉ chia sẻ lại" không làm mất đi trách nhiệm của người chia sẻ. Nếu nội dung sai sự thật, xúc phạm người khác hoặc xâm phạm quyền riêng tư, người chuyển tiếp vẫn có thể góp phần làm cho tác hại lan rộng hơn.

Điều cần nhớ: Nội dung đã đưa lên mạng có thể vượt khỏi sự kiểm soát của người đăng. Hãy dừng lại, suy nghĩ và kiểm tra trước khi chia sẻ.

2.1.2. Bảo vệ thông tin cá nhân, tài khoản và quyền riêng tư

Thông tin cá nhân họ tên đầy đủ gắn với trường học, địa chỉ nhà, số điện thoại, ảnh gia đình có thể nhận diện nơi ở là "chìa khóa" mà kẻ xấu cần để tiếp cận, theo dõi hoặc mạo danh học sinh ngoài đời thực. Theo Điều 33 Nghị định số 56/2017/NĐ-CP ngày 09 tháng 5 năm 2017 của Chính phủ quy định chi tiết một số điều của Luật Trẻ em, "thông tin bí mật đời sống riêng tư, bí mật cá nhân của trẻ em" được pháp luật liệt kê rất cụ thể và việc đưa các thông tin này lên mạng phải có sự đồng ý của cha, mẹ hoặc người chăm sóc trẻ; với trẻ từ đủ 7 tuổi trở lên, cần phải có thêm sự đồng ý của chính trẻ. Không phải mọi thông tin cá nhân đều phải giữ bí mật tuyệt đối. Tuy nhiên, học sinh cần hiểu thông tin nào có thể chia sẻ, chia sẻ với ai và trong hoàn cảnh nào. Việc công khai quá nhiều thông tin có thể khiến người xấu giả mạo danh tính, tiếp cận học sinh ngoài đời thực hoặc sử dụng thông tin vào mục đích không phù hợp.

Một số thông tin cần được bảo vệ đặc biệt vì khi bị lộ hoặc sử dụng trái phép có thể dẫn đến mất tài khoản, mất tài sản, bị giả mạo danh tính hoặc bị xâm phạm quyền riêng tư. Những thông tin này bao gồm mật khẩu, mã xác thực tài khoản; thông tin về sức khỏe, tài chính; dữ liệu sinh trắc học như khuôn mặt, vân tay; và hình ảnh, video mang tính riêng tư. Học sinh không nên công khai hoặc gửi những thông tin này cho người khác khi chưa xác định rõ người nhận và mục đích sử dụng. Bảng phân tích dưới đây giúp học sinh và giáo viên xác định thứ tự ưu tiên khi hướng dẫn:

Bảng 2.2. Phân loại mức độ rủi ro của loại thông tin cá nhân

Loại thông tin	Mức độ rủi ro	Vì sao
Họ tên đầy đủ + trường, lớp đang học	Cao	Đủ để kẻ xấu xác định vị trí, thời gian biểu và tiếp cận trực tiếp ngoài đời
Địa chỉ nhà, lịch trình di chuyển hằng ngày	Cao	Nguy cơ bị theo dõi, đột nhập, tiếp cận khi không có người lớn giám sát
Ảnh, video riêng tư (kể cả trong nhóm chat kín)	Cao	Có thể bị phát tán ngoài ý muốn, dùng để đe dọa, tống tiền
Số điện thoại, tài khoản mạng xã hội của cha mẹ	Trung bình – Cao	Là điểm khởi đầu để dàn dựng kịch bản lừa đảo cả gia đình

Loại thông tin	Mức độ rủi ro	Vì sao
Thành tích học tập, sở thích cá nhân (không kèm định danh)	Thấp	Ít nguy cơ nếu không đi kèm thông tin giúp xác định danh tính, vị trí
Cảm nghĩ, sản phẩm sáng tạo cá nhân đã kiểm duyệt	Thấp	An toàn nếu không tiết lộ thông tin định danh trong nội dung hoặc bình luận

Để bảo vệ thông tin và quyền riêng tư, học sinh cần ghi nhớ:

- Không công khai địa chỉ nhà, số điện thoại, lịch trình hằng ngày hoặc vị trí hiện tại.

- Không gửi mật khẩu, mã xác thực hoặc thông tin đăng nhập cho người khác.

- Không đăng ảnh giấy tờ cá nhân, thẻ học sinh, vé, mã QR hoặc màn hình có chứa thông tin riêng tư.

- Không chia sẻ hình ảnh hoặc video riêng tư của bản thân và người khác.

- Xin phép trước khi đăng hình ảnh, thông tin hoặc nội dung trò chuyện có liên quan đến người khác.

- Chỉ cung cấp thông tin cá nhân khi thực sự cần thiết và biết rõ người hoặc tổ chức tiếp nhận.

- Chủ động kiểm tra ai có thể xem hồ sơ, bài đăng và thông tin cá nhân của mình.

Ví dụ, một tài khoản tự xưng là ban tổ chức cuộc thi gửi tin nhắn thông báo học sinh đã trúng giải và yêu cầu cung cấp họ tên, địa chỉ, ảnh căn cước của cha mẹ cùng mã xác thực để nhận quà. Dù lời đề nghị có vẻ hấp dẫn, học sinh không nên cung cấp thông tin ngay mà cần kiểm tra lại qua trang chính thức và trao đổi với cha mẹ hoặc giáo viên.

Bảo vệ quyền riêng tư cũng có nghĩa là tôn trọng dữ liệu của người khác. Học sinh không được tự ý xem trộm tin nhắn, đăng nhập tài khoản, phát tán hình ảnh hoặc chia sẻ bí mật của bạn bè. Việc một người đã gửi thông tin cho mình không đồng nghĩa với việc mình được phép chuyển tiếp thông tin đó cho người khác.

Điều cần nhớ: Thông tin cá nhân có giá trị và cần được bảo vệ. Chỉ chia sẻ khi thực sự cần thiết, đúng người và đúng mục đích.

a. Infographic minh họa: "Những gì KHÔNG nên đăng"

Hình ảnh dưới đây là nội dung KHÔNG NÊN đăng hoặc chia sẻ thông tin trên mạng xã hội để học sinh có thể hiểu và nhận thức được các thông tin trước khi sử dụng nó trên Internet, điều này sẽ giúp học sinh dễ ghi nhớ:



Hình 2.1. Những gì KHÔNG nên đăng/chia sẻ trên mạng xã hội

b. Tình huống thực tế

Tình huống: Chuyển tiếp "thông báo nghỉ học". Trong nhóm lớp có người gửi ảnh một thông báo "Ngày mai toàn trường nghỉ học" và yêu cầu mọi người chia sẻ ngay.

Đối với tình huống này, các cấp độ trường học sẽ nên được xử lý như sau:

Tiểu học: Không chuyển tiếp ngay. Hỏi cha mẹ hoặc giáo viên.

THCS: Kiểm tra tài khoản gửi, trang của trường hoặc hỏi GVCN trước khi chia sẻ.

THPT: Kiểm tra nguồn, thời điểm, tính xác thực của văn bản và tránh trở thành người tiếp tục lan truyền thông tin chưa kiểm chứng.

Nguyên tắc an toàn: Tiểu học: hỏi người lớn. THCS: dừng và kiểm tra. THPT: kiểm chứng và chịu trách nhiệm.

Hình 2.2 minh họa về tình huống cụ thể khi học sinh gặp phải và cách ứng phó.



Hình 2.2. Cách ứng phó với tình huống thực tế cho các cấp độ trường học

2.1.3. Cảnh giác và kiểm chứng trước khi tin hoặc hành động

Thông tin trên Internet rất phong phú nhưng không phải nội dung nào cũng chính xác và không phải tài khoản nào cũng thể hiện đúng danh tính thật. Tin giả, tài khoản mạo danh, quảng cáo sai lệch, liên kết lừa đảo và nội dung do trí tuệ nhân tạo tạo ra ngày càng khó nhận biết. Vì vậy, học sinh cần hình thành thói quen kiểm tra trước khi tin, chia sẻ hoặc thực hiện một yêu cầu trên mạng.

Để phân tích một nguồn tin chính xác hơn, nên phân biệt ba dạng thông tin sai lệch thường bị gộp chung là "tin giả":

- *Thông tin sai không chủ đích:* người chia sẻ tin là đúng nhưng thực chất thông tin đã lỗi thời, thiếu ngữ cảnh hoặc bị hiểu nhầm.

- *Thông tin sai có chủ đích*: được tạo ra và lan truyền có chủ đích nhằm đánh lừa người đọc, thường vì mục đích lừa đảo, câu tương tác hoặc định hướng dư luận.

- *Nội dung bị chỉnh sửa/giả mạo bằng công nghệ (deepfake)*: hình ảnh, giọng nói, video bị dựng hoặc chỉnh sửa bằng AI để trông giống người thật – hình thức ngày càng khó phân biệt bằng mắt thường; cần đặc biệt cảnh giác với các đoạn ghi âm/gọi video "khẩn cấp" yêu cầu chuyển tiền.

Cảnh giác không có nghĩa là nghi ngờ tất cả mọi người và mọi thông tin. Cảnh giác là biết đặt câu hỏi, tìm thêm bằng chứng và không hành động vội vàng khi chưa xác định được độ tin cậy.

Học sinh cần đặc biệt thận trọng khi gặp những nội dung:

- Đưa ra phần thưởng hoặc lợi ích quá hấp dẫn.

- Yêu cầu phải hành động ngay nếu không sẽ mất cơ hội hoặc bị khóa tài khoản.

- Yêu cầu cung cấp mật khẩu, mã xác thực hoặc chuyển tiền.

- Sử dụng tiêu đề gây sốc, kích động sự sợ hãi, tức giận hoặc tò mò.

- Không ghi rõ tác giả, nguồn tin hoặc thời điểm đăng.

- Giả danh thầy cô, bạn bè, cơ quan nhà nước hoặc tổ chức quen thuộc.

- Dẫn đến một trang web có địa chỉ lạ, sai chính tả hoặc khác với địa chỉ chính thức.

- Sử dụng hình ảnh, giọng nói hoặc video có dấu hiệu bất thường.

Khi tiếp nhận một thông tin, học sinh nên kiểm tra người đăng, nguồn gốc, thời điểm và bằng chứng đi kèm; đồng thời đối chiếu với những nguồn đáng tin cậy khác. Nếu chưa kiểm chứng được, học sinh không nên chia sẻ hoặc làm theo nội dung đó.

Cách kiểm tra một nguồn tin:

- Dấu tích xanh (tài khoản đã xác minh): chỉ là một tín hiệu tham khảo, không đồng nghĩa mọi nội dung đăng tải đều chính xác, vẫn cần đối chiếu với nguồn chính thống.

- Ngày đăng: tin cũ bị chia sẻ lại không ghi rõ thời gian là một chiêu thức phổ biến để gây hoang mang về một sự việc "mới".

- Tác giả/đơn vị đăng tải: ưu tiên các cơ quan báo chí được cấp phép, cổng thông tin của Bộ, ngành, chính quyền địa phương.

- Đối chiếu chéo: nếu chỉ một trang không rõ nguồn gốc đưa tin trong khi báo chí chính thống im lặng, khả năng cao đó là tin giả.

- Cảm xúc khi đọc: tin giả thường cố tình kích động sợ hãi, phẫn nộ hoặc thương cảm mạnh để thúc đẩy chia sẻ ngay lập tức – đây tự nó là một dấu hiệu cần chậm lại.

Quy tắc "Dừng – Nghĩ – Kiểm tra"

DỪNG: không vội bấm Chia sẻ/Chuyển tiếp ngay khi vừa đọc tiêu đề giật gân.

NGHĨ: đặt câu hỏi "nguồn tin này có đáng tin không? Mình có đang bị dẫn dắt cảm xúc không?"

KIỂM TRA: tra cứu lại trên báo chí chính thống hoặc hỏi thầy cô, cha mẹ trước khi tin và chia sẻ tiếp.

Ví dụ, trong nhóm lớp xuất hiện thông báo "ngày mai toàn trường được nghỉ học" kèm ảnh chụp một văn bản nhưng không có nguồn chính thức. Học sinh không nên lập tức chuyển tiếp sang các nhóm khác. Cách xử lý phù hợp là kiểm tra trang thông tin của nhà trường hoặc hỏi giáo viên chủ nhiệm.

Nguyên tắc này cũng áp dụng với nội dung do công cụ trí tuệ nhân tạo cung cấp. Câu trả lời của AI có thể rõ ràng và thuyết phục nhưng vẫn có thể thiếu chính xác, lỗi thời hoặc tạo ra nguồn tài liệu không có thật. Vì vậy, học sinh cần đối chiếu với sách giáo khoa, tài liệu chính thức hoặc nguồn đáng tin cậy trước khi sử dụng.

Điều cần nhớ: Đừng vội tin chỉ vì một nội dung được trình bày hấp dẫn hoặc được nhiều người chia sẻ. Hãy dừng lại, kiểm tra và xác minh trước khi hành động.

2.1.4. Tôn trọng bản thân và người khác trên môi trường mạng

Giao tiếp trên Internet cũng cần tuân theo những chuẩn mực như giao tiếp trực tiếp. Việc không nhìn thấy phản ứng của người đối diện không có nghĩa là lời nói hoặc hành động trên mạng không gây tổn thương. Một bình luận chế giễu, bức ảnh bị chỉnh sửa hoặc tin nhắn công kích có thể ảnh hưởng nghiêm trọng đến danh dự, tâm lý và cuộc sống của người khác.

Tôn trọng người khác trên môi trường mạng được thể hiện qua những hành vi như:

- Sử dụng ngôn ngữ lịch sự, phù hợp với hoàn cảnh.
- Tôn trọng sự khác biệt về ngoại hình, năng lực, hoàn cảnh và quan điểm.
- Không xúc phạm, miệt thị, đe dọa hoặc cô lập người khác.
- Không tham gia các nhóm được lập ra để nói xấu hoặc công kích một người.
- Không cổ vũ, bình luận hoặc chia sẻ nội dung bắt nạt.
- Không tự ý công khai hình ảnh, tin nhắn hoặc bí mật của người khác.
- Biết nhận lỗi, sửa sai và gỡ bỏ nội dung khi hành vi của mình gây ảnh hưởng.

Học sinh cũng cần biết bảo vệ sự tôn trọng dành cho chính mình. Khi bị xúc phạm, gây áp lực hoặc yêu cầu làm điều khiến bản thân không thoải mái, các em có quyền từ chối, dừng tương tác và tìm kiếm sự hỗ trợ. Không ai có quyền buộc học sinh phải gửi

ảnh riêng tư, tiết lộ bí mật hoặc tiếp tục một cuộc trò chuyện khiến các em lo lắng, sợ hãi.

Ví dụ, một nhóm học sinh lấy ảnh của bạn trong lớp, chỉnh sửa thành hình gây cười rồi chia sẻ trong nhóm chat. Một số bạn không trực tiếp chỉnh sửa nhưng bình luận, gửi biểu tượng cười hoặc chuyển tiếp hình ảnh. Những hành động này đều góp phần làm tổn thương người trong ảnh. Cách ứng xử phù hợp là không tham gia, đề nghị dừng chia sẻ, hỗ trợ người bị ảnh hưởng và thông báo cho giáo viên khi cần thiết.

Trước khi bình luận hoặc gửi một nội dung, học sinh có thể tự hỏi: "Nếu người khác nói hoặc làm điều này với mình, mình sẽ cảm thấy thế nào?". Đây là cách đơn giản để cân nhắc tác động của hành vi đối với người khác.

Điều cần nhớ: Hãy đối xử với người khác trên mạng như cách mình mong muốn được đối xử. Không tham gia, cổ vũ hoặc tiếp tay cho hành vi gây tổn thương.

2.1.5. Chủ động lên tiếng và tìm kiếm sự hỗ trợ khi cần thiết

Trong quá trình sử dụng Internet, học sinh có thể gặp những tình huống khiến mình bối rối, lo lắng, xấu hổ hoặc sợ hãi. Đó có thể là một tin nhắn đe dọa, lời mời gặp mặt của người lạ, yêu cầu gửi ảnh riêng tư, tài khoản bị chiếm quyền, nội dung bắt nạt hoặc một đường liên kết đáng ngờ đã vô tình được mở.

Khi gặp những tình huống như vậy, học sinh không nên im lặng, che giấu hoặc tự mình đối phó với người xấu. Việc chủ động tìm kiếm sự hỗ trợ không phải là biểu hiện của sự yếu đuối. Ngược lại, đó là cách hành động bình tĩnh và có trách nhiệm.

Học sinh cần:

- Dừng tương tác khi cảm thấy bất an hoặc bị gây áp lực.
- Không tranh cãi, đe dọa lại hoặc làm theo yêu cầu của đối tượng.
- Không chuyển tiền hoặc tiếp tục cung cấp thông tin.
- Trao đổi với cha mẹ, giáo viên hoặc người lớn đáng tin cậy.
- Sử dụng chức năng chặn và báo cáo khi phù hợp.
- Giữ lại những thông tin cần thiết để người lớn có thể hỗ trợ xử lý.
- Báo ngay khi bản thân hoặc bạn bè có nguy cơ bị tổn hại.

Ví dụ, một người quen qua mạng yêu cầu học sinh gửi ảnh riêng tư và đe dọa sẽ tung các tin nhắn trước đó nếu em từ chối. Học sinh không nên tiếp tục thương lượng

hoặc gửi thêm nội dung. Em cần dừng cuộc trò chuyện, lưu lại thông tin cần thiết và báo ngay cho cha mẹ, giáo viên hoặc người lớn đáng tin cậy.

Khi một người bạn tâm sự rằng đang bị bắt nạt hoặc đe dọa trên mạng, học sinh không nên hứa giữ bí mật bằng mọi giá. Nếu sự việc có thể ảnh hưởng đến sự an toàn của bạn, cần khuyến khích bạn tìm người lớn hỗ trợ hoặc chủ động báo cho người có trách nhiệm.

Trong trường hợp cần tư vấn hoặc hỗ trợ liên quan đến trẻ em, học sinh và người lớn có thể liên hệ Tổng đài quốc gia bảo vệ trẻ em 111. Nếu có dấu hiệu nguy hiểm trực tiếp đến tính mạng, sức khỏe hoặc an toàn, cần báo ngay cho gia đình, nhà trường hoặc cơ quan công an gần nhất.

Điều cần nhớ: Khi có điều gì khiến em lo lắng hoặc không an toàn, hãy dừng lại và nói với người lớn đáng tin cậy. Không cần phải giải quyết mọi việc một mình.

2.1.6. Sử dụng Internet cân bằng, lành mạnh và có mục đích

Internet mang lại nhiều lợi ích cho học tập, giao tiếp và giải trí. Tuy nhiên, để những lợi ích đó không đi kèm với ảnh hưởng tiêu cực, học sinh cần biết kiểm soát thời gian, lựa chọn cách sử dụng phù hợp và xác định rõ mục đích mỗi khi tham gia môi trường mạng.

a. Sử dụng Internet cân bằng

Sử dụng Internet cân bằng trước hết là biết kiểm soát thời gian sử dụng thiết bị và các dịch vụ trực tuyến. Nếu dành quá nhiều thời gian cho mạng xã hội, trò chơi hoặc video giải trí, học sinh có thể bị thiếu ngủ, giảm khả năng tập trung, ít vận động và không còn đủ thời gian cho học tập, gia đình hoặc các hoạt động trực tiếp.

Không phải mọi khoảng thời gian sử dụng thiết bị đều có tính chất giống nhau. Thời gian học trực tuyến, tìm kiếm tài liệu hoặc làm bài tập không nên được đánh giá giống với thời gian lướt mạng xã hội và xem video giải trí. Vì vậy, học sinh cần quan tâm cả tổng thời gian sử dụng và mục đích của từng hoạt động.

Để duy trì sự cân bằng, học sinh nên:

- Lập kế hoạch thời gian học tập và giải trí trong ngày.

- Xác định trước khoảng thời gian dành cho mạng xã hội, trò chơi và video.

- Hoàn thành nhiệm vụ học tập trước khi tham gia hoạt động giải trí trực tuyến.

- Nghỉ giải lao hợp lý khi phải sử dụng thiết bị trong thời gian dài.

- Không để việc sử dụng Internet làm ảnh hưởng đến giờ ngủ, bữa ăn, vận động và giao tiếp với gia đình.

- Sử dụng các chức năng theo dõi, giới hạn thời gian trên thiết bị khi cần thiết.

- Tự dừng hoặc nhờ người lớn hỗ trợ nếu không thể kiểm soát được thời gian sử dụng.

Bảng 2.3. Khuyến nghị thời gian sử dụng theo độ tuổi

Nhóm tuổi	Khuyến nghị thời gian màn hình	Ghi chú
Dưới 2 tuổi	Không khuyến khích, trừ gọi video có người lớn cùng tham gia	Giai đoạn phát triển nhận thức nền tảng qua tương tác trực tiếp
2–4 tuổi	Tối đa 1 giờ/ngày, có giám sát	Cần chia nhỏ thời gian, ưu tiên nội dung giáo dục
5–17 tuổi (học sinh phổ thông)	Không quá 2 giờ/ngày cho mục đích giải trí (không tính thời gian học tập)	Khuyến nghị được nhiều cơ sở y tế tại Việt Nam áp dụng, định hướng theo WHO

Một số dấu hiệu cần lưu ý là thường xuyên thức khuya để sử dụng mạng; không thể dừng dù đã có kế hoạch; cảm thấy bồn chồn hoặc tức giận khi không được dùng thiết bị; bỏ bê học tập, vận động hoặc giao tiếp trực tiếp; sử dụng mạng để trốn tránh mọi cảm xúc tiêu cực.

Ví dụ, một học sinh mở máy tính để tìm tài liệu làm bài nhưng liên tục chuyển sang xem video và mạng xã hội. Sau nhiều giờ, bài tập vẫn chưa hoàn thành và em phải thức khuya. Trong trường hợp này, vấn đề không chỉ nằm ở tổng thời gian sử dụng thiết bị mà còn ở việc không kiểm soát được mục đích và sự phân tâm.

Cha mẹ cũng cần nhận biết một số dấu hiệu sử dụng Internet thiếu cân bằng ở trẻ như: thường xuyên thức khuya, trì hoãn việc học, bỏ bữa hoặc ít vận động, cảm thấy khó chịu khi phải rời thiết bị, không thể dừng dù đã có kế hoạch, hoặc dành phần lớn thời gian rảnh cho các hoạt động trực tuyến.

Điều cần nhớ: Hãy chủ động quản lý thời gian sử dụng Internet, không để Internet chiếm mất thời gian dành cho giấc ngủ, học tập, vận động và những người xung quanh.

b. Sử dụng Internet lành mạnh

Sử dụng Internet lành mạnh là lựa chọn nội dung, cách tương tác và thói quen sử dụng không gây tổn hại đến sức khỏe thể chất, tinh thần của bản thân và người khác.

Học sinh cần:

- Lựa chọn nội dung phù hợp với độ tuổi và nhu cầu.

- Không tham gia các thử thách nguy hiểm hoặc hoạt động có thể gây tổn thương.

- Tránh những nội dung khiến bản thân thường xuyên lo lắng, sợ hãi, tức giận hoặc tự ti.

- Không chạy theo lượt thích, bình luận hoặc sự công nhận trên mạng.

- Duy trì tư thế ngồi phù hợp, khoảng cách an toàn với màn hình và nghỉ mắt định kỳ.

- Không sử dụng điện thoại khi đi đường, điều khiển phương tiện hoặc trong những tình huống cần tập trung.

- Duy trì các hoạt động ngoài trời, vận động, giao tiếp trực tiếp và sở thích không sử dụng thiết bị.

- Chia sẻ với cha mẹ, giáo viên khi nội dung trên mạng ảnh hưởng tiêu cực đến cảm xúc hoặc tâm lý.

Ví dụ, một học sinh thường xuyên xem những nội dung so sánh ngoại hình và bắt đầu cảm thấy tự ti, lo lắng về bản thân. Thay vì tiếp tục theo dõi, em có thể ẩn hoặc bỏ theo dõi những tài khoản đó, lựa chọn nội dung tích cực hơn và trao đổi với người lớn đáng tin cậy nếu cảm xúc tiêu cực kéo dài.

Điều cần nhớ: Nội dung và cách sử dụng Internet cần góp phần bảo vệ sức khỏe, tinh thần và sự phát triển của học sinh, không làm các em mệt mỏi, lo lắng hoặc tổn thương.

c. Sử dụng Internet có mục đích

Sử dụng Internet có mục đích là biết rõ mình truy cập để làm gì và tập trung vào hoạt động đã xác định. Nếu không có mục đích rõ ràng, học sinh rất dễ bị cuốn từ một thông báo sang một video, trò chơi hoặc nội dung khác mà không nhận ra thời gian đang trôi qua.

Trước khi mở thiết bị hoặc truy cập Internet, học sinh nên tự hỏi:

- Mình đang vào mạng để làm gì?

- Hoạt động này có thực sự cần thiết không?

- Mình dự định sử dụng trong bao lâu?

- Khi nào công việc được xem là hoàn thành?

- Nội dung này có phù hợp với mục tiêu học tập hoặc giải trí của mình không?

Khi sử dụng Internet để học tập, học sinh nên xác định rõ nhiệm vụ, chuẩn bị nguồn tài liệu cần thiết và hạn chế những ứng dụng gây phân tâm. Khi sử dụng để giải trí, các em cũng cần lựa chọn nội dung phù hợp và xác định điểm dừng.

Ví dụ, nếu cần tìm hiểu về biến đổi khí hậu để làm bài thuyết trình, học sinh nên xác định những thông tin cần tìm, ưu tiên nguồn đáng tin cậy và lưu lại tài liệu cần thiết. Việc chuyển sang xem các nội dung không liên quan khiến quá trình học tập kéo dài nhưng không đạt được kết quả mong muốn.

Điều cần nhớ: Trước khi truy cập Internet, hãy xác định rõ mục đích; trong khi sử dụng, hãy tập trung; khi hoàn thành, hãy chủ động dừng lại.

2.2. Kỹ năng sử dụng mạng an toàn

Các nguyên tắc an toàn là bước đầu tiên, nhưng để tự bảo vệ mình trên Internet, học sinh còn cần biến những nguyên tắc đó thành thói quen hằng ngày. Một tài khoản có mật khẩu tốt nhưng vẫn có thể gặp rủi ro nếu người dùng đưa mã xác thực cho người khác; một thiết bị được cài phần mềm bảo vệ vẫn có thể bị lừa nếu người dùng bấm vào đường liên kết giả mạo; và ngay cả tài khoản riêng tư cũng không hoàn toàn an toàn nếu học sinh tin tưởng một người lạ quá nhanh.

Vì vậy, phần này tập trung vào ba nhóm kỹ năng rất gần với việc sử dụng Internet hằng ngày của học sinh: bảo vệ tài khoản, giao tiếp an toàn với người khác và giữ thiết bị an toàn, nhận diện lừa đảo. Đây là những kỹ năng không chỉ cần biết mà cần được thực hành thường xuyên.

2.2.1. Xây dựng và quản lý mật khẩu mạnh

Mật khẩu là lớp bảo vệ đầu tiên của tài khoản. Nếu mật khẩu quá ngắn, dễ đoán hoặc được dùng chung cho nhiều dịch vụ, nguy cơ mất tài khoản sẽ tăng lên đáng kể. Chẳng hạn, nếu một ứng dụng bị lộ dữ liệu và học sinh sử dụng cùng một mật khẩu cho email, mạng xã hội và trò chơi trực tuyến, người xấu có thể thử chính mật khẩu đó trên các tài khoản khác.

Vì vậy, một nguyên tắc quan trọng là: mật khẩu cần đủ dài, khó đoán và không dùng lại cho nhiều tài khoản quan trọng. Những tài khoản như email, mạng xã hội, tài khoản học tập hoặc tài khoản có liên quan đến thanh toán cần được bảo vệ cẩn thận hơn.

a. Công thức "Câu chuyện + số + ký tự đặc biệt"

Không nên sử dụng tên, ngày sinh, số điện thoại, tên trường, lớp hoặc những thông tin người khác dễ biết để làm mật khẩu. Các dạng như Hoan2012, 12345678, password, tên thú cưng hoặc ngày sinh đều có thể bị đoán khá dễ. Thay vì cố tạo một chuỗi ký tự ngắn và khó nhớ, học sinh có thể sử dụng cụm mật khẩu dài gồm nhiều từ không liên quan trực tiếp đến thông tin cá nhân của mình. Có thể thêm số hoặc ký tự đặc biệt nếu dịch vụ yêu cầu. Cách này vừa giúp mật khẩu dài hơn, vừa dễ nhớ hơn so với một chuỗi ký tự ngẫu nhiên ngắn.

Thay vì dùng ngày sinh hay tên riêng dễ đoán, học sinh nên ghép một câu ngắn có ý nghĩa với bản thân, thêm số và ký tự đặc biệt. Ví dụ minh họa cách tạo (không nên dùng nguyên văn ví dụ này):

Ví dụ minh họa công thức đặt mật khẩu

Câu chuyện gốc: "Mẹ yêu học tập của con năm 2026"

Rút gọn + biến tấu: MeYeuHocT@p2026!

Nguyên tắc: tối thiểu 8 ký tự, có chữ hoa/thường, số và ký tự đặc biệt, không trùng với mật khẩu của tài khoản khác, không chứa tên, ngày sinh, số điện thoại của bản thân.

Khi đặt mật khẩu, học sinh nên nhớ ba điều: dài – riêng – không chứa thông tin dễ đoán và nên đầy đủ yếu tố: *chữ hoa/thường, số và ký tự đặc biệt*. Đối với các tài khoản quan trọng, nên ưu tiên mật khẩu từ khoảng 8 ký tự trở lên nếu dịch vụ cho phép. Quan trọng hơn, mỗi tài khoản nên có một mật khẩu riêng để nếu một tài khoản gặp sự cố, các tài khoản khác không bị ảnh hưởng theo.

Ghi nhớ: Một mật khẩu tốt không cần quá khó nhớ, nhưng phải đủ dài, khó đoán và không dùng lại cho nhiều tài khoản.

b. Các mức bảo vệ tài khoản

Mật khẩu chỉ là một phần của việc bảo vệ tài khoản. Mức độ an toàn sẽ tăng lên khi học sinh kết hợp mật khẩu tốt với các biện pháp xác thực bổ sung.

Bảng 2.4. Các mức độ bảo vệ tài khoản

Phương thức	Mức độ an toàn	Ưu điểm / hạn chế
Mật khẩu đơn giản, dễ đoán	Thấp	Dễ nhớ nhưng dễ bị dò hoặc bị lộ khi dịch vụ khác bị rò rỉ dữ liệu
Mật khẩu mạnh, riêng cho từng tài khoản	Trung bình – Cao	An toàn hơn nhiều nhưng khó nhớ nếu không dùng công cụ hỗ trợ
Mật khẩu mạnh + Xác thực 2 lớp (2FA)	Cao	Ngay cả khi lộ mật khẩu, kẻ xấu vẫn cần thêm mã xác thực thứ hai để đăng nhập
Mật khẩu mạnh + 2FA + Trình quản lý mật khẩu	Rất cao	Loại bỏ việc dùng chung/đoán mật khẩu; đòi hỏi thiết lập ban đầu và ghi nhớ mật khẩu chính

Bảng 2.4 chỉ thể hiện mức bảo vệ tương đối. Không có phương thức nào bảo đảm an toàn tuyệt đối. Người dùng vẫn cần cảnh giác với các trang đăng nhập giả, tin nhắn lừa đảo và yêu cầu cung cấp mã xác thực.

c. Kích hoạt xác thực 2 lớp (2FA)

Xác thực hai lớp, thường viết tắt là 2FA – Two-Factor Authentication, là cơ chế yêu cầu thêm một bước xác minh ngoài mật khẩu. Khi tính năng này được bật, người đăng nhập có thể phải xác nhận trên một thiết bị khác, nhập mã dùng một lần hoặc sử dụng ứng dụng xác thực.

Điều này tạo thêm một lớp bảo vệ. Nếu người khác biết được mật khẩu nhưng không có bước xác minh thứ hai, họ sẽ khó đăng nhập vào tài khoản hơn. Học sinh nên ưu tiên bật xác thực hai lớp cho những tài khoản quan trọng như email, mạng xã hội và các tài khoản có chứa nhiều thông tin cá nhân. Tùy nền tảng, mục này thường nằm trong phần Bảo mật, Đăng nhập và bảo mật, Xác minh hai bước hoặc Xác thực hai yếu tố.

Khi sử dụng 2FA, cần đặc biệt nhớ: mã xác thực cũng là thông tin bí mật. Không cung cấp mã OTP hoặc mã xác minh cho bất kỳ ai qua điện thoại, tin nhắn hoặc mạng xã hội, kể cả khi người đó tự xưng là nhân viên ngân hàng, nhà mạng, giáo viên hoặc cơ quan chức năng.

Nếu một người yêu cầu em đọc mã vừa nhận được trên điện thoại với lý do "xác minh tài khoản", "nhận thưởng" hoặc "hỗ trợ kỹ thuật", hãy dừng lại và kiểm tra qua kênh chính thức.

Ghi nhớ: Mật khẩu là lớp bảo vệ thứ nhất; xác thực hai lớp là lớp bảo vệ thứ hai. Mã OTP không được chia sẻ cho người khác.

Một số cách xác thực 2FA trên các nền tảng ứng dụng phổ biến:

- Google/Gmail: vào Quản lý Tài khoản Google → Bảo mật → Xác minh 2 bước, chọn nhận mã qua ứng dụng xác thực hoặc SMS.

- Zalo: vào Cài đặt → Tài khoản và bảo mật → Xác thực 2 lớp để yêu cầu nhập thêm mã khi đăng nhập trên thiết bị lạ.

- Ngay cả khi lộ mật khẩu, 2FA vẫn ngăn được phần lớn nguy cơ kẻ xấu đăng nhập trái phép vì thiếu mã xác thực thứ hai.

d. Sử dụng trình quản lý mật khẩu

Khi có nhiều tài khoản, việc nhớ một mật khẩu riêng cho từng tài khoản có thể trở nên khó khăn. Trình quản lý mật khẩu là công cụ giúp tạo, lưu và tự động điền mật khẩu theo cách được bảo vệ. Thay vì ghi mật khẩu vào giấy để ở nơi dễ nhìn, lưu trong tin nhắn hoặc sử dụng một mật khẩu cho tất cả tài khoản, học sinh THCS và THPT có thể sử dụng trình quản lý mật khẩu cùng sự hướng dẫn của cha mẹ hoặc người lớn tin cậy. Nhiều trình duyệt, điện thoại và ứng dụng hiện nay đã tích hợp sẵn chức năng quản lý mật khẩu. Khi sử dụng công cụ này, người dùng thường chỉ cần ghi nhớ một mật khẩu chính để mở kho mật khẩu. Mật khẩu chính cần đặc biệt mạnh và không được chia sẻ với người khác.

Một số công cụ quản lý mật khẩu có phiên bản miễn phí, chẳng hạn Bitwarden [3]. Bitwarden là một trình quản lý mật khẩu mã nguồn mở, có phiên bản miễn phí, giúp tạo mật khẩu ngẫu nhiên đủ mạnh cho từng tài khoản và lưu trữ có mã hóa, thay vì phải ghi nhớ hoặc dùng chung một mật khẩu cho nhiều nơi. Học sinh nên đặt một mật khẩu chính (master password) thật mạnh cho ứng dụng quản lý này và không chia sẻ với bất kỳ ai. Ngoài ra, trình duyệt và hệ điều hành cũng có các công cụ tích hợp sẵn. Việc lựa chọn công cụ nào nên dựa trên độ tuổi, thiết bị và sự hướng dẫn của gia đình. Tài liệu không yêu cầu học sinh phải sử dụng một sản phẩm cụ thể.

Ghi nhớ: Không cần nhớ hàng chục mật khẩu giống nhau. Hãy dùng mật khẩu riêng cho từng tài khoản và sử dụng công cụ hỗ trợ phù hợp khi cần.

2.2.2. Giao tiếp an toàn với người lạ

Internet giúp học sinh kết nối với nhiều người có cùng sở thích, cùng chơi game, học chung hoặc tham gia các cộng đồng trực tuyến. Tuy nhiên, một điểm khác biệt quan trọng giữa giao tiếp trực tiếp và giao tiếp trên mạng là chúng ta không phải lúc nào cũng biết chính xác người ở phía bên kia là ai.

Một người tự giới thiệu là "học sinh cùng tuổi", "bạn của bạn em" hoặc "người cùng sở thích" không có nghĩa thông tin đó chắc chắn đúng. Vì vậy, học sinh không cần nghi ngờ tất cả mọi người, nhưng cần biết giữ giới hạn an toàn khi trò chuyện với người chỉ quen qua mạng.

a. Nhận diện dấu hiệu bất thường

Trong những lần trò chuyện đầu tiên, học sinh nên thận trọng nếu một người mới quen có những biểu hiện bất thường như nhanh chóng tỏ ra quá thân thiết; liên tục khen ngợi, tặng quà ảo hoặc hứa cho tiền, vật phẩm trong game; hỏi nhiều thông tin về địa chỉ, trường học, gia đình hoặc lịch sinh hoạt; yêu cầu chuyển sang cuộc trò chuyện riêng; muốn em xóa tin nhắn hoặc giữ bí mật với cha mẹ và thầy cô.

Đặc biệt cần cảnh giác nếu người đó yêu cầu gửi ảnh riêng tư, bật camera trong hoàn cảnh không phù hợp, chuyển tiền, cung cấp mã xác thực hoặc hẹn gặp mà không muốn người lớn biết. Những dấu hiệu này chưa chắc đã chứng minh người đó có ý đồ xấu, nhưng đủ để em dừng lại và hỏi ý kiến một người lớn tin cậy.

Khi trò chuyện với người chỉ quen qua mạng, em không nên vội chia sẻ số điện thoại, địa chỉ nhà, trường lớp, lịch trình hoặc những thông tin riêng tư khác. Nếu muốn gặp một người quen qua mạng ngoài đời thực, cần trao đổi trước với cha mẹ hoặc người lớn tin cậy và chỉ thực hiện trong điều kiện an toàn.

Một nguyên tắc rất quan trọng là: nếu một người cố yêu cầu em giấu cha mẹ hoặc thầy cô những việc liên quan đến tiền, ảnh riêng tư, gặp mặt hoặc điều khiển em sợ hãi, đó là dấu hiệu cần dừng liên lạc.

> **Ghi nhớ:**
>
> Không có lý do chính đáng nào để một người quen qua mạng yêu cầu giữ bí mật cuộc trò chuyện với cha mẹ.
>
> Cảm thấy áy náy, sợ hãi hoặc bối rối khi trò chuyện là dấu hiệu cần dừng lại và nói với người lớn ngay, kể cả khi đã trót chia sẻ điều gì đó.

Người đáng tin sẽ tôn trọng giới hạn của em và không ép em giữ bí mật về điều khiến em cảm thấy bất an.

b. Hành vi trên mạng và vi phạm pháp luật

Một số hành vi trên mạng không chỉ là cách cư xử không phù hợp mà còn có thể vi phạm pháp luật. Pháp luật nghiêm cấm việc dụ dỗ, ép buộc, đe dọa hoặc lợi dụng trẻ em để thực hiện những hành vi xâm hại. Những hành vi này có thể xảy ra trực tiếp hoặc thông qua mạng xã hội, ứng dụng nhắn tin, trò chơi trực tuyến và các nền tảng khác.

Đối với học sinh, điều quan trọng không phải là ghi nhớ tên tội danh hoặc mức hình phạt, mà là nhận ra rằng nếu một người yêu cầu em gửi hình ảnh riêng tư, giữ bí mật một mối quan hệ, làm điều khiến em khó chịu hoặc đe dọa sẽ phát tán thông tin nếu em không làm theo, em có quyền dừng lại và tìm kiếm sự giúp đỡ.

Ngay cả khi em đã trót gửi một thông tin, hình ảnh hoặc đồng ý làm điều gì đó, em vẫn nên nói với người lớn tin cậy. Việc tiếp tục im lặng vì sợ bị trách mắng có thể khiến người gây hại có thêm cơ hội gây áp lực. Cha mẹ, giáo viên và người chăm sóc khi nhận được chia sẻ của học sinh cần ưu tiên bảo vệ các em, lắng nghe và hỗ trợ xử lý sự việc thay vì vội trách lỗi.

c. Tình huống thực tế liên quan

Tình huống: Một người quen qua game muốn chuyển sang nhắn tin riêng

Một học sinh chơi game trực tuyến và thường xuyên trò chuyện với một tài khoản tự giới thiệu là học sinh cùng tuổi. Sau vài tuần, người này nói rằng hai người đã "rất thân", đề nghị chuyển sang một ứng dụng nhắn tin riêng và yêu cầu học sinh không nói với cha mẹ vì "người lớn sẽ không hiểu".

Sau đó, người này hỏi tên trường, khu vực đang sống và đề nghị gửi một bức ảnh cá nhân để "chứng minh là bạn thật". Khi học sinh từ chối, người này tỏ ra giận dữ và nói rằng nếu thật sự coi nhau là bạn thì không nên giấu.

Trong tình huống này, điều đáng chú ý không phải là việc người kia có chắc chắn là người xấu hay không, mà là cách họ đang cố gây áp lực để học sinh vượt qua giới hạn an toàn. Những yêu cầu giữ bí mật, cung cấp thông tin riêng tư và dùng cảm xúc để ép buộc đều là dấu hiệu cần cảnh giác.

Cách xử lý phù hợp là dừng việc cung cấp thêm thông tin, lưu lại những tin nhắn cần thiết, nói với cha mẹ hoặc người lớn tin cậy và sử dụng chức năng Chặn hoặc Báo cáo nếu cần.

Bài học: Không cần chứng minh mình là "người bạn tốt" bằng cách chia sẻ thông tin hoặc làm điều khiến bản thân không thoải mái.

d. Sử dụng chức năng Báo cáo và Chặn

Hầu hết các mạng xã hội, ứng dụng trò chuyện và trò chơi trực tuyến đều cung cấp chức năng Báo cáo (Report) và Chặn (Block). Đây là những công cụ giúp người dùng tự bảo vệ mình khi gặp tài khoản có hành vi quấy rối, đe dọa, giả mạo hoặc gửi nội dung không phù hợp.

Khi gặp tài khoản đáng ngờ, học sinh không cần tranh cãi hoặc cố tự "điều tra" người đó. Nếu việc lưu bằng chứng không làm tăng nguy hiểm, hãy chụp màn hình những nội dung quan trọng hoặc ghi lại tên tài khoản, đường liên kết và thời gian xảy ra sự việc. Sau đó, có thể sử dụng chức năng Báo cáo và Chặn.

Việc Báo cáo giúp nền tảng biết rằng tài khoản hoặc nội dung có thể vi phạm quy tắc cộng đồng. Chặn giúp hạn chế người đó tiếp tục liên hệ với em. Tuy nhiên, với các trường hợp nghiêm trọng như đe dọa, tống tiền, giả mạo, phát tán thông tin riêng tư hoặc nghi ngờ có hành vi xâm hại trẻ em, chỉ bấm Báo cáo là chưa đủ. Học sinh cần nói ngay với người lớn tin cậy để được hỗ trợ.

Không nên tiếp tục nhắn tin chỉ để "thu thập thêm bằng chứng", cũng không nên tự hẹn gặp người đó để xác minh danh tính.

Ghi nhớ: Lưu bằng chứng khi an toàn – Báo cáo – Chặn – Nói với người lớn.

2.2.3. Cập nhật phần mềm và nhận diện lừa đảo

Thiết bị an toàn và thói quen sử dụng cẩn trọng luôn đi cùng nhau. Một chiếc điện thoại đã cài phần mềm bảo vệ vẫn có thể gặp rủi ro nếu người dùng mở tệp không rõ nguồn hoặc đưa mật khẩu cho trang giả mạo. Ngược lại, người dùng rất cẩn thận vẫn có thể gặp nguy hiểm nếu thiết bị đã lâu không được cập nhật và còn tồn tại lỗ hổng bảo mật.

Vì vậy, học sinh cần thực hiện đồng thời hai việc: giữ thiết bị được cập nhật và biết nhận diện những yêu cầu đáng ngờ.

a. Luôn cập nhật hệ điều hành và ứng dụng

Các bản cập nhật của điện thoại, máy tính, trình duyệt hoặc ứng dụng không chỉ mang đến giao diện và tính năng mới. Một vai trò rất quan trọng của chúng là sửa các lỗi bảo mật có thể bị người xấu lợi dụng.

Học sinh nên bật chế độ cập nhật tự động nếu thiết bị cho phép. Khi hệ điều hành hoặc ứng dụng thông báo có bản cập nhật bảo mật, không nên trì hoãn quá lâu. Những ứng dụng không còn sử dụng cũng nên được gỡ bỏ để giảm nguy cơ từ phần mềm cũ hoặc không còn được hỗ trợ.

Phần mềm độc hại có nhiều dạng. Có loại cố đánh cắp mật khẩu, có loại theo dõi hoạt động trên thiết bị, có loại khóa hoặc làm hỏng dữ liệu. Học sinh không cần ghi nhớ toàn bộ các tên kỹ thuật này. Quan trọng hơn là hình thành một số thói quen: chỉ cài ứng dụng từ nguồn đáng tin cậy; không tải các bản "crack", "mod", phần mềm nhận quà hoặc vật phẩm miễn phí từ trang lạ; không mở tệp không rõ người gửi; và thường xuyên cập nhật thiết bị.

Nếu điện thoại hoặc máy tính đột nhiên xuất hiện ứng dụng lạ, hoạt động bất thường, tự mở quảng cáo, nóng máy hoặc tiêu thụ dữ liệu nhiều bất thường, học sinh nên nói với cha mẹ hoặc người có kiến thức kỹ thuật để kiểm tra thay vì tự cài thêm nhiều ứng dụng "diệt virus" từ nguồn không rõ.

Ghi nhớ: Cập nhật đều đặn – chỉ cài ứng dụng đáng tin – không tải phần mềm lạ để nhận quà hoặc mở khóa tính năng.

b. Nhận diện tin nhắn, cuộc gọi lừa đảo

Lừa đảo giả mạo, thường được gọi là phishing, là hình thức trong đó người xấu giả danh một tổ chức hoặc người đáng tin để khiến người dùng bấm vào đường liên kết, cung cấp thông tin hoặc chuyển tiền.

Đối tượng giả mạo có thể tự xưng là giáo viên, nhà trường, ngân hàng, nhà mạng, cơ quan nhà nước, đơn vị tổ chức cuộc thi hoặc thậm chí là người thân. Nội dung thường tạo ra hai loại cảm xúc: quá lo sợ hoặc quá vui mừng. Ví dụ: "Tài khoản của em sắp bị khóa", "Hồ sơ thi đang có lỗi", "Em vừa nhận được học bổng", "Em trúng phần thưởng", "Người thân đang gặp việc khẩn cấp".

Sau đó, người nhận thường bị thúc giục phải hành động ngay: bấm vào liên kết, quét mã QR, tải ứng dụng, cung cấp mật khẩu, mã OTP hoặc chuyển tiền.

Có thể nhận diện một thông điệp đáng ngờ qua một số dấu hiệu: tạo cảm giác quá gấp gáp; yêu cầu giữ bí mật; đường liên kết có tên miền lạ hoặc gần giống tên thật; yêu cầu cung cấp mật khẩu hoặc OTP; yêu cầu cài ứng dụng từ bên ngoài kho ứng dụng; hoặc thông tin không xuất hiện trên kênh chính thức.

Ví dụ minh họa: tin nhắn giả mạo "Giải thưởng học sinh giỏi"

Một học sinh nhận được tin nhắn:

"Chúc mừng em đạt giải Học sinh giỏi cấp Thành phố. Bấm vào đường liên kết dưới đây để nhận phần thưởng trước 18 giờ hôm nay."

Tin nhắn không đến từ tài khoản chính thức của trường. Khi mở trang liên kết, hệ thống yêu cầu nhập tài khoản, mật khẩu và mã OTP để "xác nhận người nhận".

Trong trường hợp này, học sinh không nên tiếp tục thao tác. Hãy kiểm tra thông tin với giáo viên chủ nhiệm hoặc thông báo chính thức của nhà trường. Nếu đã nhập mật khẩu hoặc OTP, cần nói ngay với cha mẹ hoặc người lớn tin cậy, đổi mật khẩu và kiểm tra tài khoản.

Một nguyên tắc rất dễ nhớ là:

DỪNG – KIỂM TRA – XÁC MINH

Dừng: Không bấm vội vào liên kết, quét mã QR hoặc làm theo yêu cầu khẩn cấp.

Kiểm tra: Xem người gửi, địa chỉ trang web, nội dung và yêu cầu có bất thường không.

Xác minh: Liên hệ lại với nhà trường, ngân hàng, người thân hoặc đơn vị liên quan qua kênh chính thức mà em đã biết từ trước.

Đặc biệt, không cung cấp mật khẩu hoặc mã OTP cho bất kỳ ai qua điện thoại, tin nhắn hoặc mạng xã hội.

2.3. Trách nhiệm phối hợp Gia đình – Nhà trường – Học sinh

Sử dụng mạng an toàn không phải là trách nhiệm của riêng học sinh. Một học sinh dù đã được trang bị nhiều kỹ năng vẫn có thể gặp tình huống vượt quá khả năng tự xử lý. Vì vậy, cần có sự phối hợp giữa học sinh, gia đình, nhà trường, cơ quan quản lý và doanh nghiệp cung cấp dịch vụ mạng. Theo Điều 34 Nghị định 56/2017/NĐ-CP, cơ quan quản lý nhà nước, tổ chức hoạt động vì trẻ em, nhà trường và gia đình đều có trách nhiệm cụ thể trong việc truyền thông nâng cao nhận thức, phổ biến kỹ năng cho cả trẻ em lẫn người chăm sóc. Bảng dưới đây phân chia trách nhiệm thực hành cụ thể theo từng chủ thể, giúp việc triển khai tài liệu và infographic đạt hiệu quả cao hơn khi có sự phối hợp đồng bộ:

Bảng 2.5. Trách nhiệm của các chủ thể

Chủ thể	Trách nhiệm chính
Học sinh	Thực hiện các nguyên tắc sử dụng mạng an toàn; bảo vệ tài khoản và thông tin cá nhân; kiểm tra trước khi bấm, tải hoặc chia sẻ; không tham gia bắt nạt, phát tán tin giả hoặc nội dung gây tổn thương người khác; báo sớm cho cha mẹ, thầy cô hoặc người lớn tin cậy khi gặp tình huống bất thường; không cố tự giải quyết những sự cố nghiêm trọng.
Gia đình	Thường xuyên trao đổi với con về hoạt động trên mạng theo cách phù hợp với độ tuổi; cùng con thiết lập quyền riêng tư, thời gian sử dụng thiết bị và những nguyên tắc trong gia đình; hướng dẫn con nhận biết lừa đảo, nội dung xấu và người lạ trên mạng; lắng nghe khi con gặp sự cố, tránh trách mắng hoặc cấm đoán ngay; phối hợp với nhà trường khi vấn đề liên quan đến bạn học, nhóm lớp hoặc ảnh hưởng đến việc học và tâm lý của học sinh.
Giáo viên chủ nhiệm	Là một trong những đầu mối gần gũi để học sinh có thể phản ánh sự cố; thường xuyên nhắc lại các nguyên tắc sử dụng mạng an toàn trong sinh hoạt lớp; nắm bắt những vấn đề phát sinh trong nhóm lớp và quan hệ giữa học sinh trên môi trường mạng; tiếp nhận thông tin kín đáo, không công khai sự việc trước tập thể; phối hợp với gia đình, giáo viên bộ môn và nhà trường; tiếp tục hỏi thăm, hỗ trợ học sinh sau sự cố khi cần.
Giáo viên Tin học	Trang bị và cho học sinh thực hành các kỹ năng cụ thể như tạo và bảo vệ tài khoản, mật khẩu và xác thực nhiều lớp; cài đặt quyền riêng tư; nhận biết phishing, mã độc và website giả; sử dụng chức năng Block/Report; kiểm tra nguồn thông tin; sử dụng AI và các công cụ số an toàn. Nên sử dụng tình huống, bài tập thực hành và infographic thay vì chỉ giải thích lý thuyết.
Giáo viên GDCD/Giáo dục kinh tế và pháp luật	Giúp học sinh hiểu quyền và trách nhiệm khi tham gia môi trường số; tôn trọng quyền riêng tư, danh dự và dữ liệu của người khác; nhận biết hành vi bắt nạt, giả mạo, phát tán thông tin sai hoặc nội dung riêng tư; hiểu trách nhiệm đối với nội dung mình đăng, bình luận và chia sẻ; hình thành cách ứng xử có văn hóa và biết tìm đến các kênh hỗ trợ phù hợp.
Nhà trường/Ban giám hiệu	Xây dựng quy định sử dụng Internet, thiết bị và AI phù hợp; công bố rõ đầu mối tiếp nhận phản ánh; tổ chức kênh phản ánh kín đáo, bảo vệ danh tính và quyền riêng tư của học sinh; phối hợp gia đình và cơ quan có trách nhiệm khi xảy ra sự cố; tổ chức tuyên truyền, tập huấn và cập nhật học liệu; theo dõi, hỗ trợ học sinh sau những sự cố nghiêm trọng.

Hình 2.3 dưới đây mô tả về trách nhiệm phối hợp giữa gia đình, nhà trường và học sinh theo các cấp học. Ở cấp độ tiểu học, học sinh còn nhỏ nên gia đình và nhà trường giữ vai trò hướng dẫn, thiết lập giới hạn và hỗ trợ trực tiếp nhiều hơn. Ở cấp THCS, học sinh bắt đầu sử dụng mạng độc lập hơn, vì vậy cần vừa tăng cường kỹ năng tự bảo vệ, vừa duy trì sự giám sát và trao đổi thường xuyên giữa gia đình với nhà trường. Đối với cấp THPT, học sinh cần được trao quyền tự chủ cao hơn, biết tự đánh giá rủi ro, chịu trách nhiệm đối với hành vi trên mạng và chủ động tìm kiếm sự hỗ trợ khi cần; gia đình và nhà trường chuyển dần từ "kiểm soát" sang đồng hành, tư vấn và hỗ trợ. Vì vậy, trách

nhiệm của ba bên cần được xác định theo từng cấp học, phù hợp với độ tuổi, mức độ tự chủ và những rủi ro mà học sinh có thể gặp trên môi trường mạng.



Hình 2.3. Trách nhiệm giữa gia đình, nhà trường và học sinh

2.4. Bảng tự đánh giá kỹ năng sử dụng mạng an toàn

Công cụ tự kiểm tra nhanh dưới đây giúp học sinh (có thể cùng giáo viên hoặc cha mẹ) rà soát mức độ thực hành các nguyên tắc đã nêu trong chương, từ đó xác định nội dung nào cần được nhắc lại hoặc thực hành thêm:

Bảng 2.6. Bảng đánh giá kỹ năng sử dụng mạng an toàn

Nội dung tự đánh giá	Có	Chưa
A. Dành cho học sinh Tiểu học		
Em chỉ sử dụng ứng dụng, trò chơi hoặc tài khoản trực tuyến khi được cha mẹ, thầy cô hoặc người lớn tin cậy cho phép và hướng dẫn.	☐	☐
Em không cung cấp tên đầy đủ, địa chỉ nhà, số điện thoại, tên trường/lớp hoặc hình ảnh riêng tư cho người lạ trên mạng.	☐	☐
Em biết hỏi cha mẹ hoặc thầy cô trước khi bấm vào đường liên kết lạ, tải tệp hoặc cài ứng dụng mới.	☐	☐
Em không nhắn tin riêng hoặc hẹn gặp người chỉ quen qua mạng.	☐	☐
Em biết sử dụng quy tắc *"Dừng – Nghĩ – Kiểm tra"* khi gặp nội dung lạ hoặc đáng ngờ.	☐	☐

Em biết dừng lại và nói với cha mẹ, thầy cô hoặc người lớn tin cậy khi có nội dung trên mạng khiến em sợ hãi, khó chịu hoặc bị ép buộc.	☐	☐
Em biết không chia sẻ mật khẩu hoặc mã xác thực cho người khác.	☐	☐
Em biết không đăng hoặc chuyển tiếp hình ảnh, video của bạn bè khi chưa được đồng ý.	☐	☐
Em có thực hiện thời gian sử dụng thiết bị theo quy định của gia đình và nhà trường.	☐	☐
Thiết bị (điện thoại/máy tính) của em luôn được cập nhật phần mềm mới nhất.	☐	☐
B. Dành cho học sinh THCS/THPT		
Tài khoản Zalo/TikTok/Facebook của em đã ở chế độ riêng tư.	☐	☐
Em không đăng ảnh có tên trường, lớp hoặc địa chỉ nhà rõ ràng.	☐	☐
Em đã đặt mật khẩu mạnh, khác nhau cho từng tài khoản.	☐	☐
Em đã bật xác thực 2 yếu tố (2FA) cho tài khoản email/mạng xã hội chính.	☐	☐
Em biết cách sử dụng nút Report/Block khi gặp tài khoản đáng ngờ.	☐	☐
Em không nhắn tin riêng hoặc hẹn gặp người chỉ quen qua mạng.	☐	☐
Em áp dụng quy tắc "Dừng – Nghĩ – Kiểm tra" trước khi chia sẻ tin.	☐	☐
Em có theo dõi thời gian sử dụng mạng xã hội hằng ngày của bản thân.	☐	☐
Thiết bị (điện thoại/máy tính) của em luôn được cập nhật phần mềm mới nhất.	☐	☐
Em biết mình nên nói với ai (cha mẹ, thầy cô) khi gặp vấn đề trên mạng.	☐	☐

Gợi ý sử dụng: nếu học sinh đánh dấu "Chưa" từ 3 mục trở lên, giáo viên/phụ huynh nên dành thời gian ôn lại trực tiếp các mục tương ứng trong Chương 2, thay vì chỉ phát tài liệu và infographic để học sinh tự đọc.

2.5. Kết luận chương

Sử dụng Internet an toàn không chỉ phụ thuộc vào các công cụ bảo mật hay thiết lập kỹ thuật, mà quan trọng hơn là hình thành ở học sinh nhận thức đúng, thói quen tốt và khả năng tự bảo vệ trong từng tình huống cụ thể. Những nguyên tắc được trình bày trong chương này cho thấy an toàn trên môi trường mạng bắt đầu từ những hành động rất gần gũi: suy nghĩ trước khi đăng và chia sẻ, bảo vệ thông tin cá nhân, kiểm chứng thông tin trước khi tin hoặc hành động, tôn trọng người khác, chủ động tìm kiếm sự hỗ trợ và duy trì việc sử dụng Internet cân bằng, lành mạnh, có mục đích.

Bên cạnh nhận thức, học sinh cần chuyển các nguyên tắc thành những kỹ năng thực hành thường xuyên như sử dụng mật khẩu mạnh và riêng biệt, bật xác thực hai lớp, bảo vệ mã OTP, cập nhật thiết bị, nhận diện dấu hiệu lừa đảo, thận trọng khi giao tiếp với người chỉ quen qua mạng, đồng thời biết sử dụng chức năng Báo cáo và Chặn khi cần thiết. Các quy tắc đơn giản như "Dừng – Nghĩ – Kiểm tra" hay "Dừng – Kiểm tra – Xác minh" có thể trở thành phản xạ quan trọng giúp học sinh tránh những quyết định vội vàng trước thông tin, đường liên kết hoặc yêu cầu đáng ngờ.

Tuy nhiên, trách nhiệm bảo đảm an toàn mạng không thể đặt hoàn toàn lên học sinh. Gia đình cần đồng hành và tạo môi trường để các em sẵn sàng chia sẻ; nhà trường cần thường xuyên giáo dục kỹ năng số và có quy trình hỗ trợ khi xảy ra sự cố; các cơ quan quản lý và nền tảng trực tuyến cần duy trì cơ chế bảo vệ, cảnh báo và tiếp nhận phản ánh. Khi học sinh có kiến thức, kỹ năng và điểm tựa hỗ trợ phù hợp, Internet sẽ trở thành một môi trường học tập, giao tiếp và sáng tạo tích cực hơn thay vì là nguồn phát sinh những rủi ro khó kiểm soát.

CHƯƠNG 3. CÁC RỦI RO PHỔ BIẾN KHI THAM GIA MÔI TRƯỜNG MẠNG

Chương 3 giúp các em hiểu rõ hơn những rủi ro có thể gặp, dấu hiệu nhận biết và hậu quả có thể xảy ra. Hiểu đúng về rủi ro không nhằm làm học sinh lo sợ khi sử dụng Internet, mà giúp các em chủ động nhận biết tình huống bất thường, biết dừng lại đúng lúc và lựa chọn cách xử lý phù hợp.

Để nhận diện rủi ro trực tuyến một cách có hệ thống, các nghiên cứu quốc tế thường sử dụng khung 4C, gồm: rủi ro về nội dung (Content) khi trẻ tiếp xúc với nội dung có khả năng gây hại; rủi ro về tiếp xúc (Contact) khi trẻ bị người khác tiếp cận với mục đích không phù hợp; rủi ro về hành vi (Conduct) khi trẻ tham gia, chứng kiến hoặc trở thành người bị ảnh hưởng bởi hành vi có hại trên mạng; và rủi ro về hợp đồng, thương mại (Contract) như lừa đảo, khai thác dữ liệu hoặc giao dịch không phù hợp. Khung 4C được Sonia Livingstone và Mariya Stoilova phát triển trong dự án CO:RE – Children Online: Research and Evidence [4].

Để thuận tiện cho học sinh theo dõi, chương này tổ chức các nguy cơ thường gặp thành ba nhóm gần với thực tế sử dụng Internet: rủi ro kỹ thuật và phần mềm độc hại; rủi ro xã hội – tâm lý; và rủi ro sức khỏe – phát triển. Các nhóm này không hoàn toàn tách biệt mà có thể xuất hiện đồng thời trong một tình huống.

Thông qua các tình huống và minh họa trong chương, học sinh cần hình thành một phản xạ quan trọng: Nhận biết dấu hiệu bất thường: **Dừng lại – Kiểm tra – Tìm sự hỗ trợ khi cần**.

3.1. Rủi ro kỹ thuật và phần mềm độc hại

Nhóm rủi ro này liên quan trực tiếp đến công nghệ và có thể gây thiệt hại về dữ liệu, tài khoản và tài chính cho học sinh cũng như gia đình. Ba dạng rủi ro phổ biến gồm lừa đảo qua tin nhắn, mã độc từ trò chơi hoặc ứng dụng và giả mạo bằng trí tuệ nhân tạo. Dù sử dụng những kỹ thuật khác nhau, các thủ đoạn này thường đồng thời khai thác điểm yếu của thiết bị và sự mất cảnh giác của người dùng.

Các đối tượng thường giả mạo một cá nhân hoặc tổ chức đáng tin cậy, chẳng hạn như người thân, nhà trường hoặc ngân hàng. Sau đó, chúng tạo ra tình huống khẩn cấp hoặc giới hạn thời gian để thúc ép nạn nhân hành động ngay mà chưa kịp kiểm chứng. Vì vậy, thay vì chỉ ghi nhớ từng dấu hiệu riêng lẻ, học sinh cần nhận ra đặc điểm chung của các thủ đoạn này: *giả mạo danh tính, tạo áp lực, thúc ép hành động*. Khi gặp tình huống có những dấu hiệu trên, học sinh cần bình tĩnh, dừng lại và xác minh thông tin

qua một kênh đáng tin cậy trước khi thực hiện bất kỳ yêu cầu nào. Ba nhóm rủi ro dưới đây là những tình huống học sinh có thể thường gặp.

3.1.1. Phishing và Smishing tinh vi

Phishing là hình thức giả mạo email, website hoặc đường liên kết để đánh cắp thông tin cá nhân, thông tin đăng nhập hoặc dụ người dùng thực hiện hành động có lợi cho kẻ lừa đảo. Smishing là phishing được thực hiện qua SMS hoặc ứng dụng nhắn tin như Zalo, Messenger.

Các thủ đoạn này thường không tấn công trực tiếp vào hệ thống bảo mật mà lợi dụng tâm lý của người dùng. Đối tượng lừa đảo thường:

- Mạo danh người hoặc tổ chức đáng tin cậy như giáo viên, nhà trường, ngân hàng.

- Đưa ra thông báo bất ngờ hoặc tạo cảm giác khẩn cấp.

- Yêu cầu người nhận bấm vào liên kết, quét mã QR, đăng nhập hoặc cung cấp thông tin bảo mật.

Trong thời gian thi cử và tuyển sinh, học sinh có thể nhận được thông báo giả như:

“Đã có điểm thi, bấm vào đây để xem ngay” hoặc

“Hồ sơ của bạn có lỗi, cần cập nhật gấp”.

Đường liên kết có thể dẫn đến một website được thiết kế gần giống trang chính thức nhằm lấy mật khẩu, mã OTP hoặc thông tin cá nhân. Vì vậy, cơ quan chức năng thường khuyến cáo học sinh và cha mẹ chỉ tra cứu điểm thi, kết quả tuyển sinh qua hệ thống chính thức của Bộ Giáo dục và Đào tạo, Sở Giáo dục và Đào tạo hoặc nhà trường [5], [6], [7].

Hình 3.1 minh họa một kịch bản giả mạo kết quả thi học kỳ qua các kênh mạng xã hội như Zalo/Facebook: một tài khoản hoặc trang thông tin mạo danh nhà trường gửi thông báo “Đã có kết quả thi, hãy bấm vào đường link để xem điểm”, sau đó dẫn tới một website yêu cầu đăng nhập tài khoản hoặc cung cấp thông tin cá nhân. Nếu người nhận đăng nhập hoặc cung cấp thông tin theo đường link được gửi đến thì thông tin cá nhân của họ sẽ bị thu thập bất hợp pháp và có thể được sử dụng để lấy tài sản, vi phạm pháp luật hoặc mạo danh trong các tình huống lừa đảo khác.



Hình 3.1. Sơ đồ kịch bản giả mạo "kết quả thi học kỳ" lan truyền qua Zalo/Facebook

Thủ đoạn tương tự cũng xuất hiện trong lĩnh vực ngân hàng, chẳng hạn thông báo giả về điểm thưởng sắp hết hạn hoặc tài khoản đang gặp sự cố. Dù nội dung khác nhau, các thông báo lừa đảo thường có chung một cách thức: *mạo danh, tạo áp lực, thúc giục hành động.*

Khi nhận được thông báo đáng ngờ, học sinh cần:

- Không vội bấm vào liên kết, quét mã QR hoặc tải tệp đính kèm.

- Không cung cấp mật khẩu, mã OTP và thông tin cá nhân.

- Tự truy cập website hoặc ứng dụng chính thức để kiểm tra.

- Liên hệ với giáo viên, nhà trường hoặc người lớn tin cậy qua số điện thoại đã biết trước.

- Báo cáo và chặn tài khoản gửi thông tin giả mạo.

Ghi nhớ: Một thông báo càng thúc giục "xem ngay", "xử lý ngay", "sắp hết hạn" hoặc yêu cầu cung cấp mật khẩu, mã OTP hay thông tin cá nhân thì càng cần **Dừng lại – Kiểm tra nguồn – Xác minh** qua kênh chính thức.

Hình 3.2 minh họa ví dụ tình huống có thể xảy ra khi học sinh bị lừa đảo, tình huống này có thể dành cho bất cứ học sinh dù ở cấp độ nào. Tình huống cụ thể như sau:

Tình huống: *"Hồ sơ dự thi của em có lỗi. Bấm vào đây và đăng nhập trong 10 phút."*

- Tiểu học: Không bấm. Đưa điện thoại cho cha mẹ hoặc thầy cô.

- THCS: Không bấm, không nhập mật khẩu. Tự mở trang chính thức để kiểm tra.

- THPT: Kiểm tra tên miền, người gửi và kênh chính thức. Lưu bằng chứng và báo cáo nếu xác định là giả mạo.



Hình 3.2. Minh họa lừa đảo/phishing và cách đối phó

3.1.2. Malware từ game và ứng dụng crack

Mã độc (malware) là phần mềm được tạo ra nhằm gây hại cho thiết bị hoặc người dùng, chẳng hạn như đánh cắp thông tin, chiếm quyền tài khoản, theo dõi hoạt động, tự hiển thị quảng cáo hoặc điều khiển thiết bị trái phép.

Học sinh có thể vô tình cài mã độc khi tải game, ứng dụng hoặc tệp từ những nguồn không đáng tin cậy. Những bản game "mod", "hack", "cheat", ứng dụng "crack" hoặc chương trình hứa mở khóa tính năng trả phí có thể đã bị thay đổi và cài thêm phần mềm độc hại. Để hiểu rõ về các chế độ "mod", "hack", "cheat", các em có thể tham khảo Bảng 3.1 dưới đây:

Bảng 3.1. Phân loại các chế độ trong khi cài đặt trò chơi

Thuật ngữ	Hiểu đơn giản	Ví dụ	Điều cần lưu ý
Game mod *(modified game)*	Phiên bản trò chơi đã được chỉnh sửa so với bản gốc. Có thể thay đổi hình ảnh, nhân vật, bản đồ, tính năng hoặc cách chơi.	Một bản mod thay giao diện hoặc thêm bản đồ mới.	Mod không phải lúc nào cũng xấu. Một số trò chơi cho phép mod chính thức. Tuy nhiên, bản mod tải từ nguồn không rõ có thể chứa mã độc hoặc yêu cầu quyền truy cập nguy hiểm.
Game hack	Trong ngữ cảnh trò chơi, thường chỉ việc can thiệp trái phép vào game hoặc tài khoản để thay đổi kết quả, vượt qua giới hạn hoặc có được lợi thế không được nhà phát hành cho phép.	Can thiệp để có vật phẩm, tiền ảo hoặc khả năng đặc biệt không đúng quy định của game.	Có thể vi phạm điều khoản sử dụng, dẫn đến khóa tài khoản; các công cụ được quảng cáo là "hack game" cũng có thể chứa mã độc hoặc đánh cắp tài khoản.
Cheat	Gian lận trong trò chơi bằng mã, công cụ hoặc cách thức tạo lợi thế không công bằng so với người chơi khác.	Công cụ giúp nhìn thấy thông tin mà người chơi bình thường không thấy hoặc tự động thực hiện một số thao tác.	Có thể làm mất công bằng, vi phạm quy định của trò chơi và khiến tài khoản bị xử lý.

Một số lời mời thường được dùng để thu hút học sinh là:

- Tặng vật phẩm miễn phí.

- Nhận tiền ảo miễn phí.

- Hack game.

- Mở khóa toàn bộ tính năng.

- Cày thuê nhanh.

- Tải bản trả phí miễn phí.

Ngoài mã độc, học sinh còn có thể gặp trang web giả yêu cầu nhập tài khoản game, người lạ yêu cầu cài ứng dụng điều khiển thiết bị từ xa hoặc quảng cáo dụ thanh toán để nhận quà.

Dấu hiệu cần chú ý: Hãy cẩn thận khi:

- Ứng dụng không có trên kho ứng dụng chính thức.

- Tệp được gửi qua nhóm chat, mạng xã hội hoặc trang web lạ.

- Ứng dụng yêu cầu những quyền không liên quan đến chức năng của nó.

- Một trang web yêu cầu nhập mật khẩu game để nhận quà.

- Người lạ yêu cầu cài thêm phần mềm để "hỗ trợ" hoặc "cày thuê".

- Một lời mời hứa cho vật phẩm hoặc tính năng có giá trị hoàn toàn miễn phí.

Để sử dụng game và ứng dụng an toàn

- Chỉ tải ứng dụng từ kho ứng dụng hoặc trang chính thức của nhà phát hành.

- Không cài tệp không rõ nguồn gốc.

- Không sử dụng bản "crack", "hack", "cheat" hoặc "mod" không đáng tin cậy.

- Không nhập mật khẩu vào trang web hứa tặng quà hoặc vật phẩm.

- Kiểm tra quyền truy cập trước khi cho phép ứng dụng sử dụng ảnh, camera, micro, danh bạ hoặc vị trí.

- Không cài ứng dụng điều khiển từ xa theo yêu cầu của người lạ trên mạng.

- Không tự ý thanh toán trong game; với học sinh nhỏ, cần trao đổi với cha mẹ hoặc người lớn phụ trách.

Nếu sau khi cài một ứng dụng mà điện thoại hoặc máy tính hoạt động bất thường, xuất hiện nhiều quảng cáo lạ, tài khoản có đăng nhập không rõ nguồn gốc hoặc ứng dụng tự mở, hãy dừng sử dụng và báo cho người lớn để kiểm tra.

Tình huống điển hình về rủi ro này có thể được minh họa như sau: bạn bè gửi file "nhận kim cương miễn phí" và nói đã thử thành công.

- Tiểu học: Không tải ứng dụng nếu cha mẹ/thầy cô chưa cho phép.

- THCS: Không tải tệp ngoài nguồn chính thức, không cấp quyền lạ.

- THPT: Ngoài các bước trên, cần hiểu rằng crack/mod không rõ nguồn có thể gây mất tài khoản, dữ liệu và ảnh hưởng cả thiết bị dùng chung của gia đình.

Điều cần nhớ: *"Miễn phí"* không có nghĩa là an toàn**.** Một món quà trong game không đáng để đổi lấy tài khoản, thông tin cá nhân hoặc quyền kiểm soát thiết bị.

3.1.3. Deepfake và AI lừa đảo

Deepfake là hình ảnh, video hoặc âm thanh được tạo ra hoặc chỉnh sửa bằng trí tuệ nhân tạo để mô phỏng khuôn mặt, giọng nói hay hành động của một người có thật.

Deepfake có thể được sử dụng trong giải trí, giáo dục nhưng cũng có thể bị lợi dụng để giả mạo, lừa đảo hoặc gây tổn hại cho người khác.

Một thủ đoạn phổ biến là chiếm quyền hoặc tạo tài khoản mạng xã hội giả mạo người quen, sau đó nhắn tin hỏi vay tiền hoặc yêu cầu chuyển tiền gấp. Để tăng độ tin cậy, kẻ lừa đảo có thể gửi đoạn ghi âm, video giả hoặc thực hiện cuộc gọi ngắn có hình ảnh và giọng nói giống người bị mạo danh. Chúng thường viện lý do mạng yếu, hình ảnh mờ hoặc âm thanh chập chờn để che giấu dấu hiệu bất thường.



Hình 3.3. Kịch bản cuộc gọi deepfake giả giọng người thân, bạn bè để vay tiền gấp

Học sinh cũng có thể gặp tình huống tương tự: một tài khoản có tên và ảnh đại diện giống bạn cùng lớp nhắn tin mượn tiền, kèm theo đoạn ghi âm hoặc video ngắn. Tài khoản thật của người bạn có thể đã bị chiếm quyền hoặc hình ảnh, giọng nói của bạn đã bị làm giả từ những nội dung được đăng công khai trên mạng.

Một số dấu hiệu đáng ngờ gồm:

- Cuộc gọi rất ngắn, hình ảnh mờ hoặc thường xuyên bị gián đoạn.

- Hình ảnh, khẩu hình và giọng nói không hoàn toàn khớp nhau.

- Khuôn mặt thiếu tự nhiên hoặc biểu cảm thay đổi bất thường.

- Người gọi tránh trả lời câu hỏi riêng mà hai bên đều biết.

- Liên tục thúc giục chuyển tiền, giữ bí mật hoặc hành động ngay.

Tuy nhiên, deepfake ngày càng khó nhận biết chỉ bằng mắt và tai. Vì vậy, cách bảo vệ đáng tin cậy nhất không phải là cố xác định video thật hay giả, mà là xác minh bằng

một kênh khác. Khi nhận được yêu cầu bất thường, học sinh cần dừng lại, gọi đến số điện thoại đã biết trước hoặc hỏi trực tiếp người liên quan; không chuyển tiền và không cung cấp mật khẩu, mã OTP hay thông tin cá nhân.



Hình 3.4. 5 dấu hiệu nhận diện một cuộc gọi/video giả mạo bằng công nghệ deepfake

AI còn có thể bị lợi dụng để tạo hình ảnh giả mạo nhằm chế giễu, xúc phạm hoặc làm tổn hại danh dự của người khác. Trong môi trường học đường, việc dùng ảnh của bạn học để tạo và phát tán nội dung giả mạo không phải là hành động "đùa cho vui". Hành vi này có thể gây tổn thương nghiêm trọng cho nạn nhân, vi phạm quyền riêng tư, danh dự và nhân phẩm, đồng thời có thể bị xử lý theo quy định của nhà trường và pháp luật [8].

Để phòng tránh, học sinh cần hạn chế công khai quá nhiều hình ảnh, video và giọng nói cá nhân; kiểm soát người có thể xem nội dung đã đăng; không tạo, chia sẻ hoặc tiếp tục phát tán nội dung giả mạo người khác.

Hãy xem xét tình huống giả mạo AI trong hình 3.5 để hiểu rõ về các dấu hiệu lừa đảo: "Một cuộc gọi có hình ảnh và giọng nói giống người thân yêu cầu chuyển tiền gấp." Với từng cấp độ trường học nên xử lý tình huống như sau:

- Tiểu học: Không làm theo; gọi cha mẹ hoặc người lớn ở gần.

- THCS: Dừng cuộc gọi và liên hệ lại người đó bằng số đã biết.

- THPT: Xác minh qua một kênh độc lập; không dựa duy nhất vào giọng nói/hình ảnh; lưu lại thông tin cần thiết nếu nghi ngờ lừa đảo.



Hình 3.5. Giả giọng nói sử dụng AI để lừa đảo

Ghi nhớ: Không vội tin chỉ vì nhìn thấy khuôn mặt hoặc nghe thấy giọng nói quen thuộc. Khi có yêu cầu bất thường, hãy **dừng lại – kiểm tra – xác minh qua kênh khác**.

3.2. Rủi ro xã hội và tâm lý

Không phải mọi nguy cơ trên Internet đều đến từ virus, phần mềm độc hại hay lừa đảo. Nếu nhóm rủi ro kỹ thuật chủ yếu gây thiệt hại về tài sản, thì nhóm rủi ro xã hội và tâm lý tác động trực tiếp đến điều khó phục hồi hơn nhiều: cảm giác an toàn, lòng tự trọng và sức khỏe tinh thần của học sinh. Học sinh còn có thể gặp những tình huống làm mình buồn, lo lắng, xấu hổ, sợ hãi hoặc cảm thấy bị cô lập. Những tình huống này có thể xảy ra trong nhóm chat lớp, mạng xã hội, trò chơi trực tuyến, diễn đàn hoặc khi trò chuyện với người lạ.

Một lời bình luận ác ý, một bức ảnh bị chia sẻ để chế giễu, một tin đồn trong nhóm lớp hoặc một người lạ liên tục nhắn tin gây áp lực đều có thể ảnh hưởng đến cảm giác an toàn của học sinh. Vì vậy, khi một hoạt động trên mạng khiến các em khó chịu, sợ hãi, bị ép buộc hoặc không biết phải xử lý thế nào, các em không nên cố chịu đựng một mình.

Một nguyên tắc đơn giản có thể ghi nhớ là: dừng tương tác → lưu bằng chứng → chặn/báo cáo → nói với người đáng tin cậy.

3.2.1. Bắt nạt mạng (Cyberbullying)

Bắt nạt mạng là một trong những rủi ro xã hội đáng quan tâm đối với trẻ em và thanh thiếu niên khi sử dụng Internet. Hành vi này có thể xuất hiện dưới nhiều hình thức như gửi tin nhắn xúc phạm, chế giễu người khác trong nhóm chat, đăng hoặc chia sẻ hình ảnh nhằm làm người khác xấu hổ, tung tin sai sự thật, mạo danh tài khoản hoặc cố tình cô lập một người khỏi cộng đồng trực tuyến. Một số dạng thường gặp:

Chế giễu và xúc phạm:

Dùng lời nói, biệt danh, bình luận hoặc hình ảnh để làm nhục hay hạ thấp người khác.

Công kích tập thể:

Nhiều người cùng bình luận, nhắn tin hoặc chế giễu một học sinh trong nhóm chat hay trên mạng xã hội.

Lan truyền tin đồn:

Đăng hoặc chuyển tiếp thông tin chưa được kiểm chứng nhằm làm ảnh hưởng đến danh dự hoặc mối quan hệ của một người.

Chia sẻ hình ảnh hoặc thông tin riêng tư:

Đăng lại ảnh, đoạn chat hoặc thông tin cá nhân của người khác khi chưa được đồng ý để trêu chọc hoặc làm người đó xấu hổ.

Mạo danh:

Dùng tên, ảnh hoặc tạo tài khoản giống người khác để đăng nội dung, nhắn tin hoặc gây hiểu lầm.

Cô lập trên mạng:

Cố tình loại một người khỏi nhóm chat, nhóm học tập hoặc hoạt động trực tuyến nhằm làm người đó cảm thấy bị xa lánh.

Chỉnh sửa hoặc tạo nội dung giả:

Sử dụng ảnh, video hoặc AI để tạo nội dung giả mạo nhằm chế giễu hoặc làm tổn thương người khác.

Những dấu hiệu học sinh cần chú ý:

Không phải học sinh nào bị bắt nạt cũng kể ngay với người lớn. Một số em có thể sợ bị trách, sợ bị cấm dùng điện thoại hoặc lo rằng sự việc sẽ trở nên nghiêm trọng hơn.

Học sinh nên tìm sự giúp đỡ nếu gặp một hoặc nhiều tình huống như:

- Thường xuyên nhận tin nhắn, bình luận hoặc hình ảnh khiến mình buồn, sợ hoặc khó chịu.

- Bị nhiều người cùng chế giễu hoặc công kích.

- Ảnh, thông tin hoặc đoạn trò chuyện riêng bị chia sẻ mà mình không đồng ý.

- Có tài khoản giả mạo tên hoặc hình ảnh của mình.

- Bị cố tình loại khỏi nhóm hoặc bị lôi kéo người khác cùng tẩy chay.

- Bị đe dọa nếu không làm theo một yêu cầu nào đó.

- Cảm thấy lo lắng mỗi khi có thông báo mới hoặc không muốn vào nhóm lớp, mạng xã hội hay trò chơi mình từng thích.

Người lớn cũng nên chú ý khi học sinh đột nhiên né tránh thiết bị, buồn bực sau khi lên mạng, không muốn đến trường, mất hứng thú với bạn bè hoặc thường xuyên lo lắng về những gì đang xảy ra trong nhóm trực tuyến. Những dấu hiệu này không tự động có nghĩa là học sinh đang bị bắt nạt, nhưng là lý do để người lớn quan tâm và trò chuyện với các em.

Học sinh nên làm gì khi chứng kiến hoặc là nạn nhân của bắt nạt mạng

Nếu em là người bị bắt nạt: Điều đầu tiên là không nên đáp trả bằng cách xúc phạm hoặc đe dọa lại. Việc tranh cãi có thể khiến sự việc tiếp tục lan rộng.

Học sinh có thể thực hiện lần lượt:

1. Dừng tương tác: Không tiếp tục tranh cãi với tài khoản đang công kích.

2. Lưu lại thông tin cần thiết: Có thể lưu ảnh chụp màn hình, tên tài khoản, thời gian và đường dẫn để người lớn hoặc nhà trường hiểu được điều đã xảy ra.

3. Chặn và báo cáo: Sử dụng chức năng chặn hoặc báo cáo của ứng dụng nếu phù hợp.

4. Nói với người mình tin cậy: Hãy cho cha mẹ, giáo viên chủ nhiệm, giáo viên tư vấn hoặc một người lớn tin cậy biết.

5. Không tự giải quyết những tình huống nghiêm trọng: Nếu có đe dọa, giả mạo, phát tán thông tin riêng tư hoặc sự việc tiếp tục kéo dài, học sinh cần để người lớn và nhà trường hỗ trợ xử lý.

Nếu em chứng kiến bạn bị bắt nạt: Người đứng ngoài cũng có thể giúp ngăn bắt nạt lan rộng.

Không nên:

- Bình luận hùa theo.

- Thả biểu tượng chế giễu.

- Chụp lại rồi gửi sang nhóm khác.

- Chia sẻ tiếp hình ảnh hoặc nội dung làm tổn thương bạn.

Nên:

- Hỏi thăm và động viên bạn.

- Báo cáo nội dung vi phạm.

- Khuyên bạn nói với người lớn.

- Báo cho giáo viên hoặc người có trách nhiệm nếu sự việc tiếp tục.

Một lần chia sẻ lại nội dung chế giễu có thể khiến sự việc lan rộng hơn, ngay cả khi người chia sẻ nghĩ rằng mình "chỉ gửi cho vui".

Nếu em nhận ra mình đã tham gia bắt nạt người khác: Học sinh đôi khi có thể tham gia theo đám đông mà chưa nhận ra hậu quả. Nếu nhận ra hành động của mình đã làm người khác tổn thương, hãy dừng lại, xóa nội dung mình đã đăng nếu có thể, không tiếp tục chia sẻ và tìm cách sửa sai phù hợp. Giáo viên hoặc cha mẹ có thể giúp các em xử lý tình huống. Mục tiêu không chỉ là tìm người để trách phạt, mà còn giúp học sinh hiểu tác động của hành vi và biết cách giao tiếp có trách nhiệm hơn trên mạng.

3.2.2. Tin giả và thao túng thông tin

Tin giả là thông tin sai sự thật hoặc gây hiểu lầm, được tạo ra hay chia sẻ mà chưa được kiểm chứng. Đối với học sinh, tin giả không chỉ xuất hiện trong các bài viết hoặc tin nhắn, mà còn có thể được thể hiện dưới dạng video gây sốc, tiêu đề kích thích tò mò hoặc các "thử thách" được giới thiệu như nội dung giải trí, từ đó khiến người xem vội tin, chia sẻ hoặc bắt chước trước khi kiểm tra mức độ an toàn.

Thao túng thông tin là việc sử dụng nội dung, hình ảnh hoặc cách diễn đạt nhằm tác động đến cảm xúc và khiến người xem tin, chia sẻ hoặc hành động theo một hướng nhất định. Một số dạng thao túng thông tin thường gặp như chỉ lựa chọn những thông tin có lợi; tách lời nói, hình ảnh hoặc video khỏi bối cảnh; phóng đại một chi tiết để làm sai lệch mức độ của sự việc. Nội dung còn có thể cố tình khơi gợi sợ hãi, tức giận hoặc

thương cảm; tạo cảm giác được nhiều người ủng hộ; lặp lại một quan điểm nhiều lần hoặc che giấu mục đích quảng cáo nhằm dẫn dắt suy nghĩ và hành động của người xem.

Tin giả và thao túng thông tin có liên quan nhưng không hoàn toàn giống nhau. Tin giả thường chứa nội dung không đúng sự thật. Trong khi đó, nội dung thao túng có thể sử dụng một phần sự thật nhưng cố tình che giấu thông tin quan trọng, tách hình ảnh hoặc lời nói khỏi bối cảnh, phóng đại một chi tiết hay chỉ đưa ra những bằng chứng có lợi cho kết luận đã định trước. Vì vậy, một nội dung không hoàn toàn bịa đặt vẫn có thể khiến người xem hiểu sai vấn đề.

Đối với học sinh, tin giả và nội dung thao túng có thể xuất hiện dưới nhiều hình thức như tin đồn trong nhóm chat, bài viết giả mạo, hình ảnh chỉnh sửa, video cắt ghép, quảng cáo trá hình hoặc các trào lưu nguy hiểm được giới thiệu như hoạt động giải trí. UNICEF lưu ý rằng thông tin sai lệch có thể lan truyền nhanh và rộng; trẻ em có thể tiếp nhận chúng không chỉ từ mạng xã hội mà còn thông qua bạn bè, cha mẹ, người chăm sóc và giáo viên [9].

Khi gặp một thông tin gây sốc hoặc trào lưu đang lan truyền, học sinh cần:

- Kiểm tra tác giả, nguồn đăng và thời điểm công bố.
- Đối chiếu với nguồn chính thức hoặc ít nhất một nguồn đáng tin cậy khác.
- Không làm theo những hành động có nguy cơ gây hại.
- Không chia sẻ nội dung chỉ vì nhiều người đang quan tâm.
- Báo cho cha mẹ, giáo viên hoặc nền tảng nếu nội dung có thể gây nguy hiểm.

Ghi nhớ: Hãy áp dụng quy tắc **Dừng – Nghĩ – Kiểm tra**. Nhiều lượt xem không có nghĩa là đúng; nhiều người làm theo không có nghĩa là an toàn.

3.2.3. Dụ dỗ (Grooming) và ép buộc trên mạng (Sextortion)

Dụ dỗ (hay còn gọi là Grooming) là quá trình một người có ý đồ xấu từng bước tiếp cận, tạo lòng tin và kiểm soát trẻ em nhằm thực hiện hành vi xâm hại hoặc bóc lột. Quá trình này thường kéo dài qua nhiều lần trò chuyện, bắt đầu bằng những lời hỏi thăm, quan tâm hoặc tặng quà tưởng như vô hại. Đối tượng có thể nhanh chóng tỏ ra thân thiết, yêu cầu giữ bí mật, chuyển sang trò chuyện riêng hoặc sử dụng ứng dụng có tính năng tự xóa tin nhắn. Điều đáng lưu ý không nằm ở nội dung cụ thể của từng tin nhắn, mà ở một khuôn mẫu hành vi lặp lại: mức độ thân mật được đẩy nhanh bất thường so với thời gian quen biết, kèm theo xu hướng ngày càng rõ rệt muốn tách cuộc trò chuyện ra khỏi

tầm quan sát của người khác, chẳng hạn đề nghị chuyển từ nhóm chat chung sang nhắn tin riêng, rồi từ ứng dụng nhắn tin quen thuộc sang một ứng dụng khác ít người trong gia đình biết đến hoặc có tính năng tự xóa tin nhắn. Sau khi tạo được lòng tin, người này có thể yêu cầu trẻ cung cấp thông tin, hình ảnh riêng tư hoặc thực hiện những hành động khiến trẻ cảm thấy không thoải mái, hoặc chuyển sang sextortion. Hình 3.6 thể hiện mô hình khái quát các giai đoạn của hành vi Grooming trên Internet.



Hình 3.6. Mô hình khái quát các giai đoạn hành vi grooming trên mạng

Sextortion là tình huống một người sử dụng hình ảnh, video hoặc thông tin riêng tư để đe dọa, ép buộc nạn nhân chuyển tiền hoặc tiếp tục làm theo yêu cầu. Đối tượng thường đe dọa gửi nội dung đó cho gia đình, bạn bè hoặc đăng lên mạng. Hành vi này được gọi là *sexual extortion*, thường được biết đến với tên *sextortion*. Các em có thể hiểu đơn giản: một người có hoặc nói rằng họ có nội dung riêng tư của em và đe dọa sẽ gửi cho gia đình, bạn bè hoặc đăng lên mạng nếu em không làm theo yêu cầu của họ. Đây là hành vi ép buộc và gây hại, không phải lỗi của người bị đe dọa. Hình 3.7 mô tả về các giai đoạn của hành vi Sextortion trên mạng.



Hình 3.7. Các giai đoạn của hành vi Sextortion

Một số vụ việc tại Việt Nam cho thấy thanh thiếu niên đã bị lợi dụng nội dung riêng tư để gây sức ép và chiếm đoạt tiền [10], [11], [12].

Những dấu hiệu nhận biết grooming và sextortion gồm:

- Người mới quen tỏ ra thân thiết quá nhanh hoặc liên tục tặng quà.

- Yêu cầu giữ bí mật về mối quan hệ hoặc nội dung trò chuyện.

- Muốn chuyển sang nhắn tin riêng hay ứng dụng khó kiểm soát.

- Xin thông tin, hình ảnh riêng tư hoặc đưa ra yêu cầu khiến trẻ khó chịu.

- Đe dọa, gây áp lực hoặc yêu cầu chuyển tiền.

Tại Việt Nam, cơ quan công an đã nhiều lần cảnh báo về các hành vi sử dụng hình ảnh hoặc video riêng tư để đe dọa, cưỡng ép nạn nhân chuyển tiền như một số tình huống ở Hà Nội, Đồng Tháp [12].

Nếu gặp tình huống này, học sinh cần lưu ý:

- Không chụp, lưu trữ và chuyển tiếp hình ảnh nhạy cảm của trẻ em (kể cả của chính mình);

- Dừng liên lạc, chặn tài khoản;

- Không tiếp tục làm theo yêu cầu và không chuyển tiền;

- Ghi lại thông tin tài khoản, đường liên kết, thời gian xảy ra sự việc, các tin nhắn đe dọa;

- Báo ngay cho cha mẹ, giáo viên, người lớn tin cậy hoặc cơ quan công an.

Ghi nhớ:

- Nạn nhân không có lỗi vì đã bị lừa hoặc đe dọa và cần được bảo vệ, hỗ trợ kịp thời.

- Người thực sự quan tâm sẽ không yêu cầu em giữ bí mật với gia đình, cung cấp nội dung riêng tư hoặc làm điều khiến em sợ hãi và không thoải mái.

Nguyên tắc khi người lớn trò chuyện với học sinh gặp sự cố trên mạng: Khi học sinh tìm đến nhờ giúp đỡ, cha mẹ, giáo viên và người chăm sóc nên ưu tiên lắng nghe và giúp các em cảm thấy an toàn trước khi hỏi chi tiết sự việc.

Nên nói theo hướng:

- Cảm ơn em đã nói cho cô/chú biết.

- Em kể từ từ, chúng ta sẽ cùng tìm cách xử lý.

- Điều quan trọng bây giờ là giúp em an toàn.

- Em có thể cho cô/chú biết điều gì làm em lo nhất không?

Nên tránh những câu như:

- Tại sao em lại bấm vào đó?

- Ai bảo em nói chuyện với người lạ?

- "Biết thế sao còn làm?"

- "Đưa điện thoại đây, từ giờ cấm dùng mạng."

Những câu trách móc dễ khiến học sinh xấu hổ hoặc sợ hãi và có thể làm các em không muốn tìm đến người lớn vào lần sau.

Người lớn nên thực hiện bốn việc:

LẮNG NGHE → TRẤN AN → CÙNG KIỂM TRA → CÙNG XỬ LÝ

Không nên ép học sinh kể đi kể lại quá nhiều lần trước nhiều người. Không tự ý chia sẻ câu chuyện, ảnh chụp hoặc thông tin của học sinh cho người không cần biết. Với sự việc nghiêm trọng, cần phối hợp giữa gia đình, nhà trường và cơ quan có trách nhiệm nhưng vẫn cố gắng bảo vệ sự riêng tư và cảm giác an toàn của học sinh.

3.3. Rủi ro sức khỏe và phát triển

Nhóm rủi ro cuối cùng khác biệt với hai nhóm trên ở chỗ nó không đến từ một đối tượng xấu cụ thể, mà đến từ chính cách các nền tảng công nghệ được thiết kế để giữ chân người dùng càng lâu càng tốt, cũng như từ những khoảng trống trong hệ thống

kiểm duyệt nội dung mà không một nền tảng nào, dù đầu tư công nghệ đến đâu, có thể lấp đầy hoàn toàn.

3.3.1. Nghiện mạng xã hội và giảm tập trung

Mạng xã hội có thể mang lại thông tin và kết nối hữu ích, nhưng việc sử dụng quá mức hoặc khó kiểm soát có thể ảnh hưởng đến sức khỏe của học sinh. Các tính năng như cuộn liên tục, tự động phát video, thông báo và đề xuất nội dung hấp dẫn dễ khiến người dùng kéo dài thời gian sử dụng. Dấu hiệu đáng chú ý là thường xuyên dùng lâu hơn dự định, cảm thấy khó dừng, thức khuya xem mạng xã hội hoặc bỏ bê học tập và các hoạt động hằng ngày.

Sử dụng mạng xã hội kéo dài, đặc biệt vào buổi tối, có thể làm giảm thời gian và chất lượng giấc ngủ, gây mệt mỏi, căng thẳng và ảnh hưởng đến tâm trạng. Việc liên tục kiểm tra thông báo hoặc chuyển sự chú ý giữa bài học và điện thoại còn làm gián đoạn quá trình suy nghĩ, khiến học sinh khó tập trung, ghi nhớ kém và mất nhiều thời gian hơn để hoàn thành nhiệm vụ. Một số nghiên cứu tại Việt Nam cũng ghi nhận mối liên hệ giữa việc sử dụng mạng xã hội thiếu kiểm soát với rối loạn giấc ngủ, giảm lòng tự trọng, tăng sự phân tâm và kết quả học tập thấp hơn [13]. Các kết quả này không có nghĩa mạng xã hội là nguyên nhân duy nhất gây ra mọi vấn đề, nhưng cho thấy học sinh cần sử dụng mạng xã hội một cách cân bằng và có kiểm soát.

Để hạn chế rủi ro, học sinh nên:

- Xác định rõ mục đích và thời gian sử dụng mạng xã hội.
- Tắt những thông báo không cần thiết trong thời gian học.
- Để điện thoại xa bàn học và chỉ kiểm tra vào thời điểm đã định.
- Không sử dụng mạng xã hội trong bữa ăn hoặc ngay trước giờ ngủ.
- Dành thời gian cho vận động, giao tiếp trực tiếp và các hoạt động ngoài trời.
- Trao đổi với cha mẹ hoặc giáo viên nếu cảm thấy khó tự kiểm soát việc sử dụng.

Ghi nhớ: Rủi ro không chỉ nằm ở việc sử dụng bao lâu mà còn ở việc khó kiểm soát và để mạng xã hội ảnh hưởng đến sức khỏe, học tập và cuộc sống hằng ngày.

3.3.2. Tiếp xúc nội dung độc hại không phù hợp

Nội dung không phù hợp là nội dung không phù hợp với độ tuổi, khả năng nhận thức hoặc hoàn cảnh của học sinh. *Nội dung độc hại* là nội dung có thể gây sợ hãi, tổn thương, hiểu sai hoặc khuyến khích hành vi nguy hiểm. Đó có thể là hình ảnh bạo lực,

lời lẽ thù ghét, thông tin sai lệch, quảng cáo không phù hợp, trò chơi nguy hiểm hoặc nội dung kích động bắt nạt và phân biệt đối xử.

Học sinh có thể gặp những nội dung này khi tìm kiếm thông tin, xem video, chơi game hoặc sử dụng mạng xã hội. Trong nhiều trường hợp, các em không chủ động tìm kiếm mà nội dung vẫn xuất hiện qua quảng cáo, đường liên kết, nội dung do người khác chia sẻ hoặc hệ thống đề xuất tự động. Các nền tảng thường sử dụng công nghệ tự động, đội ngũ kiểm duyệt và phản hồi của người dùng để phát hiện nội dung vi phạm. Tuy nhiên, không có hệ thống kiểm duyệt nào hoàn toàn chính xác. Một số nội dung không phù hợp vẫn có thể lọt qua, trong khi nội dung an toàn đôi khi lại bị nhận diện nhầm. Ngay cả các nền tảng dành cho trẻ em cũng không thể bảo đảm mọi video đều đã được nhân viên kiểm tra trước khi hiển thị.

Sự phát triển của AI tạo sinh làm cho việc kiểm soát nội dung trở nên khó khăn hơn. AI có thể tạo ra số lượng lớn hình ảnh và video trong thời gian ngắn. Trong số đó có những nội dung lặp lại, sai lệch, chất lượng thấp hoặc được thiết kế để thu hút lượt xem mà không mang lại giá trị phù hợp cho trẻ em.

Đối với trò chơi điện tử có nội dung bạo lực, một số nghiên cứu ghi nhận mối liên hệ giữa việc tiếp xúc thường xuyên với trò chơi bạo lực và một số biểu hiện hoặc cảm xúc mang tính gây hấn. Mặc dù không thể kết luận rằng cứ chơi game có nội dung bạo lực thì học sinh sẽ trở nên bạo lực, gia đình cũng cần quan tâm đồng thời đến phân loại độ tuổi của trò chơi, thời gian chơi, cách chơi và những thay đổi trong cảm xúc, học tập hoặc sinh hoạt của học sinh.

Để hạn chế nguy cơ tiếp xúc với nội dung độc hại hoặc không phù hợp, học sinh và gia đình có thể sử dụng SafeSearch của Google, Restricted Mode của YouTube và các chế độ kiểm soát nội dung phù hợp với độ tuổi. Tuy nhiên, các công cụ này chỉ có tác dụng hỗ trợ, không thể thay thế sự hướng dẫn và trao đổi thường xuyên giữa trẻ em với người lớn.

Khi bất ngờ gặp nội dung gây khó chịu, sợ hãi hoặc không phù hợp, học sinh nên:

- Dừng xem và không tiếp tục mở các đường liên kết liên quan.
- Không bình luận, tải xuống hoặc chia sẻ lại nội dung.
- Sử dụng chức năng chặn hoặc báo cáo nếu biết cách thực hiện.
- Nói với cha mẹ, giáo viên hoặc người lớn tin cậy để được hỗ trợ.
- Không tự trách mình nếu nội dung xuất hiện ngoài ý muốn.

Ghi nhớ: Công cụ lọc nội dung có thể hỗ trợ nhưng không bảo vệ tuyệt đối. Khi gặp nội dung không phù hợp, hãy **dừng xem – không chia sẻ – báo cáo với người lớn**.

3.4. Phân tích tổng hợp: Ma trận rủi ro

Sau khi phân tích chi tiết từng dạng rủi ro theo ba nhóm, một câu hỏi thực tế mà nhà trường và phụ huynh thường đặt ra là: nếu nguồn lực tuyên truyền, giám sát có giới hạn, nên ưu tiên nhóm rủi ro nào trước? Để trả lời câu hỏi này một cách trực quan, các rủi ro được đánh giá mức độ phổ biến, nghiêm trọng, khả năng học sinh tự nhận biết và khả năng phòng tránh như bảng dưới đây:

Bảng 3.2. Ma trận phân tích các rủi ro

Nhóm rủi ro	Loại rủi ro	Mức độ phổ biến	Mức độ nghiêm trọng	Khả năng học sinh tự nhận biết	Khả năng phòng tránh
Rủi ro kỹ thuật và phần mềm độc hại	Phishing và smishing	Cao	Cao	Trung bình	Cao
	Mã độc từ game và ứng dụng crack	Trung bình	Cao	Thấp	Cao
	Deepfake và lừa đảo bằng AI	Trung bình	Cao	Thấp	Trung bình
Rủi ro xã hội và tâm lý	Bắt nạt trực tuyến	Cao	Cao	Trung bình	Trung bình
	Tin giả và thao túng thông tin	Cao	Trung bình	Trung bình	Trung bình
	Grooming và sextortion	Khó xác định	Rất cao	Thấp	Trung bình
Rủi ro sức khỏe và phát triển	Nghiện mạng xã hội và giảm tập trung	Cao	Trung bình	Trung bình	Cao

	Tiếp xúc với nội dung độc hại, không phù hợp	Cao	Trung bình	Trung bình	Trung bình

Từ ma trận trên, dễ dàng nhận thấy bắt nạt trực tuyến, phishing và smishing là những rủi ro vừa phổ biến, vừa gây hậu quả nghiêm trọng, song học sinh lại khó nhận biết. Do đó, nhà trường và phụ huynh nên ưu tiên giáo dục, nhắc lại thường xuyên và luyện tập cách ứng phó qua các tình huống cụ thể. Grooming và sextortion tuy khó xác định mức độ phổ biến nhưng có hậu quả đặc biệt nghiêm trọng và khó phát hiện. Vì vậy, nhà trường cần ưu tiên xây dựng kênh phản ánh kín đáo, hướng dẫn học sinh nhận biết dấu hiệu bất thường và biết tìm đến người lớn tin cậy. Mã độc và deepfake tuy không quá phổ biến song lại gây hậu quả nghiêm trọng; để phòng tránh, nhà trường có thể lồng ghép vào các hoạt động hướng dẫn bảo vệ tài khoản, thiết bị và xác minh thông tin. Các rủi ro phổ biến nhưng thường tích lũy dần như tin giả, nội dung không phù hợp và sử dụng mạng xã hội quá mức nên được giáo dục thường xuyên trong môn học, sinh hoạt lớp và hoạt động phối hợp với gia đình.

Việc phân tích mức độ phổ biến và nghiêm trọng của các nhóm rủi ro không có nghĩa là bỏ qua những rủi ro ở nhóm sau, mà nhằm lựa chọn hình thức triển khai phù hợp: rủi ro nghiêm trọng cần có quy trình ứng phó rõ ràng; rủi ro thường gặp cần được giáo dục liên tục để hình thành thói quen an toàn.

3.5. Kết luận chương

Những rủi ro được trình bày trong chương này có thể xuất hiện từ những tình huống rất quen thuộc: một đường link thông báo kết quả thi, một tệp cài đặt trò chơi, một cuộc gọi giả mạo bằng AI, một lời chế giễu trong nhóm chat hay việc mải sử dụng mạng xã hội đến quên giờ học và giờ ngủ. Điều đáng chú ý là rủi ro trên mạng không phải lúc nào cũng dễ nhận ra ngay từ đầu. Chúng thường xuất hiện khi người dùng đang tò mò, vội vàng, lo lắng hoặc tin tưởng vào một thông tin tưởng như quen thuộc.

Vì vậy, mục tiêu của chương này không phải làm học sinh lo sợ khi sử dụng Internet, mà giúp các em nhận biết sớm nguy cơ và biết cách ứng phó phù hợp. Các nguyên tắc và kỹ năng ở Chương 2 chỉ thực sự phát huy tác dụng khi được thực hành thường xuyên: kiểm tra trước khi bấm vào đường link, suy nghĩ trước khi chia sẻ, bảo vệ thông tin cá nhân, cảnh giác với yêu cầu bất thường và biết dừng lại khi cảm thấy không an toàn.

Học sinh cũng cần nhớ rằng rủi ro thường gặp chưa chắc là nguy hiểm nhất, còn rủi ro ít gặp cũng không nên xem nhẹ. Quan trọng hơn việc ghi nhớ tên từng loại rủi ro là hình thành phản xạ: **Nhận biết – Dừng lại – Kiểm tra – Tìm sự hỗ trợ khi cần.**

Khi gặp vấn đề vượt quá khả năng tự xử lý, học sinh không nên đối mặt một mình mà cần chủ động tìm sự hỗ trợ từ cha mẹ, thầy cô hoặc người lớn tin cậy. Đây chính là nền tảng để mỗi học sinh sử dụng Internet an toàn, chủ động và có trách nhiệm.

CHƯƠNG 4. CÁC BIỆN PHÁP PHÒNG TRÁNH, ỨNG PHÓ KHI GẶP SỰ CỐ TRÊN KHÔNG GIAN MẠNG

Ở Chương 2, học sinh đã được trang bị những nguyên tắc và kỹ năng để sử dụng mạng an toàn. Chương 3 giúp nhận biết các rủi ro thường gặp và hậu quả có thể xảy ra. Tuy nhiên, dù đã cẩn thận, chúng ta vẫn có thể gặp sự cố: bấm nhầm vào đường link giả mạo, để lộ mật khẩu, mất tài khoản, bị lừa chuyển tiền, bị bắt nạt, giả mạo hoặc phát tán thông tin cá nhân trên mạng.

Khi sự cố xảy ra, điều quan trọng là không hoảng loạn, không vội làm theo yêu cầu của người lạ và biết việc nào cần thực hiện trước. Xử lý đúng ngay từ đầu có thể giúp hạn chế thiệt hại, bảo vệ tài khoản và thông tin cá nhân, đồng thời tạo điều kiện để gia đình, nhà trường hoặc cơ quan chức năng hỗ trợ kịp thời.

Vì vậy, Chương 4 tập trung vào hai nội dung chính. Mục 4.1 hướng dẫn những biện pháp phòng ngừa cần thực hiện thường xuyên để giảm khả năng xảy ra sự cố, từ bảo vệ thiết bị và tài khoản đến sự đồng hành của gia đình và nhà trường. Mục 4.2 hướng dẫn quy trình xử lý khi sự cố đã xảy ra, giúp học sinh dễ nhớ, biết cần làm gì trước, làm gì tiếp theo và tìm sự hỗ trợ ở đâu.

Thông điệp quan trọng của chương là: **Phòng ngừa để giảm rủi ro – Bình tĩnh để xử lý đúng – Tìm sự hỗ trợ khi cần.**

Lưu ý quan trọng về các kênh hỗ trợ

Khi gặp sự cố, học sinh **không nên cố gắng tự giải quyết mọi việc một mình**. Trước hết, hãy nói với cha mẹ, giáo viên hoặc người lớn tin cậy. Tùy tính chất và mức độ của sự việc, gia đình và nhà trường có thể liên hệ với cơ quan chức năng hoặc các kênh hỗ trợ phù hợp.

Các số điện thoại và địa chỉ tiếp nhận phản ánh có thể được điều chỉnh theo thời gian. Với nguy cơ trực tiếp liên quan đến an toàn của trẻ em, học sinh và gia đình có thể liên hệ Tổng đài quốc gia bảo vệ trẻ em 111. Khi có tình huống khẩn cấp về an ninh, trật tự, có thể gọi 113. Nếu có dấu hiệu lừa đảo, chiếm đoạt tài sản hoặc hành vi phạm tội trên không gian mạng, cần nhanh chóng trình báo cơ quan Công an nơi gần nhất. Đối với sự cố kỹ thuật về an ninh mạng cần hỗ trợ ứng cứu, có thể tham khảo Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT) tại vncert.vn. Khi cần kiểm tra thông tin chủ thể của một tên miền đáng ngờ, có thể sử dụng Cổng tra cứu thông tin tên miền tại tracuutenmien.gov.vn.

4.1. Các biện pháp phòng tránh chủ động

An toàn trên mạng không thể chỉ dựa vào một công cụ hay một nguyên tắc duy nhất. Một phần mềm bảo vệ tốt vẫn chưa đủ nếu người dùng dễ dàng cung cấp mật khẩu cho người khác; ngược lại, học sinh dù đã có kỹ năng vẫn có thể gặp rủi ro nếu thiết bị không được cập nhật hoặc tài khoản không được bảo vệ đúng cách. Vì vậy, cách phòng tránh hiệu quả là kết hợp nhiều biện pháp và hình thành thói quen an toàn trong quá trình sử dụng Internet hằng ngày.

Đối với học sinh, việc phòng tránh rủi ro cần có sự phối hợp của ba yếu tố: *công cụ kỹ thuật, sự đồng hành của gia đình, kiến thức và kỹ năng* được trang bị tại nhà trường. Các công cụ kỹ thuật giúp bảo vệ thiết bị, tài khoản và hạn chế nội dung không phù hợp; gia đình hướng dẫn, trao đổi và hỗ trợ khi các em gặp tình huống khó xử; còn nhà trường giúp học sinh hiểu rủi ro, thực hành kỹ năng và hình thành cách ứng xử có trách nhiệm trên môi trường mạng.

Ba yếu tố này bổ sung cho nhau và cùng hướng tới một mục tiêu: giúp học sinh chủ động nhận biết nguy cơ, phòng tránh từ sớm và biết tìm sự hỗ trợ khi cần thiết. Quan trọng hơn, an toàn mạng không nên chỉ được thực hiện khi sự cố đã xảy ra mà cần trở thành thói quen hằng ngày, giống như khóa cửa khi ra khỏi nhà hay đội mũ bảo hiểm khi tham gia giao thông.

4.1.1. Cài đặt công cụ bảo mật thiết bị

Thiết bị như điện thoại, máy tính bảng và máy tính thường đã được tích hợp một số chức năng bảo mật. Vì vậy, bước đầu tiên không phải là cài thật nhiều phần mềm bảo vệ, mà là kiểm tra và sử dụng đúng các tính năng bảo mật có sẵn, thường xuyên cập nhật hệ điều hành và ứng dụng, đồng thời chỉ cài phần mềm từ những nguồn đáng tin cậy.

Đối với điện thoại và máy tính bảng Android, học sinh nên kiểm tra Google Play Protect đang được bật. Đây là công cụ bảo mật được tích hợp trong hệ sinh thái Android, có khả năng kiểm tra ứng dụng khi cài đặt, quét định kỳ các ứng dụng đã cài và cảnh báo hoặc xử lý những ứng dụng có khả năng gây hại. Học sinh nên ưu tiên tải ứng dụng từ Google Play hoặc nguồn chính thức của nhà phát triển và không tự ý cài các tệp APK được gửi qua tin nhắn, mạng xã hội hoặc website không rõ nguồn gốc.

Đối với iPhone và iPad, hệ điều hành đã sử dụng nhiều cơ chế bảo vệ tích hợp để kiểm soát ứng dụng và hạn chế một ứng dụng can thiệp trái phép vào dữ liệu hoặc ứng dụng khác. Vì vậy, học sinh cần ưu tiên cập nhật iOS/iPadOS, cài ứng dụng từ nguồn

chính thức, chú ý các cảnh báo của hệ thống và kiểm tra quyền truy cập mà ứng dụng yêu cầu.

Đối với máy tính sử dụng Windows 10 hoặc Windows 11, học sinh có thể sử dụng Windows Security, trong đó có Microsoft Defender Antivirus, tường lửa và các chức năng bảo vệ khác được tích hợp sẵn. Cần kiểm tra chế độ bảo vệ thời gian thực đang hoạt động và thường xuyên cập nhật Windows để nhận các bản vá bảo mật mới.

Trong một số trường hợp, gia đình hoặc nhà trường có thể lựa chọn phần mềm bảo mật bổ sung nếu cần thêm các chức năng như quét mã độc, cảnh báo website lừa đảo hoặc bảo vệ khi truy cập Internet. Khi lựa chọn, nên ưu tiên công cụ có nhà phát triển rõ ràng, còn được cập nhật, có mặt trên kho ứng dụng chính thức và không yêu cầu những quyền truy cập không cần thiết. Một số sản phẩm bảo mật phổ biến hiện nay có các phiên bản dành cho thiết bị cá nhân, chẳng hạn Bitdefender Mobile Security, Malwarebytes Mobile Security hoặc Avast One. Việc nêu tên các sản phẩm này chỉ nhằm minh họa các lựa chọn đang có, không phải khuyến nghị bắt buộc hoặc quảng bá cho một sản phẩm cụ thể.

Học sinh không nên tự cài nhiều phần mềm bảo mật cùng lúc chỉ vì cho rằng "càng nhiều càng an toàn". Quan trọng hơn là duy trì những thói quen cơ bản: cập nhật thiết bị, bật các chức năng bảo vệ có sẵn, chỉ tải ứng dụng từ nguồn đáng tin cậy, kiểm tra quyền truy cập của ứng dụng và hỏi cha mẹ, giáo viên hoặc người có kiến thức kỹ thuật khi thiết bị xuất hiện dấu hiệu bất thường.

Điều cần nhớ: Công cụ bảo mật chỉ là một lớp bảo vệ. Thiết bị vẫn có thể gặp rủi ro nếu người dùng tự cung cấp mật khẩu, mã OTP, bấm vào liên kết giả mạo hoặc cài ứng dụng không rõ nguồn gốc. Vì vậy, bảo mật thiết bị phải đi cùng với thói quen sử dụng Internet an toàn.

Lịch cập nhật tự động hằng tuần – thói quen nhỏ, hiệu quả lớn

Như đã phân tích ở Chương 3, phần lớn các lỗ hổng bảo mật nghiêm trọng – kể cả những lỗ hổng từng bị khai thác để cài phần mềm gián điệp – đều đã có bản vá trước khi bị lợi dụng rộng rãi; vấn đề chỉ là người dùng có cập nhật kịp thời hay không.

Gia đình nên duy trì thói quen kiểm tra và cài đặt cập nhật hệ điều hành, trình duyệt, ứng dụng antivirus vào một khung giờ cố định mỗi tuần (ví dụ tối Chủ nhật), thay vì chỉ cập nhật khi thiết bị đã có dấu hiệu bất thường. Hầu hết thiết bị hiện nay đều hỗ trợ bật "Cập nhật tự động" trong phần Cài đặt, giúp việc này diễn ra mà không cần ghi nhớ thủ công.

Để tiện tra cứu nhanh, bảng dưới đây tổng hợp lại các công cụ theo từng nền tảng thiết bị:

Bảng 4.1. Bảng tổng hợp các công cụ hỗ trợ theo hệ điều hành

Nhu cầu	Android	iOS (iPhone/iPad)
Diệt mã độc / bảo mật thiết bị	Avast Mobile Security; Viettel Mobile Security (miễn phí, ưu tiên cho thuê bao Viettel)	Không có "diệt virus" truyền thống do kiến trúc sandbox; thay bằng cập nhật iOS đầy đủ + Lockdown Mode khi cần
Kiểm soát phụ huynh	Google Family Link (giới hạn giờ, duyệt app, báo cáo hoạt động, định vị)	Screen Time tích hợp sẵn (App Limits, Downtime, Content & Privacy Restrictions)
Lọc nội dung mạng / WiFi công cộng	VPN uy tín khi dùng WiFi công cộng; DNS lọc nội dung gia đình	VPN uy tín khi dùng WiFi công cộng; cấu hình DNS lọc nội dung ở cấp hệ thống
Sao lưu dữ liệu	Google Drive / Google Photos tự động	iCloud tự động

4.1.2. Thiết lập kiểm soát phụ huynh thông minh

Lớp phòng vệ thứ hai không nằm ở thiết bị mà nằm ở cách gia đình đồng hành cùng con trong không gian số, và Google Family Link là công cụ miễn phí, phổ biến nhất cho mục đích này trên hệ sinh thái Android. Về bản chất, Family Link không phải một phần mềm giám sát bí mật, mà là một công cụ quản lý tài khoản Google của trẻ dưới sự cho phép và liên kết trực tiếp với tài khoản của phụ huynh, với bốn nhóm tính năng chính được minh họa trong Hình 4.1:



Hình 4.1. Bốn nhóm tính năng chính của Google Family Link

Về giới hạn thời gian, phụ huynh có thể đặt một khung giờ sử dụng cụ thể mỗi ngày (ví dụ 2 giờ/ngày), cùng với "Giờ đi ngủ" hoặc "Thời gian ngừng hoạt động" – khoảng thời gian cố định mà thiết bị sẽ tự động khóa bất kể trẻ đã dùng hết giới hạn hằng ngày hay chưa. Về quản lý ứng dụng, mọi lượt tải ứng dụng mới từ Google Play của tài khoản trẻ đều cần phụ huynh phê duyệt từ xa, giúp ngăn chặn từ sớm rủi ro cài đặt ứng dụng không phù hợp hoặc chứa mã độc đã phân tích ở Chương 3. Về báo cáo hoạt động, Family Link cung cấp báo cáo định kỳ theo tuần hoặc tháng, cho biết những ứng dụng trẻ dùng nhiều nhất và tổng thời gian sử dụng – đây là cơ sở dữ liệu khách quan để mở đầu cuộc trò chuyện với con thay vì chỉ dựa vào cảm nhận chủ quan. Cuối cùng, tính năng định vị và khóa từ xa cho phép phụ huynh xem vị trí thiết bị Android hoặc khóa màn hình ngay lập tức trong tình huống khẩn cấp.

Kết hợp giới hạn phù hợp với trò chuyện và đồng hành: Công cụ kiểm soát của phụ huynh chỉ thực sự hữu ích khi được sử dụng cùng với sự trao đổi giữa cha mẹ và con. Mục đích không phải là theo dõi mọi hoạt động của trẻ hay cấm hoàn toàn việc sử dụng Internet, mà là thiết lập những giới hạn phù hợp với độ tuổi, đồng thời giúp trẻ hiểu vì sao những giới hạn đó cần thiết.

Vì vậy, gia đình nên kết hợp công cụ kỹ thuật với sự đồng hành: có thể đặt giới hạn về thời gian sử dụng, ứng dụng và nội dung phù hợp với độ tuổi, nhưng đồng thời cần giải thích cho trẻ lý do của những quy tắc đó và duy trì thói quen trò chuyện thường xuyên. Quan trọng nhất là tạo được sự tin tưởng để khi gặp nội dung xấu, bị bắt nạt, lừa

đảo hoặc một tình huống khiến mình lo lắng, học sinh sẵn sàng nói với cha mẹ thay vì cố gắng tự giải quyết hoặc che giấu sự việc. Hình 4.2 dưới đây là giải thích các hình thức giám sát: giám sát hạn chế, giám sát chủ động, giám sát kỹ thuật và cách kết hợp phù hợp.



Hình 4.2. Các hình thức cha mẹ đồng hành khi học sinh sử dụng Internet

Giám sát không có nghĩa là theo dõi mọi việc học sinh làm trên mạng. Mục tiêu là giúp các em sử dụng Internet an toàn hơn và dần hình thành khả năng tự bảo vệ bản thân. Vì vậy, cha mẹ nên nói rõ cho con biết những quy tắc hoặc công cụ nào đang được sử dụng và vì sao cần sử dụng.

Ở tiểu học, cha mẹ và thầy cô cần đồng hành nhiều hơn. Các em nên được hướng dẫn bằng những quy tắc ngắn, rõ ràng như: không bấm link lạ, không nói chuyện với người lạ, có điều gì lo lắng thì hỏi người lớn. Công cụ kỹ thuật có thể được sử dụng để giới hạn thời gian và nội dung phù hợp với tuổi.

Ở THCS, học sinh đã sử dụng Internet độc lập hơn. Cha mẹ vẫn cần có những giới hạn cần thiết nhưng nên giải thích lý do và trao đổi với con, giúp các em biết nhận diện lừa đảo, bảo vệ tài khoản, xử lý bắt nạt mạng và tự kiểm tra thông tin trước khi hành động.

Ở THPT, học sinh cần được tăng dần quyền tự chủ. Gia đình nên chuyển trọng tâm từ việc kiểm soát sang trao đổi, thống nhất nguyên tắc và hỗ trợ khi cần. Học sinh cần biết tự quản lý thời gian, bảo vệ dữ liệu, đánh giá rủi ro và chịu trách nhiệm về những gì mình đăng, bình luận hoặc chia sẻ trên mạng.

Hình 4.3 minh họa trực quan các cách cha mẹ hỗ trợ học sinh ở các cấp học khi sử dụng Internet.



Hình 4.3. Bốn cách cha mẹ hỗ trợ học sinh sử dụng Internet an toàn

Ví dụ minh họa cách mở đầu cuộc trò chuyện dựa trên báo cáo hoạt động của Family Link (không phải kịch bản cố định, chỉ mang tính gợi ý): thay vì mở đầu bằng "Sao con dùng điện thoại nhiều thế, mẹ thấy hết trong báo cáo rồi" – dễ khiến trẻ phòng thủ – có thể thử "Mẹ thấy tuần này con xem TikTok nhiều hơn tuần trước đó, có nội dung gì hay mà con muốn chia sẻ với mẹ không?". Cách đặt vấn đề thứ hai giữ đúng tinh thần giám sát chủ động: dùng dữ liệu khách quan từ công cụ kỹ thuật làm điểm khởi đầu cho đối thoại, thay vì làm bằng chứng để phán xét.

4.1.3. Giáo dục kỹ năng số tại trường học

Bên cạnh các công cụ kỹ thuật và sự đồng hành của gia đình, nhà trường là môi trường quan trọng để giúp học sinh hình thành kiến thức, kỹ năng và thói quen sử dụng

Internet an toàn. Thay vì chỉ tổ chức một vài buổi tuyên truyền riêng lẻ, hoạt động giáo dục an toàn mạng nên được thực hiện thường xuyên, tạo cơ hội để học sinh vừa học, vừa thực hành và chia sẻ kiến thức với bạn bè. Nhà trường có thể triển khai ba hình thức đơn giản: *Câu lạc bộ An toàn mạng; Cuộc thi Học sinh với An ninh mạng; Poster và Infographic.*

Câu lạc bộ An toàn mạng có thể tập hợp một nhóm học sinh quan tâm hoặc học sinh nòng cốt, được giáo viên hướng dẫn và sinh hoạt định kỳ. Các em không chỉ tìm hiểu sâu hơn về mật khẩu, lừa đảo, tin giả, bắt nạt mạng hay bảo vệ thông tin cá nhân mà còn có thể chia sẻ lại những kiến thức đó với bạn bè bằng ngôn ngữ gần gũi. Đây là cách tiếp cận peer education, học sinh hỗ trợ và chia sẻ kiến thức với học sinh. Một tổng quan hệ thống công bố trên BMC Public Health năm 2022, phân tích 73 nghiên cứu về giáo dục đồng trang lứa trong trường học ở nhóm 11–18 tuổi, cho thấy mô hình này có tiềm năng cải thiện kiến thức của người học, mặc dù hiệu quả thay đổi hành vi còn phụ thuộc vào nội dung và cách tổ chức [14].

Cuộc thi "Học sinh với An ninh mạng" giúp biến kiến thức an toàn mạng thành hoạt động ôn tập và thi đua nhẹ nhàng. Nhà trường có thể tham khảo cuộc thi trực tuyến "Học sinh với An ninh mạng 2026" được Bộ Công an và Bộ Giáo dục và Đào tạo bảo trợ, do Hiệp hội An ninh mạng quốc gia chủ trì, phối hợp với Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05), Bộ Công an; Cục Khoa học, Công nghệ và Thông tin, Bộ Giáo dục và Đào tạo cùng các đơn vị đồng hành tổ chức. Cuộc thi hướng tới cung cấp kiến thức, kỹ năng sử dụng Internet an toàn và giúp học sinh nhận diện, phòng tránh nguy cơ trên môi trường mạng [15].

Poster và infographic đặt tại lớp học, thư viện, hành lang hoặc khu vực sinh hoạt chung giúp các thông điệp an toàn mạng xuất hiện thường xuyên trong môi trường học đường. Nhà trường có thể sử dụng chính các infographic trong tài liệu này, chẳng hạn 12 nguyên tắc an toàn ở Chương 2 hoặc các nhóm rủi ro ở Chương 3. Nội dung nên ngắn, trực quan và tập trung vào những hành động học sinh có thể thực hiện ngay. Hình 4.4 minh họa về ba hình thức triển khai giáo dục kỹ năng tại trường học.



Hình 4.4. Ba trụ cột giáo dục kỹ năng số tại trường học

4.1.4. Xây dựng cơ chế tiếp nhận và xử lý phản ánh trong nhà trường

Ba hoạt động ở mục 4.1.3 tập trung vào việc nâng cao nhận thức, nhưng nhận thức tốt chỉ phát huy tác dụng đầy đủ khi đi kèm một cơ chế tiếp nhận, xử lý rõ ràng – nếu không, học sinh dù được trang bị đủ kiến thức vẫn có thể không biết phản ánh với ai, hoặc phản ánh xong nhưng không được xử lý kịp thời.

Đáng chú ý, bạo lực học đường ngày nay không chỉ diễn ra trực tiếp trong trường học mà còn có thể tiếp tục hoặc lan rộng trên môi trường mạng. Một số vụ việc đã xuất hiện tình trạng học sinh quay lại hình ảnh, video bạo lực rồi phát tán trên mạng xã hội, làm cho sự việc tiếp tục được chia sẻ, bình luận và có thể gây thêm tổn thương cho người bị hại [16]. Vì vậy, phòng ngừa bạo lực học đường cần gắn với giáo dục kỹ năng giao tiếp, giải quyết mâu thuẫn, chia sẻ thông tin và ứng xử có trách nhiệm trên môi trường mạng, đồng thời giúp học sinh biết tìm kiếm sự hỗ trợ khi gặp hoặc chứng kiến hành vi bắt nạt. Đây cũng là vấn đề về việc tăng cường chấn chỉnh, xử lý, ngăn chặn, đẩy lùi bạo lực học đường trong các cơ sở giáo dục được Bộ GD&ĐT nêu trong Công văn số 3147/BGDĐT-HSSV được Bộ Giáo dục và Đào tạo ban hành ngày 29/5/2026.

Theo hướng dẫn phòng, chống bạo lực học đường hiện nay, mô hình xử lý cấp trường nên vận hành qua nhiều lớp phối hợp thay vì dồn hết trách nhiệm lên một cá nhân giáo viên: triển khai hòm thư góp ý điện tử hoặc kênh liên lạc bảo mật để học sinh dễ dàng phản ánh mà không sợ bị lộ danh tính; phát huy vai trò của giáo viên chủ nhiệm, lực lượng Đoàn – Đội và tổ tư vấn tâm lý học đường để nắm bắt mâu thuẫn ngay từ khi

mới phát sinh, kể cả khi mâu thuẫn đó khởi nguồn trên mạng xã hội chứ không phải trong lớp học; và quan trọng không kém, thiết lập kênh liên lạc thường xuyên với công an địa bàn để khi cần, nhà trường có thể phối hợp xử lý nhanh thay vì mỗi bên tự xoay xở. Hình 4.5 mô tả hướng dẫn về quy trình tiếp nhận và xử lý phản ánh sự cố ở cấp trường học.



Hình 4.5. Quy trình tiếp nhận và xử lý phản ánh sự cố trên không gian mạng

Một vấn đề cũng cần được quan tâm khi xử lý bắt nạt hoặc hành vi không phù hợp trên mạng là: nhà trường cần làm gì với học sinh gây ra hành vi đó? Bảo vệ và hỗ trợ học sinh bị ảnh hưởng luôn là ưu tiên, nhưng đồng thời, học sinh có hành vi sai cũng cần được giúp nhận ra hậu quả, chịu trách nhiệm phù hợp và biết cách sửa chữa. Cách tiếp cận này phù hợp với quy định hiện hành của Bộ Giáo dục và Đào tạo. Theo Thông tư số 19/2025/TT-BGDĐT, việc kỷ luật học sinh phải bảo đảm tính giáo dục, nhân văn và vì sự tiến bộ của học sinh; đồng thời phải tôn trọng, khách quan, không định kiến và phù hợp với đặc điểm tâm sinh lý của từng em. Các biện pháp kỷ luật hiện hành cũng tập trung vào việc giúp học sinh nhận thức hành vi và khắc phục hậu quả: đối với học sinh tiểu học là nhắc nhở, yêu cầu xin lỗi; đối với học sinh ở các cấp học tiếp theo là nhắc nhở, phê bình hoặc yêu cầu viết bản tự kiểm điểm.

Điều đó không có nghĩa là bỏ qua hoặc xem nhẹ hành vi sai. Học sinh gây ra sự việc vẫn cần chịu trách nhiệm phù hợp, xin lỗi và khắc phục hậu quả; đồng thời nhà trường phải bảo đảm an toàn, quyền lợi và sự hỗ trợ cần thiết cho học sinh bị ảnh hưởng. Mục tiêu cuối cùng không chỉ là "xử lý một vi phạm", mà còn giúp học sinh hiểu mình đã sai ở đâu, sửa chữa điều đã gây ra và không lặp lại hành vi đó.

Một sự cố trên mạng không phải lúc nào cũng kết thúc khi nội dung đã được gỡ bỏ hoặc tài khoản vi phạm đã bị chặn. Học sinh có thể vẫn lo lắng về việc nội dung bị chia sẻ lại, sợ gặp người liên quan ở trường, ngại tham gia nhóm lớp hoặc không muốn tiếp tục sử dụng một nền tảng. Vì vậy, cơ chế hỗ trợ của nhà trường cần bao gồm cả tiếp nhận phản ánh, xử lý sự việc và theo dõi học sinh sau sự cố.

Đối với những tình huống nhạy cảm như bắt nạt mạng, bị đe dọa, bị người lạ tiếp cận với mục đích không phù hợp hoặc bị lợi dụng thông tin riêng tư, nhà trường cần đặc biệt chú ý đến bảo mật danh tính và quyền riêng tư của học sinh. Thông tin về sự việc chỉ nên được chia sẻ cho những người thực sự cần tham gia hỗ trợ và xử lý. Không công khai tên học sinh, nội dung phản ánh, hình ảnh hoặc thông tin riêng tư trong lớp học, nhóm phụ huynh hoặc những kênh không cần thiết. Hình 4.6 dưới đây minh họa về cách thức xử lý sau sự cố khi sự việc đã giải quyết xong.



Hình 4.6. Hướng dẫn xử lý sau sự cố cho từng cấp độ trường học

Ba nguyên tắc khi nhà trường xây dựng cơ chế xử lý

Bảo mật danh tính người phản ánh: học sinh sẽ chỉ dám lên tiếng nếu tin rằng việc phản ánh không khiến mình trở thành mục tiêu tiếp theo của sự trả đũa.

Phân định rõ mức độ nghiêm trọng để lựa chọn hướng xử lý phù hợp: không phải mọi mâu thuẫn trên mạng đều cần đến công an, nhưng cũng không nên xem nhẹ những dấu hiệu có thể leo thang thành xâm hại hoặc đe dọa nghiêm trọng như đã phân tích ở Chương 3.

Không khép lại vụ việc ngay sau khi xử lý kỷ luật: cả nạn nhân lẫn học sinh vi phạm đều cần được theo dõi, hỗ trợ tâm lý trong thời gian sau đó – nội dung này sẽ được phân tích kỹ hơn ở bước 7 của quy trình ứng phó tại mục 4.2.3.

Hơn nữa, từ những việc xây dựng, tiếp nhận và xử lý phản ánh, nhà trường cũng nên xây dựng một số kênh phản ánh kín đáo và an toàn để giúp học sinh vừa nhận thức được việc làm, hành vi của mình và cũng có thể phản ánh trung thực và tự nguyện. Dưới đây là một số gợi ý về các kênh phản ánh và các yếu tố bảo mật cho các tình huống nhạy cảm.

a. Kênh phản ánh trong trường

Nhà trường nên công bố ít nhất một kênh để học sinh có thể phản ánh sự cố một cách riêng tư và dễ tiếp cận. Tùy điều kiện của từng trường, có thể sử dụng:

- Giáo viên chủ nhiệm hoặc giáo viên mà học sinh tin cậy;

- Phòng/tổ tư vấn tâm lý học đường;

- Hòm thư góp ý đặt ở vị trí phù hợp;

- Biểu mẫu hoặc hộp thư điện tử dành riêng cho phản ánh về an toàn học sinh;

- Cán bộ phụ trách công tác học sinh, Đoàn – Đội hoặc bộ phận được nhà trường giao nhiệm vụ.

Học sinh cần được biết rõ có thể phản ánh với ai, bằng cách nào và thông tin của mình sẽ được bảo vệ ra sao. Kênh phản ánh nên được giới thiệu từ đầu năm học và nhắc lại trong sinh hoạt lớp, hoạt động giáo dục kỹ năng số hoặc các chương trình tuyên truyền về sử dụng mạng an toàn.

b. Nguyên tắc bảo mật cho các tình huống nhạy cảm

Bảo vệ quyền riêng tư của học sinh khi xử lý sự cố. Với các sự cố liên quan đến bắt nạt, đe dọa, grooming hoặc thông tin riêng tư, nhà trường cần:

- *Không yêu cầu học sinh kể lại sự việc trước tập thể*. Việc trao đổi nên diễn ra ở không gian phù hợp, với số người tham gia ít nhất cần thiết.

- *Không chuyển tiếp bằng chứng một cách không cần thiết*. Ảnh chụp, đoạn trò chuyện hoặc thông tin riêng tư chỉ được sử dụng phục vụ việc xác minh và hỗ trợ.

- *Không công khai danh tính người phản ánh*. Giáo viên và cán bộ xử lý cần tránh để thông tin lan sang nhóm lớp, bạn bè hoặc nhóm phụ huynh nếu không cần thiết.

- *Không dùng lời nói khiến học sinh cảm thấy bị trách móc*. Khi học sinh chủ động tìm đến nhà trường, phản ứng đầu tiên nên là lắng nghe, bảo đảm an toàn và cùng tìm hướng giải quyết.

Có thể dùng những câu như:

"Cảm ơn em đã nói với cô/thầy."

"Em có thể kể từ từ, chúng ta sẽ cùng tìm cách xử lý."

"Điều gì làm em lo nhất lúc này?"

Tránh những câu như: "Sao em lại làm thế?", "Ai bảo em nói chuyện với người lạ?", "Biết nguy hiểm sao vẫn làm?". Những cách hỏi này có thể khiến học sinh e ngại và không muốn tiếp tục tìm kiếm sự hỗ trợ.

4.2. Quy trình ứng phó khẩn cấp khi gặp sự cố

Dù đã thực hiện các biện pháp phòng tránh, sự cố trên mạng vẫn có thể xảy ra: bấm nhầm vào đường link giả mạo, để lộ mật khẩu, mất tài khoản, bị lừa đảo, bắt nạt, đe dọa hoặc phát tán thông tin cá nhân. Khi đó, bình tĩnh và xử lý đúng ngay từ đầu có thể giúp hạn chế thiệt hại và ngăn sự việc trở nên nghiêm trọng hơn. Điều quan trọng là học sinh không nên vội vàng làm theo yêu cầu của người lạ, tự tìm cách giải quyết bằng mọi giá hoặc che giấu sự việc vì lo sợ bị trách phạt. Thay vào đó, hãy dừng lại, xác định điều gì đang xảy ra và thực hiện từng bước phù hợp. Nếu tình huống vượt quá khả năng tự xử lý, cần chủ động nói với cha mẹ, thầy cô hoặc người lớn tin cậy để được hỗ trợ càng sớm càng tốt.

Quy trình 7 bước được minh họa trong Hình 4.7 dưới đây được tổng hợp và hệ thống hóa từ các khuyến cáo nhất quán của cơ quan chức năng, chia thành ba giai đoạn để dễ ghi nhớ ngay cả trong tình huống hoảng loạn.



Hình 4.7. Quy trình 7 bước ứng phó khi gặp sự cố trên không gian mạng

4.2.1. Bước 1–3: Phản ứng ngay lập tức

Ba bước đầu tiên cần được thực hiện trong vài phút đầu ngay khi phát hiện sự cố – dù đó là nhận ra mình vừa bấm vào một đường link giả mạo, phát hiện tài khoản đang bị một kẻ lạ nhắn tin đe dọa, hay nghi ngờ thiết bị đã dính mã độc sau khi cài một ứng dụng lạ. Bước đầu tiên, ngắt kết nối WiFi hoặc dữ liệu di động ngay lập tức, có mục đích chặn đứng khả năng mã độc (nếu có) tiếp tục truyền dữ liệu ra ngoài hoặc tải thêm các thành phần độc hại khác về máy – đây là phản xạ tương tự nguyên tắc "cách ly" trong xử lý sự cố an toàn thông tin ở quy mô lớn, chỉ khác là áp dụng ở quy mô một thiết bị cá nhân.

Bước thứ hai, chụp lại toàn bộ bằng chứng trước khi thực hiện bất kỳ hành động nào khác – ảnh chụp màn hình cuộc trò chuyện, đường link đáng ngờ, thông tin tài khoản của đối tượng, thời gian xảy ra sự việc. Đây là bước rất dễ bị bỏ qua vì tâm lý muốn xóa ngay nội dung gây khó chịu hoặc đáng sợ, nhưng lại là bằng chứng quan trọng nhất nếu sau này cần trình báo cơ quan chức năng hoặc nhà trường can thiệp; việc lưu bằng chứng trước khi chặn tài khoản là điều kiện tiên quyết để một vụ việc bắt nạt hay lừa đảo có thể được xử lý đến nơi đến chốn. Một lưu ý rất quan trọng là KHÔNG chụp, sao lưu, hay chuyển tiếp những hình ảnh nhạy cảm của học sinh ra bên ngoài hoặc cho người khác. Bước thứ ba, chặn (block) tài khoản có hành vi xấu và tuyệt đối không phản hồi, không chuyển tiền dưới bất kỳ hình thức nào – nhắc lại đúng nguyên tắc cốt lõi đã phân tích xuyên suốt Chương 3 khi đề cập đến phishing, deepfake và sextortion: một khi đã

chuyển tiền hoặc phản hồi, không có gì bảo đảm đối tượng sẽ dừng lại, trong khi im lặng và chặn tài khoản gần như luôn là lựa chọn an toàn hơn tương tác thêm với đối tượng.

Vì sao thứ tự 3 bước này quan trọng

Một sai lầm phổ biến là thực hiện ngược thứ tự – ví dụ hoảng loạn xóa ngay cuộc trò chuyện hoặc chặn tài khoản trước khi kịp chụp lại bằng chứng, khiến việc trình báo sau này thiếu căn cứ để cơ quan chức năng xử lý.

Ghi nhớ đơn giản theo thứ tự "Ngắt – Lưu – Chặn": ngắt kết nối để cách ly nguy cơ kỹ thuật, lưu bằng chứng trước khi mọi dấu vết biến mất, rồi mới chặn tương tác với đối tượng.

4.2.2. Bước 4–5: Báo cáo và phối hợp

Sau khi đã kiểm soát được tình huống trước mắt, hai bước tiếp theo chuyển trọng tâm từ "tự xử lý" sang "tìm kiếm sự hỗ trợ đúng nơi" – đây cũng là bước mà học sinh dễ bỏ qua nhất vì tâm lý xấu hổ hoặc sợ bị trách mắng. Bước thứ tư, báo ngay cho cha mẹ hoặc một người lớn thực sự tin cậy (có thể là giáo viên chủ nhiệm nếu chưa sẵn sàng nói với gia đình), càng sớm càng tốt, không chờ đến khi "chắc chắn nghiêm trọng" mới lên tiếng; phần lớn thiệt hại nghiêm trọng trong các vụ sextortion hay lừa đảo đến từ việc nạn nhân trì hoãn quá lâu trước khi tìm kiếm sự giúp đỡ.

Bước thứ năm, trình báo qua đúng kênh chính thức tùy theo tính chất sự việc. Với các vấn đề liên quan trực tiếp đến an toàn của trẻ em – bị đe dọa, bắt nạt, có dấu hiệu bị dụ dỗ, xâm hại – Tổng đài điện thoại quốc gia bảo vệ trẻ em (111) là kênh nên được ưu tiên hàng đầu: đây là dịch vụ công miễn phí, hoạt động 24/24 giờ tất cả các ngày trong tuần kể cả lễ, Tết, do Cục Bà mẹ và Trẻ em, Bộ Y tế quản lý, có đội ngũ tư vấn viên chuyên trách và có thể tiếp nhận qua nhiều kênh khác nhau (gọi điện, Zalo 111, ứng dụng App 111, website tongdai111.vn) chứ không chỉ qua điện thoại. Với tình huống có dấu hiệu nguy hiểm về an ninh, trật tự cần can thiệp khẩn cấp, số 113 là đầu mối chung trên toàn quốc. Với các vụ việc liên quan đến lừa đảo qua tin nhắn, cuộc gọi viễn thông, đầu số 156 (gọi hoặc nhắn tin) và 5656 (nhắn tin) do Cục An ninh mạng, Bộ Công an vận hành là kênh tiếp nhận chính thức trên toàn quốc [17]. Ngoài ra, cổng thông tin vncert.vn của Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT) thuộc Cục An ninh mạng, Bộ Công an cũng là một đầu mối trực tuyến hữu ích để phản ánh các sự cố, website giả mạo. Với những vụ việc có dấu hiệu hình sự rõ ràng (lừa đảo chiếm đoạt tài sản, đe dọa tống tiền), gia đình nên đến trực tiếp hoặc liên hệ công an nơi cư trú để được hướng dẫn thủ tục trình báo chính thức. Hình 4.8 minh họa về các kênh hỗ trợ khi gặp sự cố trên không gian mạng.



Hình 4.8. Các kênh trình báo chính thức khi gặp sự cố trên không gian mạng

Song song với việc trình báo cơ quan chức năng, đừng quên báo cáo trực tiếp với chính nền tảng nơi xảy ra sự việc – Zalo, TikTok, Facebook đều có chức năng Report tích hợp sẵn cho phép nền tảng xử lý nhanh việc gỡ nội dung hoặc khóa tài khoản vi phạm, độc lập với quy trình pháp lý có thể mất nhiều thời gian hơn. Với TikTok cụ thể, ngoài chức năng report ngay trên video/tài khoản, nền tảng còn duy trì một Trung tâm an toàn (Safety Center) trực tuyến bằng tiếng Việt, cung cấp hướng dẫn chi tiết cách báo cáo từng loại nội dung – từ bắt nạt, hành vi lạm dụng cho đến tài khoản chưa đủ tuổi sử dụng nền tảng.

4.2.3. Bước 6–7: Phục hồi và phòng ngừa lâu dài

Hai bước cuối cùng thường bị xem nhẹ vì tâm lý muốn "khép lại càng nhanh càng tốt" sau khi vấn đề trước mắt đã tạm ổn, nhưng lại quyết định liệu sự cố có tái diễn hay để lại di chứng lâu dài hay không.

Bước 6. Khôi phục an toàn. Sau khi sự cố trước mắt đã được kiểm soát, cần khôi phục lại trạng thái an toàn cho tài khoản, thiết bị và thông tin của học sinh. Tùy tình huống, việc này có thể gồm thay đổi mật khẩu, kiểm tra tài khoản, điều chỉnh quyền riêng tư, báo cáo nội dung vi phạm hoặc phối hợp với nền tảng và cơ quan có trách nhiệm.

Với sự cố liên quan đến quan hệ xã hội như bắt nạt, giả mạo hoặc đe dọa, "khôi phục" không chỉ là xử lý tài khoản. Nhà trường cần xem xét học sinh có còn phải tiếp

xúc với người gây ra sự việc trong lớp, trong nhóm chat hoặc trong các hoạt động học tập hay không để có biện pháp hỗ trợ phù hợp.

Bước 7. Theo dõi và hỗ trợ sau sự cố. Nhà trường không nên mặc định sự việc đã kết thúc chỉ vì nội dung đã được gỡ, tài khoản đã bị khóa hoặc học sinh vi phạm đã được xử lý.

Giáo viên chủ nhiệm, bộ phận tư vấn hoặc người được giao hỗ trợ nên chủ động hỏi thăm học sinh trong thời gian sau sự cố. Việc theo dõi không cần tạo cảm giác "giám sát", mà nhằm giúp nhà trường nhận biết liệu sự việc có tiếp tục hay không và học sinh có cần thêm sự hỗ trợ hay không.

Có thể trao đổi với học sinh bằng những câu hỏi đơn giản:

- Gần đây sự việc có tiếp tục xảy ra không?

- Em có còn nhận được tin nhắn hoặc nội dung làm em lo lắng không?

- Khi đến trường hoặc tham gia nhóm lớp, em có cảm thấy an toàn không?

- Hiện tại em có cần thầy cô hoặc nhà trường hỗ trợ thêm điều gì không?

Với sự cố nghiêm trọng hoặc kéo dài, nhà trường nên phối hợp với gia đình và bộ phận tư vấn tâm lý học đường; khi vượt quá khả năng xử lý của nhà trường, cần kết nối với cơ quan hoặc dịch vụ hỗ trợ phù hợp.

Sự phối hợp giữa gia đình và nhà trường trong bước 6–7

Gia đình nên chủ động thông báo cho giáo viên chủ nhiệm khi con là nạn nhân của một sự cố nghiêm trọng liên quan đến bạn học hoặc ảnh hưởng đến tâm lý khi đến trường, thay vì chỉ xử lý trong phạm vi gia đình – vì nhà trường có thể cần can thiệp thêm ở khía cạnh quan hệ bạn bè, kỷ luật học đường mà gia đình không thể tự giải quyết.

Ngược lại, nhà trường khi phát hiện dấu hiệu học sinh gặp sự cố trên mạng cũng nên liên hệ gia đình sớm, theo đúng tinh thần phối hợp trách nhiệm đã nêu trong khung pháp lý ở Chương 1 (Điều 34 Nghị định 56/2017/NĐ-CP), thay vì chỉ xử lý nội bộ trong phạm vi lớp học.

4.2.4. Minh họa: áp dụng quy trình 7 bước vào một tình huống cụ thể

(Tình huống minh họa, xây dựng dựa trên kịch bản lừa đảo giả mạo "kết quả thi học kỳ" qua Zalo) để thấy rõ quy trình 7 bước vận hành như thế nào trong thực tế thay vì chỉ dừng lại ở lý thuyết, hãy hình dung lại chính xác tình huống như sau: một tài khoản Zalo Official Account mạo danh trường học gửi thông báo "Kết quả thi học kỳ

đã có, phụ huynh bấm vào đường link để xem điểm", và một phụ huynh, vì nôn nóng, đã bấm vào link và nhập một số thông tin cá nhân của con trước khi kịp nhận ra dấu hiệu bất thường.

Giai đoạn 1 (Bước 1–3): ngay khi nhận ra trang web vừa truy cập có giao diện hơi khác lạ so với cổng thông tin quen thuộc của trường – có thể là logo hơi mờ, đường dẫn (URL) không đúng tên miền của trường – phụ huynh nên lập tức tắt WiFi hoặc dữ liệu di động trên thiết bị vừa dùng để truy cập (Bước 1), để nếu đây thực sự là một trang chứa mã độc, kết nối bị cắt sẽ hạn chế nguy cơ dữ liệu tiếp tục bị truyền đi. Ngay sau đó, chụp lại ảnh màn hình toàn bộ tin nhắn gốc trên Zalo, đường link đã bấm vào và các thông tin đã lỡ nhập (Bước 2) – đây sẽ là bằng chứng quan trọng nếu cần trình báo. Cuối cùng, chặn ngay tài khoản Zalo OA giả mạo đó (Bước 3); nếu trang web có yêu cầu thanh toán một khoản phí nhỏ để "xác nhận", tuyệt đối không thực hiện giao dịch dù số tiền được yêu cầu nhỏ đến đâu.

Giai đoạn 2 (Bước 4–5): phụ huynh nên trao đổi ngay với người còn lại trong gia đình hoặc gọi điện hỏi trực tiếp giáo viên chủ nhiệm qua số điện thoại đã lưu từ trước – không phải số trong tin nhắn giả mạo – để xác nhận nhà trường có thực sự gửi thông báo dạng này hay không (Bước 4). Sau khi xác nhận đây là dấu hiệu lừa đảo, phụ huynh cần lưu lại tin nhắn, địa chỉ website và các thông tin liên quan, báo cáo tài khoản giả mạo đến đầu số 156/5656 của Cục An ninh mạng, Bộ Công an, đồng thời trình báo cơ quan Công an nơi gần nhất nếu có dấu hiệu chiếm đoạt tài sản hoặc thu thập trái phép thông tin cá nhân. Có thể sử dụng Cổng tra cứu thông tin tên miền tại tracuutenmien.gov.vn của Bộ Khoa học và Công nghệ để kiểm tra thông tin tên miền. Nếu nghi ngờ thiết bị hoặc hệ thống gặp sự cố an ninh mạng, có thể tham khảo kênh hỗ trợ của VNCERT tại vncert.vn (Bước 5).

Giai đoạn 3 (Bước 6–7): nếu nghi ngờ thiết bị đã bị cài mã độc, nên sao lưu các dữ liệu quan trọng (ảnh, danh bạ) sang Google Drive hoặc iCloud, sau đó có thể cân nhắc khôi phục cài đặt gốc thiết bị nếu phần mềm bảo mật xác nhận có mã độc, rồi cài đặt lại từ bản sao lưu sạch; đồng thời đổi mật khẩu của tài khoản Zalo và bất kỳ tài khoản nào khác dùng chung mật khẩu (Bước 6). Cuối cùng, gia đình nên dành một buổi trò chuyện ngắn với con – không phải để trách móc mà để cùng rút kinh nghiệm: "Lần sau nếu thấy tin nhắn báo điểm thi, mình sẽ luôn gọi hỏi lại cô giáo trước khi bấm vào link nhé" – biến trải nghiệm không mong muốn này thành một lần thực hành cụ thể cho nguyên tắc "Dừng – Nghĩ – Kiểm tra" đã học ở Chương 2 (Bước 7).

Ví dụ trên cho thấy một đặc điểm quan trọng của quy trình 7 bước: phần lớn thời gian và công sức không nằm ở các thao tác kỹ thuật phức tạp, mà nằm ở việc giữ đúng thứ tự hành động và không bỏ sót bước nào – đặc biệt là hai bước dễ bị bỏ qua nhất trong tâm lý hoảng loạn thực tế: chụp bằng chứng trước khi chặn (Bước 2–3), và rút kinh nghiệm sau khi mọi thứ đã ổn định (Bước 7).

4.2.5. Bài học kinh nghiệm sau khi giải quyết sự cố

Sau khi tư vấn và xử lý sự cố, cần làm gì? Việc hỗ trợ học sinh không nên kết thúc ngay khi sự cố trên mạng đã được xử lý. Sau tư vấn, giáo viên, nhà trường và gia đình nên cùng học sinh nhìn lại sự việc một cách bình tĩnh, xác định điều gì đã xảy ra, dấu hiệu nào có thể nhận biết sớm hơn và cách xử lý nào đã giúp bảo đảm an toàn. Từ đó, học sinh rút ra bài học kinh nghiệm phù hợp với lứa tuổi, chẳng hạn biết dừng lại trước khi bấm vào liên kết lạ, kiểm tra người gửi, bảo vệ thông tin cá nhân, chặn và báo cáo khi bị làm phiền, hoặc tìm người lớn hỗ trợ sớm hơn. Đồng thời, cần kiểm tra xem học sinh có còn lo lắng, sợ hãi, né tránh bạn bè, nhóm lớp hoặc nền tảng từng xảy ra sự cố hay không để tiếp tục hỗ trợ khi cần. Với những trường hợp nhạy cảm, nhà trường cần giữ kín thông tin, tôn trọng quyền riêng tư và tránh nhắc lại sự việc trước tập thể. Mục tiêu cuối cùng không chỉ là "giải quyết xong một sự cố", mà là giúp học sinh hiểu điều đã xảy ra, lấy lại cảm giác an toàn và biết cách tự bảo vệ tốt hơn trong những lần sử dụng Internet sau này. Hình 4.9 sau minh họa về những việc cần làm sau khi tư vấn và giải quyết sự cố.



Hình 4.9. Bài học kinh nghiệm sau khi tư vấn giải quyết sự cố

4.3. Kết luận chương

An toàn trên môi trường mạng không chỉ là biết cách phòng tránh rủi ro, mà còn là biết phải làm gì khi sự cố thực sự xảy ra. Các biện pháp kỹ thuật, sự đồng hành của gia đình và giáo dục kỹ năng tại nhà trường đều có vai trò quan trọng và cần hỗ trợ lẫn nhau. Công cụ có thể giúp giảm nguy cơ, nhưng chính kiến thức, kỹ năng và thói quen an toàn mới giúp học sinh chủ động bảo vệ mình trong quá trình sử dụng Internet.

Quy trình 7 bước ở mục 4.2 vì thế không nên được hiểu là một danh sách phải ghi nhớ máy móc. Điều quan trọng hơn là hình thành cách ứng phó đúng khi gặp sự cố: bình tĩnh, dừng hành động có nguy cơ, bảo vệ tài khoản và thông tin cá nhân, lưu lại bằng chứng khi cần, báo cho người tin cậy và tìm kiếm sự hỗ trợ phù hợp. Xử lý sớm và đúng cách có thể giúp hạn chế thiệt hại và ngăn sự việc trở nên nghiêm trọng hơn.

Đồng thời, xây dựng môi trường mạng an toàn không phải trách nhiệm của riêng học sinh. Gia đình cần đồng hành, nhà trường cần hướng dẫn và hỗ trợ, còn học sinh cần chủ động thực hành những kỹ năng đã được trang bị. Khi ba bên cùng phối hợp, những nguyên tắc ở Chương 2, kiến thức về rủi ro ở Chương 3 và kỹ năng ứng phó ở Chương 4 sẽ trở thành một hệ thống thống nhất: biết để phòng tránh – nhận ra để cảnh giác – bình tĩnh để xử lý – chủ động tìm sự hỗ trợ khi cần.

Mục tiêu cuối cùng không phải là tránh xa Internet, mà là giúp mỗi học sinh sử dụng công nghệ an toàn, tự tin, có trách nhiệm và biết tự bảo vệ mình trong môi trường số.

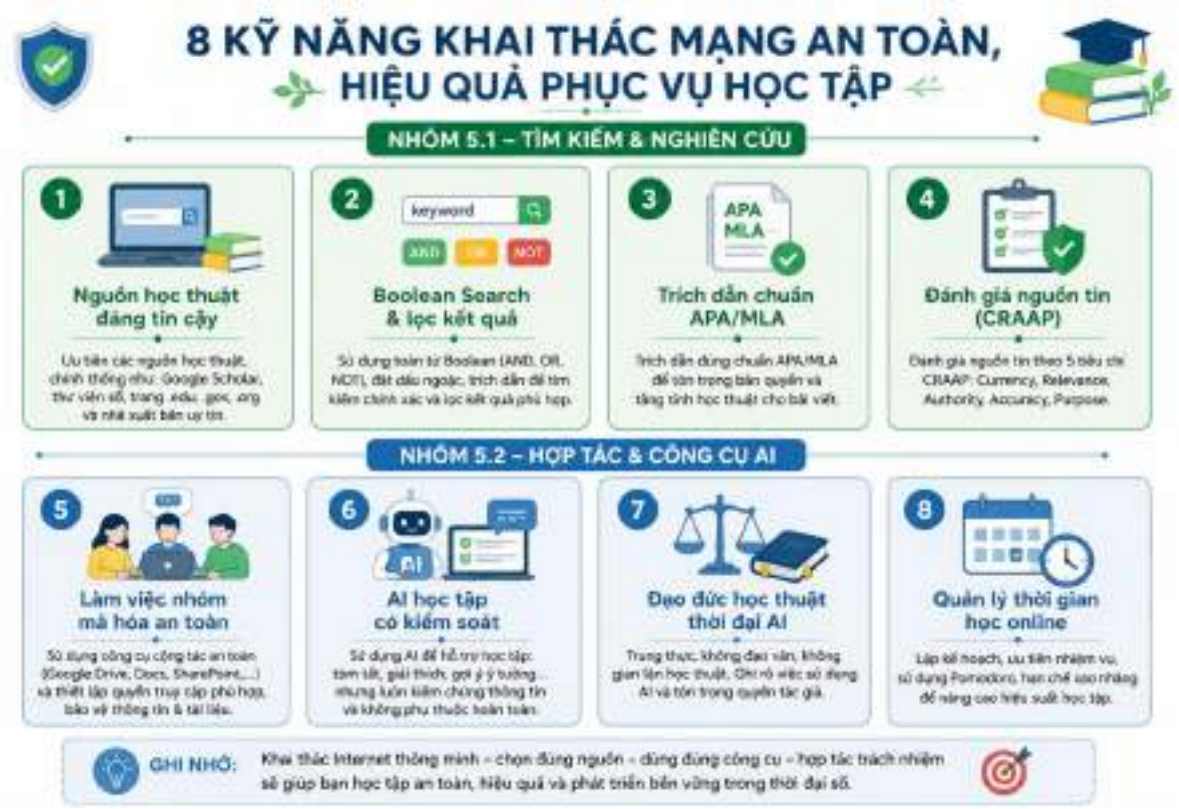
CHƯƠNG 5. MỘT SỐ KỸ NĂNG KHAI THÁC MẠNG AN TOÀN, HIỆU QUẢ PHỤC VỤ HỌC TẬP

Ở các chương trước, học sinh đã được tìm hiểu những nguyên tắc sử dụng mạng an toàn, cách nhận biết rủi ro, phòng tránh và ứng phó khi gặp sự cố. Tuy nhiên, an toàn không phải là mục tiêu duy nhất khi sử dụng Internet. Môi trường số còn mở ra nhiều cơ hội để học sinh tìm kiếm kiến thức, tự học, trao đổi với bạn bè, sáng tạo nội dung và tiếp cận những công cụ hỗ trợ học tập ngày càng phong phú.

Vì vậy, bên cạnh việc biết tự bảo vệ mình, học sinh cũng cần biết khai thác Internet một cách hiệu quả và có trách nhiệm. Một kết quả tìm kiếm xuất hiện đầu tiên chưa chắc đã chính xác; một câu trả lời do AI tạo ra chưa chắc đã đáng tin cậy; và việc có rất nhiều tài liệu trong tay cũng chưa chắc giúp học tốt nếu không biết lựa chọn, kiểm chứng và sử dụng thông tin đúng cách. Trong môi trường số, điều quan trọng không chỉ là "tìm được thông tin", mà còn là "biết thông tin nào đáng tin và sử dụng thông tin đó như thế nào".

Chương 5 vì thế tập trung vào hai nhóm kỹ năng thiết thực. Mục 5.1 hướng dẫn học sinh tìm kiếm, đánh giá, lựa chọn và trích dẫn thông tin phục vụ học tập. Mục 5.2 hướng dẫn cách học tập, hợp tác trên môi trường số và sử dụng các công cụ AI một cách phù hợp, đồng thời biết quản lý thời gian để công nghệ thực sự hỗ trợ thay vì làm gián đoạn việc học. Ngoài ra chương này cũng hướng dẫn cách sử dụng kỹ thuật soạn thảo câu lệnh khi sử dụng AI và tích hợp 8 kỹ năng trong một tuần học và làm việc hiệu quả trong phần 5.3 và 5.4.

Thông qua những kỹ năng này, học sinh từng bước chuyển từ "sử dụng Internet an toàn" sang "sử dụng Internet an toàn, thông minh và hiệu quả", biết tìm kiếm tri thức, biết kiểm chứng, biết sử dụng công cụ số đúng mục đích và chủ động chịu trách nhiệm với cách mình sử dụng công nghệ.



Hình 5.1. Tổng quan 8 kỹ năng khai thác mạng an toàn, hiệu quả phục vụ học tập

5.1. Kỹ năng tìm kiếm, đánh giá và sử dụng thông tin

Internet giúp học sinh có thể tìm kiếm thông tin cho một bài tập, một câu hỏi hay một chủ đề mình quan tâm chỉ trong vài giây. Tuy nhiên, có nhiều thông tin không có nghĩa là tất cả đều đúng và đáng tin cậy. Cùng một câu hỏi, công cụ tìm kiếm có thể trả về hàng nghìn kết quả từ cơ quan nhà nước, trường đại học, báo chí, sách điện tử, diễn đàn, mạng xã hội, video cá nhân hoặc nội dung do AI tạo ra. Nếu chỉ chọn kết quả xuất hiện đầu tiên hoặc bài viết có nhiều lượt xem, học sinh rất dễ sử dụng phải thông tin thiếu chính xác, lỗi thời hoặc không phù hợp với mục đích học tập.

Vì vậy, kỹ năng tìm kiếm trên Internet không đơn giản là "gõ từ khóa rồi chọn một kết quả". Học sinh cần biết mình đang tìm thông tin gì, nên tìm ở đâu, sử dụng từ khóa như thế nào và quan trọng hơn là biết kiểm tra thông tin tìm được trước khi sử dụng. Khi gặp một bài viết, hình ảnh, video hay câu trả lời do AI cung cấp, các em nên hình thành thói quen đặt câu hỏi: Ai cung cấp thông tin này? Thông tin được công bố khi nào? Có bằng chứng hoặc nguồn dẫn hay không? Có thể kiểm tra lại ở nguồn khác không?

Nội dung trong phần này tập trung vào bốn kỹ năng giúp học sinh từng bước thực hiện quá trình đó. Trước hết là *Nhận diện và lựa chọn nguồn thông tin đáng tin cậy*.

Tiếp theo là *Sử dụng từ khóa và các kỹ thuật tìm kiếm nâng cao* để tìm đúng thông tin cần thiết thay vì mất thời gian giữa quá nhiều kết quả. Sau khi tìm được tài liệu, học sinh cần Đánh giá độ tin cậy của nguồn bằng những tiêu chí rõ ràng, thay vì chỉ dựa vào cảm giác hoặc số lượt xem. Cuối cùng là Ghi nguồn và trích dẫn đúng cách, thể hiện sự tôn trọng đối với người tạo ra thông tin và giúp người đọc có thể kiểm tra lại nguồn đã sử dụng.

Bốn kỹ năng này tạo thành một quá trình đơn giản nhưng rất quan trọng:

TÌM ĐÚNG → KIỂM TRA → LỰA CHỌN → SỬ DỤNG VÀ GHI NGUỒN

Khi hình thành được thói quen này, học sinh không chỉ tìm kiếm thông tin nhanh hơn mà còn từng bước biết tự học, kiểm chứng thông tin và sử dụng tri thức trên Internet một cách có trách nhiệm.

5.1.1. Nhận diện và lựa chọn nguồn thông tin đáng tin cậy

Internet giúp học sinh tìm được rất nhiều thông tin chỉ trong thời gian ngắn. Tuy nhiên, không phải thông tin nào xuất hiện trên mạng cũng đúng. Một bài viết có nhiều lượt xem, một video được chia sẻ nhiều lần hoặc một câu trả lời xuất hiện đầu tiên trên công cụ tìm kiếm vẫn có thể sai, đã cũ hoặc không phù hợp với nội dung đang học.

Vì vậy, trước khi sử dụng một thông tin, học sinh nên dành ít phút để kiểm tra nguồn. Có thể bắt đầu bằng bốn câu hỏi đơn giản:

a. Ai cung cấp thông tin?

Hãy xem bài viết, video hoặc tài liệu do ai tạo ra. Những nguồn như cơ quan nhà nước, nhà trường, giáo viên, sách giáo khoa, trường đại học, viện nghiên cứu hoặc tổ chức có uy tín thường đáng tin cậy hơn những bài đăng không ghi rõ tác giả.

b. Thông tin được đăng khi nào?

Một số thông tin có thể đúng trước đây nhưng không còn phù hợp ở thời điểm hiện tại, đặc biệt là thông tin về pháp luật, công nghệ, sức khỏe, tuyển sinh hoặc các sự kiện đang diễn ra. Vì vậy, cần chú ý ngày đăng hoặc ngày cập nhật.

c. Thông tin có căn cứ không?

Nguồn đáng tin cậy thường cho biết thông tin được lấy từ đâu, có số liệu, tài liệu tham khảo hoặc dẫn đến nguồn gốc để người đọc kiểm tra lại. Nếu một bài viết chỉ khẳng định "nghe nói", "nhiều người cho rằng" hoặc đưa ra con số nhưng không nói nguồn ở đâu, học sinh cần thận trọng.

d. Có thể kiểm tra lại ở nguồn khác không?

Khi thông tin quan trọng hoặc còn nghi ngờ, không nên chỉ dựa vào một nguồn. Hãy đối chiếu với sách giáo khoa, tài liệu của giáo viên, trang thông tin chính thức hoặc một nguồn đáng tin cậy khác. Nếu vẫn chưa chắc chắn, nên hỏi giáo viên hoặc người lớn.

e. Nên ưu tiên nguồn nào?

Khi học tập, học sinh có thể ưu tiên theo thứ tự đơn giản sau:

- Sách giáo khoa, tài liệu của giáo viên và nhà trường
- Cơ quan nhà nước, trường đại học, tổ chức chuyên môn
- Báo chí và nền tảng giáo dục có nguồn rõ ràng
- Các trang tổng hợp, diễn đàn và mạng xã hội

Điều này không có nghĩa mọi thông tin trên mạng xã hội hoặc diễn đàn đều sai. Tuy nhiên, những nguồn này thường do cá nhân đăng tải và có thể chưa được kiểm tra, vì vậy cần đối chiếu trước khi sử dụng.

f. Phù hợp với từng cấp học

Với học sinh tiểu học, khi chưa biết một trang web hoặc thông tin có đáng tin hay không, các em nên ưu tiên tài liệu do thầy cô, nhà trường hoặc cha mẹ hướng dẫn. Không nên tự ý làm theo những nội dung lạ chỉ vì thấy nhiều người chia sẻ.

Với học sinh THCS, ngoài việc xem ai là người cung cấp thông tin, các em nên chú ý thời gian đăng, nguồn dẫn và kiểm tra lại ở ít nhất một nguồn khác khi thông tin quan trọng hoặc có vẻ bất thường.

Với học sinh THPT, đặc biệt khi làm bài thuyết trình, dự án hoặc nghiên cứu, cần kiểm tra kỹ tác giả, cơ quan xuất bản, thời gian công bố, số liệu và tài liệu tham khảo. Với thông tin học thuật, nên ưu tiên bài báo khoa học, sách, báo cáo của cơ quan chuyên môn hoặc tài liệu từ trường đại học và viện nghiên cứu.

Bảng 5.1 minh họa về các loại nguồn và mức độ tin cậy cũng như cách sử dụng phù hợp cho học sinh.

Một nguyên tắc đơn giản có thể áp dụng khi lựa chọn nguồn là:

Ưu tiên nguồn rõ tác giả → rõ đơn vị xuất bản → có thời gian công bố → có bằng chứng hoặc tài liệu tham khảo → có thể kiểm tra lại ở nguồn khác.

Khi chưa chắc chắn một thông tin có đáng tin hay không, cách an toàn nhất là đối chiếu ít nhất với một nguồn có uy tín khác hoặc hỏi giáo viên trước khi sử dụng.

Bảng 5.1. Bảng dữ liệu nguồn và mức độ tin cậy

Loại nguồn	Mức độ tin cậy	Cách sử dụng phù hợp
Thư viện số / học liệu điện tử của trường	Rất cao	Ưu tiên tham khảo đầu tiên vì bám sát chương trình đang học
hocmai.vn, Viettel Study, VioEdu.vn, violympic.vn, olm.vn, ioe.vn	Cao	Học bài mới, ôn tập, luyện đề có lời giải chi tiết, đã qua biên soạn chuyên môn

5.1.2. Sử dụng từ khóa và các kỹ thuật tìm kiếm nâng cao

Khi cần tìm thông tin trên Internet, cách đặt từ khóa hoặc câu hỏi có ảnh hưởng rất lớn đến kết quả nhận được. Nếu tìm quá chung chung, học sinh có thể nhận được rất nhiều kết quả không cần thiết. Ngược lại, nếu xác định rõ điều mình muốn biết và sử dụng những từ quan trọng, việc tìm kiếm sẽ nhanh và chính xác hơn.

Một cách đơn giản là thực hiện theo bốn bước:

XÁC ĐỊNH CẦN TÌM → CHỌN TỪ KHÓA → ĐIỀU CHỈNH KẾT QUẢ → KIỂM TRA NGUỒN

a. Bắt đầu bằng những từ quan trọng

Trước khi tìm kiếm, học sinh nên nghĩ xem mình thực sự cần thông tin gì và chọn những từ thể hiện rõ nhất nội dung đó.

Ví dụ, thay vì tìm:

"Em muốn biết về ô nhiễm môi trường."

có thể tìm cụ thể hơn:

"Nguyên nhân ô nhiễm không khí"

hoặc

"ô nhiễm không khí Việt Nam học sinh".

Nếu kết quả chưa phù hợp, có thể thêm hoặc thay đổi từ khóa. Chẳng hạn, thêm tên môn học, lớp, địa điểm, năm hoặc loại tài liệu cần tìm.

Điều quan trọng là không cần gõ một câu thật dài. Hãy bắt đầu bằng những từ chính, xem kết quả rồi điều chỉnh dần. Đối với học sinh tiểu học, cha mẹ hoặc thầy cô nên hỗ trợ trực tiếp, và trao đổi với các em học sinh để xem các em suy nghĩ, sau đó hỏi và cùng tìm được từ khóa mà các em mong muốn.

b. Thu hẹp kết quả khi cần

Với học sinh lớn hơn, đặc biệt là THCS và THPT, một số cách tìm đơn giản có thể giúp giảm bớt kết quả không liên quan.

- Đặt một cụm từ trong dấu ngoặc kép "..." khi muốn tìm đúng cụm từ đó. Ví dụ: "an toàn trên mạng".

- Dùng site: khi muốn tìm thông tin trong một trang hoặc một nhóm trang nhất định.
Ví dụ: "an toàn mạng" site:gov.vn để ưu tiên kết quả từ các trang cơ quan nhà nước.

- Dùng filetype:pdf khi cần tìm tài liệu dạng PDF. Ví dụ: "an toàn mạng cho học sinh" filetype:pdf.

Học sinh không cần nhớ nhiều cú pháp. Chỉ nên sử dụng những cách này khi chúng thực sự giúp việc tìm kiếm dễ hơn.

c. Tìm kiếm với sự hỗ trợ của AI

Ngoài công cụ tìm kiếm thông thường, học sinh có thể sử dụng AI để hỗ trợ tìm thông tin. Khi hỏi AI, nên nói rõ mình cần gì thay vì đặt câu hỏi quá chung chung.

Ví dụ:

"Hãy giải thích ba nguyên nhân chính gây ô nhiễm không khí cho học sinh lớp 6 và gợi ý nguồn để em kiểm tra lại."

Hoặc:

"Em cần tìm tài liệu về biến đổi khí hậu để làm bài thuyết trình lớp 10. Hãy gợi ý các từ khóa và những loại nguồn đáng tin cậy nên tìm."

AI đặc biệt hữu ích khi học sinh chưa biết nên bắt đầu tìm bằng từ khóa nào, muốn thu hẹp một chủ đề hoặc muốn được gợi ý những khía cạnh cần tìm hiểu thêm.

Tuy nhiên, AI không thay thế việc tìm và kiểm tra nguồn. Nếu AI đưa ra một con số, sự kiện, trích dẫn hoặc đường dẫn, học sinh cần mở nguồn gốc và kiểm tra trước khi sử dụng. Không nên ghi vào bài chỉ vì AI trả lời nghe có vẻ hợp lý.

d. Cách tìm kiếm phù hợp với từng cấp học

Với học sinh tiểu học, nên bắt đầu bằng những từ khóa ngắn, rõ ràng và ưu tiên các trang, tài liệu do giáo viên hoặc cha mẹ hướng dẫn. Khi sử dụng AI để tìm hoặc giải thích thông tin, nên có sự hướng dẫn của người lớn.

Ví dụ:

"vòng đời của bướm"

"cách tiết kiệm nước cho học sinh".

Với học sinh THCS, có thể kết hợp nhiều từ khóa để làm rõ điều cần tìm và bước đầu sử dụng dấu ngoặc kép hoặc giới hạn nguồn. Các em cũng có thể nhờ AI gợi ý từ khóa, giải thích khái niệm hoặc đề xuất nguồn để tiếp tục tìm hiểu.

Ví dụ:

"tác hại rác thải nhựa" học sinh

hoặc hỏi AI:

"Gợi ý cho em 5 từ khóa để tìm tài liệu về tác hại của rác thải nhựa."

Với học sinh THPT, khi làm bài thuyết trình, dự án hoặc nghiên cứu, có thể sử dụng thêm các cách tìm như site:, filetype: hoặc công cụ tìm kiếm tài liệu học thuật. AI có thể hỗ trợ tạo từ khóa, so sánh các hướng tìm kiếm, tóm tắt nội dung ban đầu hoặc gợi ý nguồn, nhưng học sinh vẫn phải đọc và kiểm tra tài liệu gốc trước khi trích dẫn.

e. Điều cần nhớ

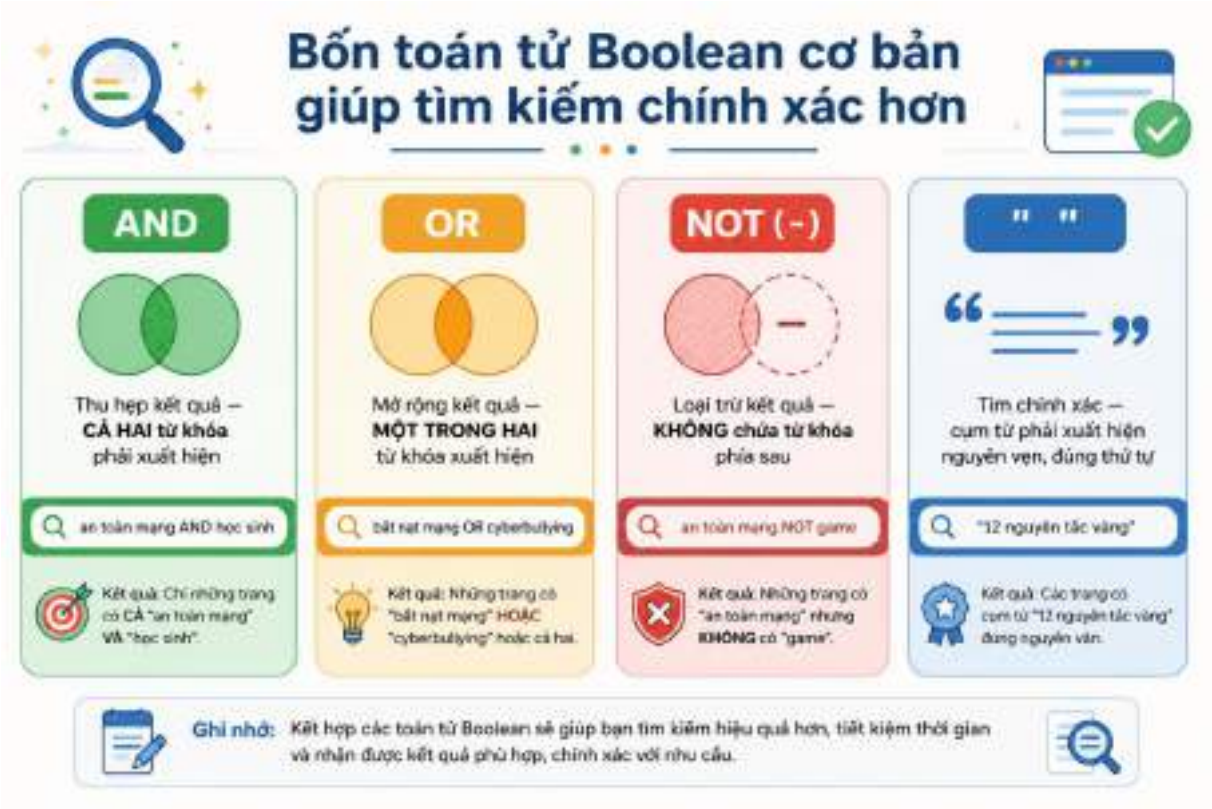
Tìm kiếm tốt không phải là tìm thật nhiều, mà là tìm đúng thông tin mình cần.

Hãy nhớ:

HỎI RÕ → TÌM ĐÚNG → ĐIỀU CHỈNH → KIỂM TRA

Kết quả xuất hiện đầu tiên chưa chắc là kết quả tốt nhất. Câu trả lời của AI cũng chưa chắc đúng. Trước khi sử dụng thông tin cho bài học, hãy xem nguồn và kiểm tra lại.

Điều quan trọng cần nhớ là tìm kiếm tốt không phải là gõ thật nhiều từ, mà là biết mình cần tìm gì và điều chỉnh từ khóa để từng bước tiến gần đến nguồn phù hợp nhất. Sau khi tìm được tài liệu, học sinh vẫn cần áp dụng các kỹ năng đánh giá nguồn ở mục tiếp theo trước khi tin tưởng và sử dụng thông tin. Hình 5.2 minh họa các phép tìm kiếm cơ bản giúp tìm kiếm chính xác hơn.



Hình 5.2. Bốn toán tử Boolean cơ bản và cách áp dụng vào tìm kiếm học thuật

Ví dụ minh họa: khi một học sinh muốn tìm tài liệu học thuật về an toàn mạng dành riêng cho đối tượng học sinh, nhưng không muốn kết quả bị lẫn với các bài viết về an toàn trong game trực tuyến (một chủ đề khác dùng chung nhiều từ khóa), câu truy vấn "an toàn mạng" AND "học sinh" NOT "game" sẽ giúp Google ưu tiên các trang có đồng thời hai cụm từ đầu (nhờ dấu ngoặc kép giữ nguyên cụm từ thay vì tách rời từng chữ) và loại bớt các trang có nhắc đến từ "game". Cần lưu ý một chi tiết kỹ thuật quan trọng: trên Google hiện nay, toán tử NOT thường được thể hiện bằng dấu trừ đứng liền trước từ khóa (ví dụ -game) thay vì gõ chữ NOT, và toán tử AND thường không cần gõ ra vì Google mặc định yêu cầu tất cả từ khóa đều xuất hiện. Điều thực sự tạo ra khác biệt lớn nhất trong tìm kiếm hằng ngày chính là cặp dấu ngoặc kép để giữ nguyên cụm từ và dấu trừ để loại trừ – hai công cụ đơn giản nhưng thường bị bỏ qua.

Bên cạnh các toán tử cơ bản, trang Advanced Search (google.com/advanced_search) cung cấp một giao diện với các trường nhập liệu tách riêng, giúp người dùng không cần nhớ cú pháp mà vẫn tận dụng được sức mạnh tìm kiếm nâng cao: giới hạn theo một trang web hoặc tên miền cụ thể (ví dụ chỉ tìm trong các trang có đuôi .edu.vn – thường là các cơ sở giáo dục), giới hạn theo định dạng tệp (ví dụ chỉ tìm tệp PDF, thường là tài liệu chính thức hơn so với một bài đăng blog), hoặc giới hạn theo khoảng thời gian bài viết được đăng – rất hữu ích khi cần tài liệu "mới nhất" thay vì một bài viết đã lỗi thời nhiều năm nhưng vẫn xếp hạng cao vì nhiều lượt truy cập cũ.

Bộ bốn toán tử tìm kiếm cơ bản nên nhớ

AND: dùng khi muốn kết quả chứa đồng thời các từ khóa đã cho. Ví dụ: an toàn mạng AND học sinh giúp tập trung vào các trang có nội dung liên quan đến cả "an toàn mạng" và "học sinh". Trên Google, AND thường có thể được lược bỏ vì công cụ tìm kiếm mặc định kết hợp các từ khóa.

OR: dùng khi muốn tìm một trong hai hoặc nhiều từ khóa tương đương. Ví dụ: bắt nạt mạng OR cyberbullying giúp mở rộng kết quả với cả thuật ngữ tiếng Việt và tiếng Anh.

NOT hoặc dấu trừ (-): dùng để loại bỏ kết quả chứa từ khóa không mong muốn. Trên Google, nên dùng dấu trừ đứng liền trước từ khóa, ví dụ: "an toàn mạng" -game.

Dấu ngoặc kép "...": dùng để tìm chính xác một cụm từ theo đúng thứ tự. Ví dụ: "Bộ Quy tắc ứng xử về bảo vệ trẻ em trên môi trường mạng" giúp thu hẹp kết quả vào đúng cụm từ cần tìm.

Ngoài bốn toán tử cơ bản đã giới thiệu, một số toán tử khác tuy ít được biết đến hơn nhưng rất hữu ích cho việc tìm tài liệu học thuật cụ thể được minh họa trong Bảng 5.2:

Bảng 5.2. Bảng mở rộng các toán tử tìm kiếm nâng cao khác

Toán tử	Cú pháp ví dụ	Công dụng
filetype:	đề thi thử hóa học filetype:pdf	Chỉ trả về kết quả là tệp PDF – thường là tài liệu chính thức, đề thi, giáo trình hơn là bài blog
site:	vật lý 12 site:violet.vn	Giới hạn tìm kiếm trong phạm vi một website hoặc một loại tên miền (ví dụ site:edu.vn)

Toán tử	Cú pháp ví dụ	Công dụng
intitle:	intitle:"an toàn mạng"	Chỉ trả về các trang có cụm từ xuất hiện ngay trong tiêu đề bài viết – dấu hiệu bài viết tập trung đúng chủ đề
*	12 nguyên tắc * an toàn mạng	Dùng như một "chỗ trống" khi không nhớ chính xác một từ trong cụm từ cần tìm.

Ví dụ minh họa quy trình tìm kiếm kết hợp nhiều toán tử: giả sử một học sinh cần tìm đề thi thử tốt nghiệp THPT môn Hóa học năm gần nhất, dạng tệp PDF để có thể tải về luyện offline, đồng thời muốn loại bỏ các trang rao bán tài liệu có phí. Một câu truy vấn kết hợp có thể là: "đề thi thử tốt nghiệp THPT" Hóa học 2026 filetype:pdf -bán -phí. Cách xây dựng câu truy vấn này cho thấy tư duy cốt lõi của tìm kiếm nâng cao: bắt đầu từ cụm từ chính xác nhất (dùng ngoặc kép), thêm bộ lọc định dạng (filetype:), rồi loại trừ các nhiễu đã biết trước (dấu trừ) – thay vì gõ một câu hỏi dài bằng ngôn ngữ tự nhiên và hy vọng công cụ tìm kiếm tự hiểu đúng ý định.

5.1.3. Đánh giá độ tin cậy của nguồn

Trích dẫn nguồn không đơn thuần là một yêu cầu hình thức để "cho đẹp" bài viết, mà là nguyên tắc cốt lõi của liêm chính học thuật: cho phép người đọc truy ngược lại nguồn gốc của một thông tin hay lập luận, đồng thời phân định rõ đâu là ý tưởng của người viết và đâu là ý tưởng được kế thừa từ người khác. Hai chuẩn trích dẫn phổ biến nhất mà học sinh THPT có thể gặp là APA (American Psychological Association), thường dùng trong các môn khoa học xã hội, tâm lý học, giáo dục, và MLA (Modern Language Association), thường dùng trong các môn ngôn ngữ, văn học. Về cấu trúc, khác biệt cơ bản dễ nhận thấy nhất là cách trích dẫn trong ngoặc đơn ngay trong bài viết: APA ưu tiên định dạng (Tên tác giả, năm xuất bản) – nhấn mạnh tính thời sự của nguồn, trong khi MLA ưu tiên định dạng (Tên tác giả, số trang) – nhấn mạnh vị trí chính xác của thông tin được trích dẫn trong toàn văn.

Đối với một trang web – loại nguồn phổ biến nhất mà học sinh sử dụng khi tự học qua mạng – thông tin tối thiểu cần ghi lại để trích dẫn đầy đủ, bất kể theo chuẩn nào, bao gồm: tên tác giả hoặc tên tổ chức chịu trách nhiệm nội dung, tiêu đề bài viết, tên trang web, ngày đăng hoặc ngày cập nhật gần nhất, và đường dẫn URL đầy đủ; với các trang không ghi rõ ngày đăng, nên bổ sung thêm ngày mà bản thân người viết truy cập trang đó ("ngày truy cập"), vì nội dung trên Internet có thể thay đổi hoặc bị gỡ bỏ theo

thời gian mà một tài liệu in không gặp phải vấn đề này. Bảng 5.3 minh họa về các yếu tố trong chuẩn APA và MLA.

Bảng 5.3. Các yếu tố của chuẩn APA và chuẩn MLA

Yếu tố	Chuẩn APA (bản 7)	Chuẩn MLA (bản 9)
Trích dẫn trong ngoặc đơn	(Tên tác giả, năm) – ví dụ (Nguyễn, 2026)	(Tên tác giả số trang) – ví dụ (Nguyễn 25)
Thứ tự trong danh mục tham khảo	Tác giả. (Năm). Tiêu đề. Tên trang web. URL	Tác giả. "Tiêu đề." Tên trang web, ngày đăng, URL
Trọng tâm nhấn mạnh	Tính thời sự của nguồn (năm xuất bản đặt ngay sau tên tác giả)	Vị trí của thông tin trong toàn văn (số trang, nếu có)
Môn học thường sử dụng	Khoa học xã hội, tâm lý học, giáo dục	Ngôn ngữ, văn học



Hình 5.3. Quy trình thu thập và trích dẫn tài liệu tự động bằng Zotero

Việc ghi nhớ thủ công toàn bộ thông tin nói trên cho hàng chục nguồn tài liệu trong một bài nghiên cứu dài là không thực tế, và đây chính là lúc Zotero phát huy giá trị. Zotero là phần mềm quản lý tài liệu tham khảo miễn phí và mã nguồn mở, hoạt động dưới dạng tiện ích mở rộng trình duyệt: khi đang xem một trang tài liệu, bài báo hay sách điện tử, chỉ cần bấm vào biểu tượng Zotero trên thanh công cụ, phần mềm sẽ tự động nhận diện và lưu lại các trường thông tin cần thiết (tác giả, tiêu đề, năm, nguồn) vào thư viện cá nhân mà không cần nhập tay. Khi viết bài trên Microsoft Word, LibreOffice hoặc Google Docs, một tiện ích bổ sung của Zotero cho phép chèn trực tiếp trích dẫn trong ngoặc đơn vào đúng vị trí con trỏ, đồng thời tự động sinh ra danh mục tài liệu tham khảo hoàn chỉnh ở cuối bài – và quan trọng hơn, nếu người viết đổi từ chuẩn APA sang MLA (hoặc ngược lại) sau khi đã viết xong, Zotero có thể định dạng lại toàn bộ trích dẫn chỉ bằng một thao tác chọn chuẩn mới, thay vì phải sửa tay từng vị trí. Hình 5.3 minh họa quy trình thu thập và trích dẫn tài liệu tự động bằng Zotero.

Bên cạnh trích dẫn đúng chuẩn, việc tự kiểm tra bài viết của mình trước khi nộp cũng là một bước nên có, đặc biệt khi bài viết có sử dụng nhiều đoạn diễn giải lại từ tài liệu tham khảo. Grammarly là công cụ hỗ trợ viết được nhiều học sinh, sinh viên sử dụng, nhưng cần lưu ý một điểm quan trọng để tránh hiểu nhầm: gói miễn phí của Grammarly chỉ bao gồm kiểm tra ngữ pháp, chính tả, dấu câu và một số gợi ý về văn phong cơ bản – tính năng kiểm tra đạo văn (plagiarism checker), vốn cần so khớp nội dung với hàng tỷ trang web để phát hiện đoạn trùng lặp, hiện chỉ có trong gói trả phí (Grammarly Pro). Đây là một điều chỉnh cần thiết so với một số tài liệu tuyên truyền vẫn giới thiệu tính năng này như một phần của bản miễn phí.

Vậy học sinh nên tự kiểm tra đạo văn bằng cách nào khi không có công cụ trả phí?

Cách hiệu quả và miễn phí nhất vẫn là phương pháp thủ công nhưng đáng tin cậy: sau khi diễn giải lại một đoạn tài liệu tham khảo, gấp nguồn gốc lại và tự viết lại hoàn toàn bằng lời của mình thay vì chỉnh sửa vài từ trong câu gốc – đây cũng là kỹ năng liêm chính học thuật thực chất hơn nhiều so với việc chỉ chạy qua một công cụ dò trùng lặp.

Nhiều trường đại học tại Việt Nam có cấp quyền truy cập Turnitin – công cụ kiểm tra đạo văn chuyên dụng cho môi trường học thuật – cho sinh viên của trường; học sinh THPT có dự định học lên cao có thể tìm hiểu thêm qua thư viện trường đại học ở địa phương nếu cần kiểm tra một bài viết quan trọng.

Dù dùng công cụ nào, cũng nên nhớ nguyên tắc: bản thân công cụ dò đạo văn không phải "giấy thông hành" tuyệt đối – một đoạn văn có thể vượt qua công cụ dò trùng lặp về mặt

câu chữ nhưng vẫn vi phạm liêm chính học thuật nếu ý tưởng cốt lõi được lấy từ người khác mà không ghi công.

5.1.4. Ghi nguồn và trích dẫn đúng cách

Tìm được thông tin chưa có nghĩa là thông tin đó đã đủ đáng tin để sử dụng. Trên Internet, một trang web được thiết kế chuyên nghiệp, một video có nhiều lượt xem hay một bài viết được chia sẻ rộng rãi vẫn có thể chứa thông tin thiếu chính xác, lỗi thời hoặc chỉ phản ánh quan điểm của người tạo nội dung. Vì vậy, học sinh cần biết kiểm tra nguồn trước khi tin và sử dụng, thay vì đánh giá chỉ dựa vào hình thức hoặc cảm giác.

Một công cụ đơn giản có thể hỗ trợ việc này là CRAAP Test, được thủ thư Sarah Blakeslee tại Meriam Library, California State University, Chico phát triển và công bố từ năm 2004 [18]. CRAAP gồm năm tiêu chí: Currency (Tính cập nhật), Relevance (Mức độ liên quan), Authority (Thẩm quyền của nguồn), Accuracy (Độ chính xác) và Purpose (Mục đích) [19].

Khi áp dụng, học sinh có thể lần lượt đặt năm câu hỏi: Thông tin được công bố hoặc cập nhật khi nào? Nội dung có thực sự phù hợp với điều mình đang tìm không? Ai là tác giả hoặc tổ chức chịu trách nhiệm về thông tin? Nội dung có bằng chứng, tài liệu tham khảo và có thể kiểm tra lại ở nguồn khác không? Cuối cùng, thông tin được tạo ra nhằm cung cấp kiến thức, quảng cáo, thuyết phục hay tác động đến suy nghĩ của người đọc?

CRAAP không nhằm đưa ra một kết luận máy móc rằng một nguồn là "tốt" hay "xấu". Giá trị của nguồn còn phụ thuộc vào nội dung và mục đích sử dụng. Chẳng hạn, một tài liệu được xuất bản nhiều năm trước có thể không phù hợp để tìm hiểu quy định pháp luật hiện hành nhưng vẫn rất có giá trị khi nghiên cứu lịch sử. Vì vậy, năm tiêu chí trên nên được xem như những câu hỏi giúp học sinh suy nghĩ kỹ hơn trước khi sử dụng thông tin [19].

Có thể ghi nhớ CRAAP bằng năm câu hỏi ngắn: Mới không? – Đúng việc không? – Ai nói? – Có bằng chứng không? – Nói để làm gì? Đây cũng chính là cách cụ thể hóa thói quen "**Dừng – Nghĩ – Kiểm tra**" khi học tập và tiếp nhận thông tin trên Internet.



Hình 5.4. Khung CRAAP: năm tiêu chí đánh giá độ tin cậy của một nguồn thông tin

5.2. Hợp tác học tập an toàn và công cụ AI

Học tập trong môi trường số không chỉ là tự tìm kiếm và đọc tài liệu. Học sinh ngày nay còn thường xuyên trao đổi bài với bạn bè, cùng chỉnh sửa tài liệu, chia sẻ tệp, làm bài tập nhóm trực tuyến và sử dụng các công cụ trí tuệ nhân tạo (AI) để giải thích kiến thức, gợi ý ý tưởng hoặc hỗ trợ quá trình học tập. Nếu được sử dụng đúng cách, những công cụ này có thể giúp việc học trở nên thuận tiện, chủ động và sáng tạo hơn.

Tuy nhiên, sự thuận tiện cũng đi kèm những điều cần lưu ý. Khi làm việc nhóm trực tuyến, một đường link chia sẻ không được thiết lập đúng có thể khiến tài liệu bị người ngoài truy cập, thông tin cá nhân đưa vào tệp chung có thể được nhiều người nhìn thấy hơn dự kiến. Khi sử dụng AI, câu trả lời được trình bày rất rõ ràng và thuyết phục vẫn có thể chứa thông tin chưa chính xác, thiếu nguồn hoặc không phù hợp với yêu cầu của bài học. Nếu chỉ sao chép câu trả lời mà không kiểm tra và tự suy nghĩ, AI có thể khiến việc học trở thành "làm hộ" thay vì "hỗ trợ học".

Vì vậy, mục tiêu của phần này không phải là hạn chế học sinh sử dụng các công cụ số hay AI, mà giúp các em sử dụng chúng đúng mục đích và vẫn làm chủ quá trình học tập của mình. Khi làm việc nhóm, học sinh cần biết chia sẻ tài liệu đúng người, bảo vệ thông tin cá nhân và tôn trọng đóng góp của các thành viên. Khi sử dụng AI, cần biết

đặt câu hỏi phù hợp, kiểm tra lại thông tin, không cung cấp dữ liệu riêng tư và trung thực về việc sử dụng AI khi bài học hoặc giáo viên yêu cầu.

Một nguyên tắc đơn giản có thể ghi nhớ xuyên suốt phần này là:

Cùng học nhưng vẫn bảo vệ thông tin – Dùng AI để hỗ trợ tư duy, không thay thế tư duy.

5.2.1. Làm việc nhóm an toàn trên nền tảng số

Khi cùng làm bài tập nhóm, xây dựng bài thuyết trình hoặc chia sẻ tài liệu học tập, học sinh không chỉ cần quan tâm đến nội dung được chia sẻ mà còn cần chú ý ai được phép truy cập và họ được phép làm gì với tài liệu đó. Một tài liệu học tập nếu được chia sẻ quá rộng hoặc cấp quyền chỉnh sửa không cần thiết có thể bị xem, thay đổi, xóa hoặc tiếp tục chuyển cho người khác ngoài dự kiến. Học sinh nên ưu tiên sử dụng nền tảng do nhà trường cung cấp hoặc hướng dẫn sử dụng. Chẳng hạn, một số trường sử dụng Microsoft Teams và Microsoft 365 Education để tổ chức lớp học, trao đổi nhóm và chia sẻ tài liệu. Tệp được chia sẻ trong môi trường này có thể được quản lý thông qua OneDrive hoặc SharePoint của tài khoản trường học. Tùy theo chính sách của nhà trường, một số chức năng chia sẻ có thể được giới hạn bởi người quản trị hệ thống.

Khi chia sẻ một tệp hoặc thư mục, học sinh cần lựa chọn đúng người và đúng quyền truy cập. Nếu người nhận chỉ cần đọc tài liệu, nên cấp quyền chỉ xem thay vì quyền chỉnh sửa. Nếu cùng làm một bài tập hoặc bài thuyết trình, chỉ những thành viên thực sự tham gia mới cần quyền chỉnh sửa. Với OneDrive dành cho tài khoản trường học, người dùng có thể chia sẻ tài liệu cho những người cụ thể và thiết lập các mức quyền như xem hoặc chỉnh sửa; quyền truy cập cũng có thể được thay đổi hoặc thu hồi sau đó.

Học sinh cũng cần thận trọng với đường liên kết chia sẻ. Không nên đăng công khai đường liên kết của tài liệu nhóm lên mạng xã hội hoặc gửi vào những nhóm không liên quan. Nếu nền tảng cho phép lựa chọn, nên ưu tiên hình thức chỉ những người được chỉ định mới có thể truy cập thay vì để bất kỳ ai có đường liên kết đều có thể mở tài liệu. Với tài khoản do trường quản lý, một số tùy chọn chia sẻ ra bên ngoài còn có thể được nhà trường hạn chế để bảo vệ dữ liệu. Sau khi bài tập hoặc dự án kết thúc, học sinh nên kiểm tra lại danh sách những người đang có quyền truy cập. Những người không còn cần sử dụng tài liệu nên được gỡ quyền; các đường liên kết không còn cần thiết cũng nên được vô hiệu hóa. Đây là cách hạn chế tình trạng một tài liệu vẫn tiếp tục được truy cập sau khi mục đích chia sẻ ban đầu đã kết thúc.

Một tính năng khác thường bị bỏ qua nhưng rất hữu ích cho việc chia sẻ tài liệu nhóm là đường dẫn chia sẻ có thời hạn (expiring link), có sẵn trên cả OneDrive lẫn Google Drive: thay vì tạo một đường link chia sẻ tồn tại vĩnh viễn – nghĩa là bất kỳ ai có được đường link đó, kể cả sau này khi dự án đã kết thúc, vẫn có thể truy cập – người dùng có thể đặt một ngày hết hạn cụ thể cho quyền truy cập, tự động vô hiệu hóa đường link sau thời điểm đó. Đây là một ví dụ cụ thể của nguyên tắc "thông tin không nên tồn tại lâu hơn mức cần thiết" mà học sinh nên áp dụng cho chính dữ liệu học tập của mình, chứ không chỉ cho thông tin cá nhân như đã phân tích ở Chương 2.

Vì sao nên tránh gửi bài tập, tài liệu nhóm qua Messenger cá nhân

Các ứng dụng chat cá nhân như Messenger, Zalo không được thiết kế cho mục đích quản lý tài liệu học tập: tệp tin dễ bị thất lạc trong dòng chảy tin nhắn, không có phiên bản lịch sử khi cần khôi phục bản chỉnh sửa trước, và quan trọng nhất – không có cơ chế phân quyền truy cập rõ ràng như các nền tảng học tập chuyên dụng.

Nếu tài khoản Messenger hoặc Zalo của một thành viên trong nhóm bị chiếm quyền theo đúng cơ chế đã phân tích ở Chương 3, toàn bộ tệp tin từng gửi qua khung chat đó – có thể bao gồm cả bài làm, đề cương ôn tập của cả nhóm – cũng có nguy cơ bị lộ theo, trong khi một nền tảng như Teams với 2FA sẽ khó bị xâm nhập hơn nhiều.

Với các trường không sử dụng hệ sinh thái Microsoft, Google Workspace for Education (bao gồm Google Docs, Sheets, Slides, Drive, Meet) là lựa chọn thay thế phổ biến với logic bảo mật tương tự: tài khoản trường học được quản lý tập trung bởi quản trị viên (thường là bộ phận công nghệ thông tin của trường), hỗ trợ xác thực 2 lớp, và Google Drive cũng có tính năng chia sẻ tệp với quyền hạn chi tiết (chỉ xem, chỉ bình luận, được chỉnh sửa) cùng khả năng thu hồi quyền truy cập bất kỳ lúc nào – về bản chất là một hình thức "đường link có thời hạn" linh hoạt hơn, vì không cần đặt ngày hết hạn cố định mà quản trị viên tài liệu có thể chủ động tắt quyền truy cập ngay khi thấy cần thiết, ví dụ sau khi dự án nhóm đã hoàn thành và chấm điểm xong. Việc trường học sử dụng hệ sinh thái nào (Microsoft hay Google) thường không quan trọng bằng việc học sinh có tận dụng đúng các tính năng bảo mật sẵn có của hệ sinh thái đó hay không – một sai lầm phổ biến là học sinh có tài khoản trường học đầy đủ tính năng bảo mật nhưng vẫn quen tay chuyển sang trao đổi bài vở qua kênh cá nhân kém an toàn hơn vì thói quen.

5.2.2. Sử dụng AI học tập có kiểm soát

Trí tuệ nhân tạo đang trở thành một công cụ hỗ trợ học tập ngày càng phổ biến. Học sinh có thể sử dụng AI để giải thích một khái niệm khó, gợi ý cách tìm kiếm thông tin, luyện tập ngoại ngữ, xây dựng dàn ý, tóm tắt tài liệu, tạo câu hỏi ôn tập hoặc hỗ trợ thực hiện một số sản phẩm học tập. Tuy nhiên, sử dụng được công cụ AI không đồng nghĩa với việc đã có năng lực AI. Điều quan trọng hơn là học sinh biết khi nào nên sử dụng, sử dụng để làm gì, kiểm tra kết quả như thế nào và chịu trách nhiệm ra sao đối với sản phẩm cuối cùng.

Cách tiếp cận này phù hợp với Khung năng lực số cho người học ban hành theo Thông tư 02/2025/TT-BGDĐT. Khung gồm 6 miền năng lực với 24 năng lực thành phần, trong đó việc khai thác và đánh giá thông tin, giao tiếp – hợp tác, bảo vệ dữ liệu cá nhân, giải quyết vấn đề và ứng dụng AI có quan hệ trực tiếp với việc học tập bằng công nghệ số. Công văn 3456/BGDĐT-GDPT tiếp tục cụ thể hóa miền Ứng dụng trí tuệ nhân tạo thành ba năng lực: hiểu biết về AI, sử dụng AI và đánh giá AI. Yêu cầu được nâng dần theo các nhóm lớp 1–3, 4–5, 6–7, 8–9 và 10–12.

Quyết định 2422/QĐ-BGDĐT năm 2026 tiếp tục đặt việc sử dụng AI trong một phạm vi rộng hơn gồm bốn mạch nội dung: tư duy lấy con người làm trung tâm, đạo đức AI, các kỹ thuật và ứng dụng AI, thiết kế hệ thống AI. Khung nhấn mạnh rằng công cụ chỉ là phương tiện hỗ trợ hoạt động học tập; năng lực AI không chỉ là khả năng viết câu lệnh hay thao tác với một ứng dụng cụ thể. Mức độ tự chủ, khả năng kiểm chứng, trách nhiệm và chất lượng quyết định của học sinh phải tăng dần theo cấp học.

Công văn 5588/BGDĐT-GDPT hướng dẫn triển khai Khung giáo dục AI từ năm học 2026–2027 còn yêu cầu cơ sở giáo dục lựa chọn và rà soát công cụ AI theo độ tuổi học sinh, mục tiêu giáo dục và điều khoản sử dụng; đồng thời phải quan tâm đến bảo vệ dữ liệu cá nhân, sở hữu trí tuệ và an toàn thông tin. Đặc biệt, nhà trường không nên bắt buộc học sinh phải sử dụng tài khoản cá nhân hoặc những công cụ chưa được rà soát.

AI nên được sử dụng để hỗ trợ quá trình học, không phải để thay học sinh suy nghĩ hoặc làm thay toàn bộ nhiệm vụ. Một câu trả lời được AI trình bày trôi chảy vẫn có thể sai, thiếu thông tin, sử dụng nguồn không tồn tại hoặc không phù hợp với yêu cầu của bài học. Vì vậy, học sinh cần xem kết quả của AI là một gợi ý cần được kiểm tra, không phải đáp án mặc nhiên đúng. Yêu cầu kiểm chứng kết quả AI xuất hiện xuyên suốt cả Khung năng lực số và Khung giáo dục AI của Bộ GD&ĐT. Bảng 5.4 đề cập tới việc sử dụng AI phù hợp với từng cấp học.

Bảng 5.4. Bảng hướng dẫn sử dụng AI phù hợp với từng cấp học

Cấp học	Cách sử dụng phù hợp	Kỹ năng cần hình thành	Những điều cần đặc biệt lưu ý
Tiểu học	- Làm quen với AI qua hoạt động có hướng dẫn. - Nhận biết AI trong đời sống - Sử dụng một số công cụ học tập đơn giản do giáo viên hoặc nhà trường lựa chọn.	- Biết AI do con người tạo ra - Biết AI có thể trả lời sai; bước đầu kiểm tra kết quả bằng điều đã học hoặc nguồn giáo viên cung cấp - Biết bảo vệ thông tin cá nhân.	- Không phụ thuộc vào AI - Không tự ý tạo tài khoản hoặc nhập thông tin cá nhân - Khi gặp nội dung lạ, khó hiểu hoặc không phù hợp phải hỏi người lớn.
THCS	Dùng AI để giải thích kiến thức, gợi ý ý tưởng, tạo câu hỏi luyện tập, hỗ trợ tìm kiếm và xử lý thông tin, thực hiện sản phẩm hoặc dự án nhỏ.	- Biết đặt yêu cầu phù hợp, so sánh kết quả với nhiều nguồn, nhận biết thông tin sai hoặc thiên lệch; - Hiểu quyền riêng tư, bản quyền và trách nhiệm khi dùng AI.	- Không sao chép nguyên câu trả lời để nộp - Không để AI thay thế tư duy; kiểm tra nguồn trước khi sử dụng - Khai báo việc dùng AI khi được yêu cầu.
THPT	Sử dụng AI có mục tiêu trong học tập, nghiên cứu, phân tích dữ liệu, sáng tạo sản phẩm, giải quyết vấn đề và bước đầu thiết kế hoặc đánh giá giải pháp AI.	- Biết xây dựng và điều chỉnh prompt - Phân tích độ tin cậy, giới hạn và thiên lệch - Đối chiếu nguồn - Đánh giá rủi ro, tính minh bạch, đạo đức và tác động của AI.	- Tuân thủ quy định của từng môn học; không sử dụng AI để gian lận - Tôn trọng dữ liệu, bản quyền và quyền riêng tư - Chịu trách nhiệm về sản phẩm cuối cùng.

Từ các yêu cầu trên, có thể hướng dẫn học sinh bằng một quy trình thực hành thống nhất gồm 6 bước, minh họa ở Hình 5.5:

Xác định nhiệm vụ: Trước khi mở AI, học sinh cần biết mình muốn AI hỗ trợ việc gì: giải thích kiến thức, tìm ý tưởng, luyện tập, tìm nguồn hay kiểm tra sản phẩm. Không nên mở AI và hỏi một cách ngẫu nhiên khi chưa xác định mục tiêu.

Lựa chọn công cụ: Ưu tiên công cụ được nhà trường hoặc giáo viên hướng dẫn, phù hợp với độ tuổi và mục tiêu học tập. Không tự ý cung cấp tài khoản, dữ liệu hoặc cấp quyền truy cập không cần thiết cho một ứng dụng chưa được kiểm tra.

Đặt yêu cầu: Câu hỏi gửi cho AI nên nói rõ nhiệm vụ, bối cảnh, đối tượng và yêu cầu đầu ra. Học sinh có thể yêu cầu AI giải thích, đưa ví dụ hoặc gợi ý cách thực hiện, nhưng nên tránh yêu cầu AI "làm toàn bộ bài để nộp".

Kiểm chứng: Không sử dụng ngay câu trả lời đầu tiên. Học sinh cần so sánh với sách giáo khoa, tài liệu giáo viên cung cấp, nguồn chính thức hoặc những nguồn độc lập đáng tin cậy khác. Với số liệu, sự kiện và trích dẫn, cần tìm lại nguồn gốc trước khi đưa vào sản phẩm.

Hoàn thiện bằng tư duy của bản thân: Học sinh lựa chọn nội dung phù hợp, sửa sai, tổ chức lại thông tin, bổ sung suy nghĩ và tạo ra sản phẩm của chính mình. AI hỗ trợ quá trình nhưng người học vẫn phải hiểu và giải thích được điều mình viết hoặc trình bày.

Khai báo khi cần: Khi quy định của giáo viên hoặc nhà trường yêu cầu, học sinh nêu rõ công cụ AI đã dùng, mục đích sử dụng, phần AI hỗ trợ và cách mình đã kiểm tra, chỉnh sửa kết quả.



Hình 5.5. Quy trình 6 bước sử dụng AI trong học tập

Hình 5.6 minh họa các công cụ phổ biến hỗ trợ học tập có kiểm soát dựa trên những công cụ AI uy tín và có trách nhiệm.



Hình 5.6. Ba công cụ AI học tập phổ biến hiện nay

Gemini for Education là công cụ AI của Google dành cho môi trường giáo dục. Công cụ này có thể hỗ trợ học sinh tìm ý tưởng, giải thích kiến thức, tóm tắt nội dung và hỗ trợ học tập trong hệ sinh thái Google. Khi sử dụng, học sinh vẫn cần kiểm tra lại thông tin và tuân theo hướng dẫn của giáo viên, nhà trường.

VioEdu là nền tảng học tập trực tuyến của Việt Nam, ứng dụng AI và dữ liệu học tập để hỗ trợ học sinh luyện tập theo năng lực. Hệ thống có thể phân tích kết quả học tập, nhận biết nội dung học sinh còn yếu và gợi ý bài tập phù hợp. VioEdu phù hợp với học sinh phổ thông, đặc biệt ở bậc tiểu học và THCS.

ChatGPT là công cụ AI có thể trò chuyện và hỗ trợ nhiều hoạt động học tập như giải thích bài, gợi ý ý tưởng, tạo câu hỏi ôn tập, tóm tắt và chỉnh sửa văn bản. Với học sinh phổ thông, ChatGPT nên được dùng như một công cụ hỗ trợ tư duy, không dùng để làm thay toàn bộ bài tập. Các em cần kiểm tra lại thông tin trước khi sử dụng và bảo vệ dữ liệu cá nhân.

Mỗi công cụ có thế mạnh riêng, học sinh nên lựa chọn theo mục tiêu học tập, độ tuổi và hướng dẫn của giáo viên hoặc nhà trường. Bất kể sử dụng công cụ AI nào, một nguyên tắc không thể thương lượng là luôn tự kiểm tra lại thông tin AI cung cấp trước khi sử dụng, đặc biệt với các số liệu, trích dẫn, sự kiện cụ thể. Nguyên nhân kỹ thuật

nằm ở chính cách các mô hình ngôn ngữ lớn (large language model) hoạt động: mô hình được huấn luyện để tạo ra chuỗi văn bản có xác suất xuất hiện hợp lý về mặt ngôn ngữ, chứ không có một cơ chế nội tại để "biết" điều mình vừa viết ra có đúng sự thật hay không – hiện tượng này được giới chuyên môn gọi là "ảo giác" (hallucination): AI có thể trình bày một thông tin sai, hoàn toàn bịa đặt (một số liệu không tồn tại, một trích dẫn không ai từng nói) với giọng điệu tự tin y hệt như khi trình bày một thông tin chính xác, khiến người dùng khó phân biệt nếu không chủ động đối chiếu lại. Đây là lý do vì sao, dù các công cụ như *Gemini for Education* hay *ChatGPT* có nhiều lớp kiểm soát an toàn về nội dung độc hại, không một công cụ AI nào – kể cả những công cụ có tích hợp tính năng duyệt web để hiển thị nguồn tham khảo – có thể thay thế hoàn toàn bước tự kiểm tra thủ công của người dùng.

Ví dụ minh họa cơ chế "ảo giác" (tình huống giả định để minh họa, không phải một câu trả lời AI cụ thể đã ghi nhận): một học sinh hỏi AI về năm thành lập của một tổ chức giáo dục, và AI trả lời một năm cụ thể kèm theo một chi tiết bổ sung nghe rất hợp lý (ví dụ tên người sáng lập). Nếu học sinh không đối chiếu lại, thông tin sai này có thể được đưa thẳng vào bài tiểu luận và xuất hiện như một "sự thật" trong bài nộp – trong khi trên thực tế, mô hình AI chỉ đang tạo ra một câu trả lời nghe có vẻ đúng dựa trên các mẫu hình dữ liệu đã học, không tra cứu lại một nguồn xác thực nào tại thời điểm trả lời (trừ khi công cụ có bật rõ tính năng duyệt web và trích dẫn nguồn cụ thể kèm theo). Đây chính là lý do phần lớn giáo viên đại học hiện nay, khi cho phép sinh viên dùng AI hỗ trợ nghiên cứu, đều yêu cầu đối chiếu lại mọi số liệu, trích dẫn với nguồn gốc trước khi đưa vào bài viết chính thức.

Ba câu hỏi nên tự đặt ra trước khi dùng thông tin từ AI

Thông tin này có được kiểm chứng qua đối chiếu với một nguồn độc lập khác (SGK, Hocmai, Google Scholar) hay chỉ dựa vào một mình câu trả lời của AI?

Nếu đây là một số liệu hoặc trích dẫn cụ thể, mình có thể tìm thấy chính nguồn gốc của nó không, hay AI chỉ đưa ra một con số nghe có vẻ hợp lý?

Mình có đang dùng AI để hiểu sâu hơn một vấn đề, hay đang dùng AI để né tránh việc tự tư duy? – câu hỏi này sẽ được phân tích kỹ hơn ở mục tiếp theo về đạo đức học thuật.

5.2.3. Đạo đức học thuật và tính trung thực khi sử dụng AI

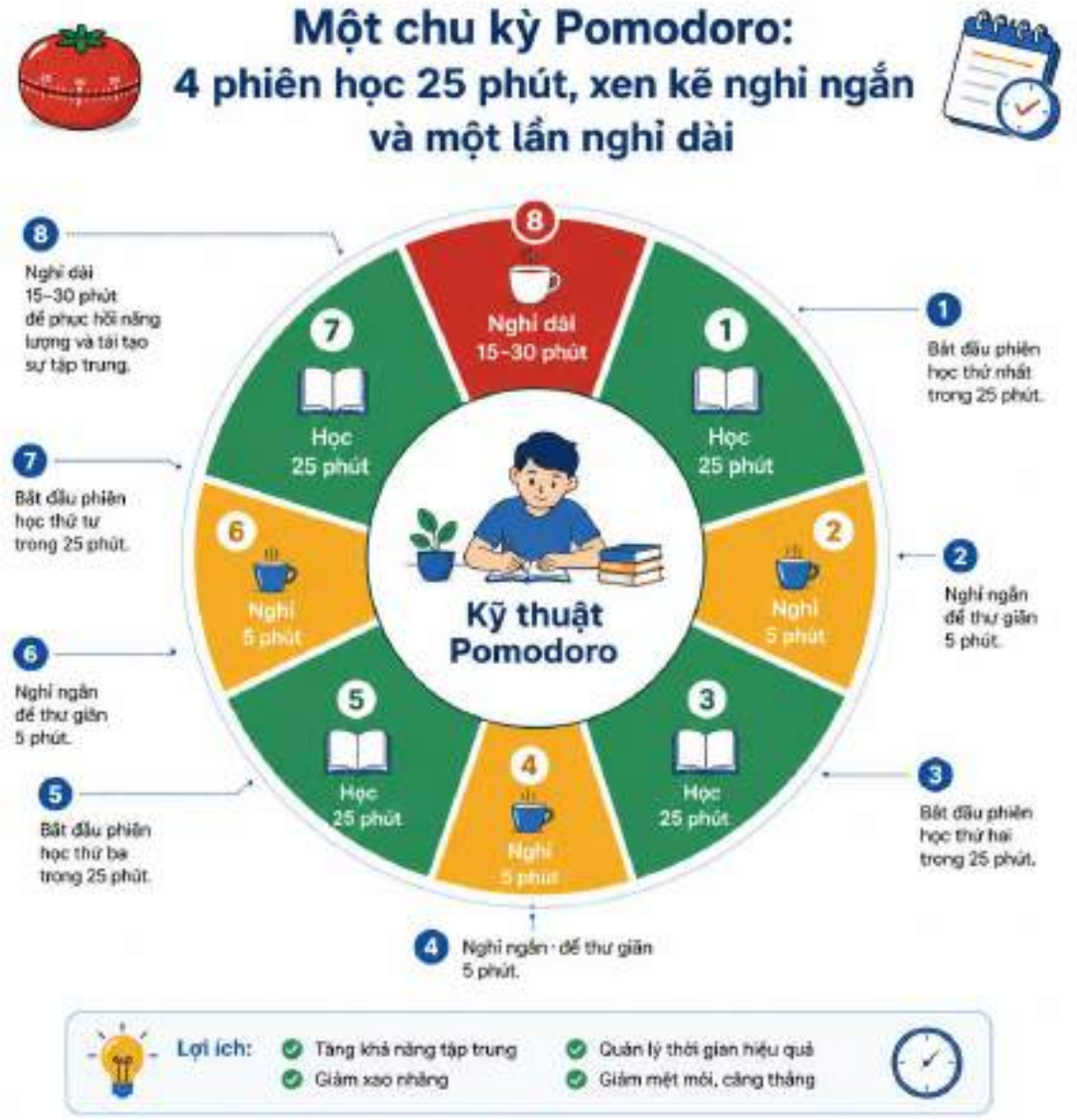
Ranh giới giữa "dùng AI để hỗ trợ học tập" và "dùng AI để làm thay bài tập" không phải lúc nào cũng rõ ràng, và đây là một chủ đề mà nhiều trường học trên thế giới, bao gồm cả các trường đã triển khai ChatGPT Edu hay Gemini for Education, vẫn đang

trong quá trình xây dựng quy định cụ thể. Một cách phân định tương đối hữu ích là xem xét vai trò của AI trong từng công đoạn làm bài: sử dụng AI để giải thích lại một khái niệm chưa hiểu, gợi ý dàn ý trước khi tự viết, hoặc kiểm tra lại lỗi ngữ pháp sau khi đã hoàn thành bài viết của chính mình, thường được xem là hỗ trợ học tập chính đáng – tương tự việc hỏi bạn bè, tra từ điển, hay nhờ giáo viên giải thích thêm. Ngược lại, việc yêu cầu AI viết toàn bộ bài luận rồi nộp như sản phẩm của chính mình, hoặc dùng AI giải toàn bộ đề kiểm tra rồi chép lại nguyên văn, thuộc về hành vi vi phạm liêm chính học thuật – về bản chất không khác gì việc chép bài từ diễn đàn giải bài, chỉ khác ở công cụ được sử dụng.

Một khía cạnh thường bị bỏ sót là yêu cầu công khai minh bạch việc sử dụng AI: nhiều trường đại học và ngày càng nhiều trường phổ thông yêu cầu học sinh, sinh viên ghi chú rõ trong bài nộp nếu có sử dụng công cụ AI hỗ trợ, tương tự như việc trích dẫn một nguồn tài liệu tham khảo đã học. Về nguyên tắc, nếu một ý tưởng hoặc một đoạn văn có đóng góp đáng kể từ AI, việc không công bố điều này khi được yêu cầu công khai cũng là một hình thức không trung thực học thuật, dù không giống hoàn toàn với đạo văn truyền thống. Học sinh nên chủ động tìm hiểu quy định cụ thể của trường hoặc giáo viên bộ môn về việc sử dụng AI cho từng loại bài tập, thay vì tự suy đoán ranh giới cho phép, vì quy định này có thể khác nhau đáng kể giữa các môn học (một bài luận Văn có thể có yêu cầu khắt khe hơn một bài tập lập trình, nơi việc tham khảo mã nguồn từ AI có thể được khuyến khích như một kỹ năng thực hành có kiểm soát).

5.2.4. Quản lý thời gian học online hiệu quả

Nghịch lý của việc học trực tuyến là chính công cụ giúp học sinh tiếp cận tri thức – chiếc điện thoại hoặc máy tính kết nối mạng – cũng là công cụ dễ khiến học sinh xao nhãng nhất, đúng như cơ chế "phần thưởng biến đổi" (là cơ chế trong đó người dùng không biết trước khi nào mình sẽ gặp một nội dung thú vị, nhận được lượt thích, bình luận, tin nhắn hoặc thông báo mới. Chính sự không chắc chắn này có thể khiến người dùng muốn tiếp tục kiểm tra, cuộn xem hoặc quay lại ứng dụng nhiều lần, từ đó dễ bị phân tâm khi học tập) của các nền tảng mạng xã hội. Vì vậy, kỹ năng cuối cùng trong chương này không phải một công cụ tìm kiếm hay một nền tảng học tập, mà là một kỹ thuật quản lý sự chú ý của chính bản thân học sinh trong lúc học trực tuyến. Hình 5.7 mô tả một chu trình học Pomodoro về các phiên học 25 phút, xen kẽ nghỉ ngắn và nghỉ dài.



Hình 5.7. Một chu kỳ Pomodoro điển hình

Kỹ thuật Pomodoro, do Francesco Cirillo phát triển từ cuối thập niên 1980 (tên gọi xuất phát từ chiếc đồng hồ bấm giờ hình quả cà chua pomodoro trong tiếng Ý – mà ông dùng khi còn là sinh viên), chia thời gian học thành các phiên tập trung cao độ kéo dài 25 phút, xen kẽ với 5 phút nghỉ ngắn; sau khoảng 4 phiên liên tiếp, người học nghỉ một khoảng dài hơn (thường 15–30 phút) trước khi bắt đầu chu kỳ mới.

Ứng dụng Forest là một công cụ hỗ trợ áp dụng kỹ thuật Pomodoro theo hướng trực quan và có yếu tố tạo động lực: khi bắt đầu một phiên tập trung, người dùng "trồng" một cây ảo trên màn hình; nếu rời khỏi ứng dụng để mở mạng xã hội hoặc ứng dụng giải trí khác trước khi hết thời gian đã đặt, cây sẽ "chết" ngay lập tức – một hình thức phản hồi tức thì, trực quan hơn nhiều so với chỉ nhìn đồng hồ đếm ngược. Một tính năng

đáng chú ý khác của Forest là khả năng mời bạn bè cùng "trồng cây" trong cùng một phiên học, tạo ra một dạng trách nhiệm xã hội nhẹ nhàng (nếu một người trong nhóm mất tập trung, cây của cả nhóm bị ảnh hưởng) – có thể xem là một hình thức lành mạnh của áp lực đồng trang lứa.

Nhiều nền tảng học tập trực tuyến có chức năng giúp học sinh theo dõi quá trình học, chẳng hạn số bài đã hoàn thành, thời gian đã học hoặc kết quả luyện tập. Học sinh nên thường xuyên xem lại những thông tin này, có thể vào cuối mỗi tuần, để biết mình đã học được những gì, còn bài nào chưa hoàn thành và có cần điều chỉnh thời gian học hay không. Với học sinh nhỏ tuổi, cha mẹ hoặc thầy cô có thể cùng xem và giúp các em sắp xếp thời gian học phù hợp. Thói quen này giúp học sinh học tập chủ động, đều đặn và biết tự điều chỉnh khi cần.

5.3. Kỹ thuật soạn thảo câu lệnh khi sử dụng AI (Prompt engineering)

5.3.1. Prompt là gì?

Prompt là câu lệnh hoặc câu hỏi người dùng đưa vào công cụ AI để yêu cầu AI thực hiện một nhiệm vụ. Viết prompt tốt giúp AI hiểu rõ yêu cầu và trả lời phù hợp hơn.

Học sinh cần lưu ý giới hạn độ tuổi của từng công cụ. ChatGPT không dành cho trẻ dưới 13 tuổi [20], người từ 13 đến dưới 18 tuổi cần có sự đồng ý của cha mẹ hoặc người giám hộ. Claude hiện chỉ dành cho người từ 18 tuổi trở lên [21]. Vì vậy, học sinh chỉ nên sử dụng công cụ AI phù hợp với độ tuổi và theo hướng dẫn của giáo viên, nhà trường hoặc cha mẹ.

- *Tiểu học*: Học sinh chủ yếu làm quen với cách diễn đạt yêu cầu rõ ràng thông qua hoạt động do giáo viên hoặc cha mẹ hướng dẫn. Các em không tự tạo tài khoản trên những nền tảng không cho phép độ tuổi của mình và không tự cung cấp thông tin cá nhân cho công cụ AI.

- *THCS*: Học sinh bắt đầu thực hành cách đặt câu hỏi và viết prompt có cấu trúc. Với học sinh chưa đủ độ tuổi của nền tảng, việc sử dụng phải thông qua hoạt động do giáo viên hoặc cha mẹ tổ chức. Học sinh từ đủ 13 tuổi chỉ sử dụng những công cụ cho phép độ tuổi của mình và tuân thủ yêu cầu về sự đồng ý của cha mẹ hoặc người giám hộ.

- *THPT*: Học sinh có thể thực hành các kỹ thuật prompt nâng cao hơn nhưng vẫn phải tuân thủ điều kiện độ tuổi của từng nền tảng. Học sinh dưới 18 tuổi không sử dụng những dịch vụ chỉ dành cho người trưởng thành; khi nhà trường cung cấp công cụ hoặc tài khoản học tập, cần thực hiện theo hướng dẫn và chính sách của nhà trường.

Hãy tưởng tượng AI là một người bạn rất giỏi nhưng không nhìn thấy em. Bạn ấy không biết em học lớp mấy hay đang cần gì. Em nói càng rõ, bạn ấy giúp càng đúng.

Điều cần nhớ: Hỏi mơ hồ, nhận câu trả lời mơ hồ. Hỏi rõ ràng, nhận câu trả lời rõ ràng.

Tài liệu chia thành ba phần theo cấp học. Mỗi cấp xây dựng tiếp trên nền tảng của cấp trước.

5.3.2. Đối với cấp Tiểu học

Học sinh tiểu học chỉ cần nhớ một quy tắc: **3 chữ R – Rõ, Riêng, Rà lại**.

Theo quy định: Quyết định số 2422/QĐ-BGDĐT ngày 18 tháng 8 năm 2026 của Bộ Giáo dục và Đào tạo xác định học sinh tiểu học làm quen và trải nghiệm AI thông qua các hoạt động đơn giản, trực quan, có sự hướng dẫn và giám sát của giáo viên hoặc cha mẹ. Các em chỉ sử dụng những công cụ AI phù hợp với độ tuổi và điều khoản sử dụng của nhà cung cấp, không tự ý tạo tài khoản cá nhân trên các công cụ chưa phù hợp với độ tuổi. Việc sử dụng AI ở trường hoặc tại nhà nên được thực hiện thông qua hoạt động, công cụ hoặc tài khoản do giáo viên, nhà trường hoặc cha mẹ quản lý và hướng dẫn.

a. Chữ R thứ nhất – RÕ: Nói rõ em muốn gì

Bảng 5.5. Ví dụ về cách sử dụng Prompt cho học sinh Tiểu học

Chưa tốt	Tốt hơn
"Con mèo"	"Kể cho em 3 điều thú vị về loài mèo"
"Toán"	"Giải thích phép chia 12 : 3 bằng ví dụ chia kẹo"
"Khủng long"	"Vì sao khủng long biến mất? Trả lời ngắn trong 5 câu"

b. Chữ R thứ hai – RIÊNG: Cho AI biết em là ai

Thêm câu: "Em là học sinh lớp 3, hãy giải thích thật dễ hiểu." Khi đó AI sẽ dùng từ đơn giản và ví dụ gần gũi với em.

c. Chữ R thứ ba – RÀ LẠI: Hỏi thêm nếu chưa hiểu

- "Em chưa hiểu, bạn giải thích lại bằng cách khác nhé."
- "Cho em thêm một ví dụ nữa."
- "Nói ngắn hơn được không?"

d. Mẫu câu "điền vào chỗ trống"

Em là học sinh lớp ___. Hãy giúp em ___ về ___. Giải thích thật dễ hiểu và cho em ___ ví dụ.

Ví dụ: “Em là học sinh lớp 4. Hãy giúp em hiểu về vòng tuần hoàn của nước. Giải thích thật dễ hiểu và cho em 2 ví dụ trong cuộc sống.”

e. Những điều em cần nhớ

- Không cho AI biết tên thật, địa chỉ nhà, trường, số điện thoại hay ảnh của em.

- AI có thể nói sai. Hãy hỏi lại thầy cô hoặc bố mẹ.

- AI giúp em hiểu bài, không làm bài hộ em.

5.3.3. Cấp trung học cơ sở

Học sinh THCS học một công thức bốn phần: VAI – VIỆC – BỐI CẢNH – KẾT QUẢ.

a. Công thức bốn phần

Bảng 5.6. Ví dụ sử dụng công thức bốn phần cho THCS

Thành phần	Câu hỏi tự đặt ra	Ví dụ
VAI	AI nên đóng vai ai?	“Hãy đóng vai giáo viên Lịch sử…”
VIỆC	Em cần AI làm gì?	“…giải thích nguyên nhân chiến thắng Bạch Đằng năm 938…”
BỐI CẢNH	Em là ai, đang ở tình huống nào?	“…em học lớp 7, chuẩn bị thuyết trình 5 phút…”
KẾT QUẢ	Em muốn câu trả lời có dạng gì?	“…trình bày thành 3 ý chính, mỗi ý 2–3 câu.”

Prompt hoàn chỉnh:

Hãy đóng vai giáo viên Lịch sử. Giải thích nguyên nhân chiến thắng Bạch Đằng năm 938. Em học lớp 7 và cần chuẩn bị bài thuyết trình 5 phút. Trình bày thành 3 ý chính, mỗi ý 2–3 câu, kèm 1 câu mở đầu gây chú ý.

b. Năm kỹ thuật hữu ích

1. *Yêu cầu định dạng cụ thể*: bảng so sánh, sơ đồ ý, gạch đầu dòng, câu hỏi trắc nghiệm.

- Ví dụ: “Lập bảng so sánh động vật có xương sống và không xương sống theo 4 tiêu chí.”

2. *Chia nhỏ câu hỏi lớn*: Đừng hỏi “Dạy em toàn bộ Hóa học lớp 8”. Hãy hỏi từng bài, từng khái niệm.

3. Nhờ AI làm gia sư, không làm người giải hộ:

- Ví dụ: "Đừng cho em đáp án ngay. Hãy gợi ý từng bước để em tự giải bài toán này."

4. Tự kiểm tra kiến thức:

- Ví dụ: "Em vừa học xong bài Quang hợp. Hãy đặt cho em 5 câu hỏi, đợi em trả lời rồi chấm và giải thích chỗ sai."

5. *Hỏi tiếp để đào sâu:* "Tại sao lại như vậy?", "Có ví dụ thực tế nào không?", "Nếu … thì sao?"

c. Cảnh giác với AI

- AI có thể bịa thông tin rất tự tin, gọi là "ảo giác AI". Điều này hay xảy ra với số liệu, ngày tháng, tên người và trích dẫn.

- Luôn đối chiếu với sách giáo khoa hoặc nguồn tin cậy.

- Nộp bài do AI viết hộ là gian lận, và em cũng không học được gì.

5.3.4. Cấp trung học phổ thông

Học sinh THPT dùng AI như một công cụ tư duy và nghiên cứu, với khung C.R.E.A.T.E và bảy kỹ thuật chuyên sâu.

a. Khung prompt nâng cao C.R.E.A.T.E

Bảng 5.7. Công thức sử dụng Prompt cho học sinh THPT

Chữ	Ý nghĩa	Nội dung cần nêu
C – Context	Bối cảnh	Mục đích, đối tượng, trình độ
R – Role	Vai trò	Chuyên gia, người phản biện, giám khảo
E – Explicit task	Nhiệm vụ rõ ràng	Động từ cụ thể: phân tích, so sánh, đánh giá, tóm tắt
A – Audience & Format	Đối tượng và định dạng	Độ dài, cấu trúc, văn phong
T – Tone & Constraints	Giọng điệu và giới hạn	Tránh thuật ngữ quá khó, trong phạm vi chương trình
E – Evaluate	Đánh giá	Yêu cầu AI tự kiểm tra hoặc nêu mức độ chắc chắn

b. Bảy kỹ thuật chuyên sâu

1. *Suy luận từng bước (Chain of Thought):* Giúp AI ít sai hơn và giúp em hiểu cách tư duy.

- "Giải bài toán sau và trình bày từng bước lập luận, giải thích vì sao chọn cách làm đó."

2. *Cho ví dụ mẫu (Few-shot):* AI học theo mẫu em đưa ra.

- "Đây là 2 câu mở bài nghị luận em thích: [ví dụ 1], [ví dụ 2]. Hãy nhận xét điểm mạnh và hướng dẫn em viết một mở bài tương tự cho đề: …"

3. *Phương pháp Socrates*: AI hỏi, em trả lời.

- "Hãy dẫn dắt em hiểu định luật II Newton bằng cách chỉ đặt câu hỏi gợi mở, mỗi lần một câu, không giảng giải trực tiếp."

4. Phản biện và nhiều góc nhìn:

- "Đây là dàn ý bài nghị luận của em: […]. Hãy đóng vai giám khảo khó tính, chỉ ra 3 điểm yếu và gợi ý cách khắc phục."

- "Trình bày quan điểm ủng hộ và phản đối việc dùng mạng xã hội ở tuổi học sinh, mỗi bên 3 luận điểm."

5. Lặp và tinh chỉnh (Iteration):

Prompt đầu tiên hiếm khi hoàn hảo. Hãy chỉnh dần: "Ngắn gọn hơn", rồi "Thêm số liệu minh họa", rồi "Viết lại theo văn phong học thuật".

6. Yêu cầu AI tự đánh giá độ tin cậy:

- "Với mỗi thông tin, hãy cho biết em nên kiểm chứng ở nguồn nào, và phần nào bạn không chắc chắn."

7. Ôn thi thông minh:

- "Tạo lịch ôn tập 4 tuần cho môn Sinh học 12, chương Di truyền. Mỗi ngày 45 phút, xen kẽ lý thuyết và bài tập, tuần cuối là đề tổng hợp."

c. Ví dụ: Từ prompt yếu đến prompt mạnh

Mức độ	Prompt
Yếu	"Viết về biến đổi khí hậu"
Trung bình	"Viết bài 500 chữ về tác động của biến đổi khí hậu"
Mạnh	"Em là học sinh lớp 11, đang viết bài nghị luận xã hội 600 chữ về tác động của biến đổi khí hậu đến Đồng bằng sông Cửu Long. Đừng viết bài hộ em. Hãy giúp em: (1) lập dàn ý 3 luận điểm, (2) gợi ý loại dẫn chứng cần tìm cho mỗi luận điểm, (3) chỉ ra lỗi lập luận học sinh hay mắc với đề này."

5.3.5. Đạo đức và tư duy phản biện

- *Minh bạch*: Nếu dùng AI hỗ trợ bài làm, hãy tuân theo quy định của thầy cô và nhà trường.

- *Kiểm chứng*: AI không phải nguồn trích dẫn học thuật. Hãy tìm nguồn gốc từ sách, báo chính thống, tài liệu khoa học.

- *Thiên kiến*: AI có thể phản ánh định kiến trong dữ liệu. Luôn tự hỏi: "Góc nhìn này đã đầy đủ chưa?"

- *Bảo mật*: Không đưa thông tin cá nhân, ảnh hay dữ liệu của người khác vào AI.

Tự chủ: AI giúp em nghĩ nhanh hơn, không nghĩ thay em.

5.4. Minh họa: một tuần tự học tích hợp cả 8 kỹ năng

Tình huống minh họa mang tính tổng hợp, xây dựng để thể hiện cách 8 kỹ năng phối hợp với nhau trong thực tế – không mô tả một học sinh cụ thể nào. Để tránh cảm giác tám kỹ năng trong chương này là tám mục lý thuyết rời rạc, phần minh họa dưới đây thuật lại cách một học sinh lớp 11 có thể phối hợp toàn bộ tám kỹ năng trong một tuần chuẩn bị cho bài kiểm tra giữa kỳ môn Ngữ văn, với đề tài nghị luận xã hội về ảnh hưởng của mạng xã hội đến giới trẻ – một chủ đề đủ gần gũi để học sinh có thể tận dụng chính những phân tích đã học ở Chương 2–3 của tài liệu này.

Thứ 2: Xác định nguồn và lên kế hoạch tìm kiếm. Sau khi nhận đề bài, học sinh dành 25 phút đầu tiên (một phiên Pomodoro, kỹ năng 8) để phác thảo những khía cạnh cần tìm hiểu: số liệu về tình trạng sử dụng mạng xã hội của giới trẻ, quan điểm của chuyên gia tâm lý, và một vài ví dụ thực tế. Thay vì gõ thẳng "ảnh hưởng của mạng xã hội đến giới trẻ" vào Google – một câu hỏi sẽ trả về hàng triệu kết quả chung chung – học sinh áp dụng kỹ năng Boolean Search (kỹ năng 2) để thu hẹp phạm vi: "mạng xã hội" AND "thanh thiếu niên" AND "sức khỏe tâm thần" site:*.edu.vn, ưu tiên các trang thuộc tên miền giáo dục để tăng khả năng gặp nguồn học thuật.

Thứ 3: Đánh giá và chọn lọc nguồn. Với danh sách các bài viết tìm được, học sinh áp dụng khung CRAAP (kỹ năng 4) để lọc ra ba đến bốn nguồn đáng tin cậy nhất: kiểm tra ngày đăng (Currency) để tránh dùng số liệu quá cũ, kiểm tra tác giả (Authority) để ưu tiên bài viết từ chuyên gia tâm lý học hoặc cơ quan nghiên cứu chính thức hơn là một bài blog cá nhân, và đối chiếu xem thông tin có dẫn nguồn rõ ràng (Accuracy) hay không. Song song, học sinh cân nhắc tham khảo thêm gợi ý dàn ý từ một công cụ AI học tập như Gemini hoặc ChatGPT (kỹ năng 6) – không phải để lấy nội dung viết sẵn, mà để kiểm tra xem dàn ý tự phác thảo ở thứ Hai có bỏ sót khía cạnh quan trọng nào không, đúng tinh thần "dùng AI để hỗ trợ hiểu bài, không dùng để né tránh tư duy" đã phân tích ở phần đạo đức học thuật.

Thứ 4: Thu thập trích dẫn trong lúc đọc. Khi đọc từng nguồn đã chọn, học sinh dùng tiện ích mở rộng Zotero (kỹ năng 3) để lưu lại thông tin trích dẫn ngay tại thời điểm đọc, thay vì để dồn đến cuối tuần mới nhớ lại mình đã đọc bài nào ở đâu – một sai lầm phổ biến khiến nhiều học sinh phải tìm lại nguồn đã đọc trước đó, mất thời gian hơn nhiều so với việc ghi chú ngay từ đầu.

Thứ 5: Trao đổi nhóm và hoàn thiện dàn ý **vì bài tập có phần thảo luận nhóm nhỏ trước khi nộp bài cá nhân. H**ọc sinh trao đổi dàn ý với hai bạn cùng nhóm qua Microsoft Teams của lớp thay vì nhóm chat Messenger riêng (kỹ năng 5), đồng thời chia sẻ tài liệu tham khảo đã tổng hợp qua một đường link Google Drive có đặt quyền "chỉ xem" – tránh trường hợp một bạn trong nhóm vô tình chỉnh sửa nhầm tài liệu chung.

Thứ 6: Viết bài và tự kiểm tra. Học sinh dành hai đến ba phiên Pomodoro liên tiếp để viết bản nháp đầu tiên, sau đó dùng Zotero để tự động chèn trích dẫn và sinh danh mục tài liệu tham khảo theo chuẩn APA (kỹ năng 3) mà giáo viên yêu cầu, rồi chạy qua Grammarly bản miễn phí để rà soát lỗi ngữ pháp, chính tả – với hiểu biết rõ rằng bước này không thay thế được việc tự đọc lại toàn bộ bài để bảo đảm mọi ý đều là lời văn của chính mình (kỹ năng 7), không phải diễn giải sát nghĩa đến mức gần như sao chép từ nguồn tham khảo.

Cuối tuần: Nhìn lại báo cáo tiến độ trước khi nộp bài vào đầu tuần sau. Học sinh dành vài phút xem lại báo cáo thời gian tập trung của ứng dụng Forest trong tuần (kỹ năng 8) để tự đánh giá: những ngày nào tập trung tốt, những ngày nào bị gián đoạn nhiều – dữ liệu này sẽ hữu ích để điều chỉnh kế hoạch cho bài tập lớn tiếp theo, khép lại một chu trình tự học trọn vẹn từ tìm kiếm đến hoàn thiện sản phẩm cuối cùng.

Ví dụ trên cho thấy tám kỹ năng của chương này hiếm khi được sử dụng một cách tách biệt trong thực tế, mà đan xen vào nhau xuyên suốt một quá trình học tập bình thường – đúng như cách 12 nguyên tắc "vàng" ở Chương 2 hay quy trình 7 bước ở Chương 4 cũng không phải những mục lý thuyết độc lập, mà là các công cụ tư duy được huy động linh hoạt tùy theo tình huống cụ thể mà học sinh gặp phải.

Bảng 5.8 tổng hợp các kỹ năng và các công cụ hay nền tảng tiêu biểu được sử dụng trong học tập và nghiên cứu trong một số trường học.

Bảng 5.8. Bảng tổng hợp 8 kỹ năng và công cụ tương ứng

Kỹ năng	Công cụ / nền tảng tiêu biểu	Lợi ích cốt lõi
1. Nguồn học thuật đáng tin cậy	Hocmai.vn, Viettel Study, VnDoc, Google Scholar, thư viện số trường học	Học đúng kiến thức, tránh "nợ kiến thức" từ việc chép đáp án
2. Boolean Search & lọc kết quả	Google Advanced Search, toán tử AND/OR/NOT, dấu ngoặc kép	Tìm đúng tài liệu cần trong thời gian ngắn hơn
3. Trích dẫn chuẩn APA/MLA	Zotero (miễn phí, mã nguồn mở)	Liêm chính học thuật, dễ dàng đổi chuẩn trích dẫn
4. Đánh giá độ tin cậy nguồn (CRAAP)	Khung 5 tiêu chí: Currency, Relevance, Authority, Accuracy, Purpose	Đánh giá nguồn tin có hệ thống, không chỉ dựa cảm giác
5. Làm việc nhóm mã hóa	Microsoft Teams (2FA), OneDrive Personal Vault, link chia sẻ có thời hạn	Bảo vệ dữ liệu học tập nhóm khỏi rò rỉ, chiếm quyền tài khoản
6. AI học tập có kiểm soát	Gemini for Education, VioEdu, ChatGPT Edu/for Teachers	Hỗ trợ học tập cá nhân hóa, luôn kèm bước tự kiểm chứng
7. Đạo đức học thuật thời đại AI	Quy định của trường/giáo viên về công khai sử dụng AI	Trung thực học thuật, tránh vi phạm liêm chính không chủ ý
8. Quản lý thời gian học online	Kỹ thuật Pomodoro, ứng dụng Forest, báo cáo tiến độ hằng tuần	Duy trì sự tập trung, cân bằng thời gian học và nghỉ ngơi

Tương tự các chương trước, Bảng 5.9 giúp học sinh tự kiểm tra và rà soát mức độ thực hành 8 kỹ năng đã trình bày trong chương:

Bảng 5.9. Bảng tự đánh giá kỹ năng khai thác mạng phục vụ học tập

Nội dung tự đánh giá	Có	Chưa
Em biết ít nhất 2 nền tảng học trực tuyến uy tín phù hợp với môn học của mình	☐	☐
Em có thể tự viết một câu truy vấn tìm kiếm dùng ít nhất một toán tử Boolean (AND/OR/NOT/"...")	☐	☐
Em đã từng sử dụng Zotero hoặc biết cách trích dẫn một trang web đầy đủ thông tin (tác giả, ngày, URL)	☐	☐
Em có thể tự đặt 5 câu hỏi CRAAP để đánh giá một nguồn tin trước khi sử dụng cho bài tập	☐	☐
Nhóm học tập của em dùng nền tảng có 2FA (Teams, Google Workspace) thay vì chỉ trao đổi qua Messenger/Zalo cá nhân	☐	☐
Em biết phân biệt việc dùng AI để hỗ trợ hiểu bài và việc dùng AI để làm thay bài tập	☐	☐
Em luôn tự kiểm chứng lại số liệu, trích dẫn quan trọng mà AI cung cấp trước khi dùng	☐	☐
Em biết quy định của trường/giáo viên về việc công khai sử dụng AI trong bài nộp	☐	☐
Em đã thử áp dụng kỹ thuật Pomodoro hoặc một phương pháp quản lý thời gian học tương tự	☐	☐
Em có thói quen xem lại báo cáo tiến độ học tập hằng tuần để tự điều chỉnh kế hoạch học	☐	☐

5.5. Kết luận chương

Internet mở ra cho học sinh một không gian học tập rộng lớn, nơi các em có thể tìm kiếm kiến thức, trao đổi với bạn bè, tiếp cận nhiều nguồn học liệu và sử dụng những công cụ mới như trí tuệ nhân tạo để hỗ trợ việc học. Tuy nhiên, có nhiều thông tin và công cụ trong tay chưa đồng nghĩa với việc học sẽ hiệu quả hơn. Điều quan trọng là học sinh biết lựa chọn nguồn đáng tin cậy, kiểm tra thông tin trước khi sử dụng, ghi nguồn trung thực, hợp tác an toàn và sử dụng công nghệ đúng mục đích.

Những kỹ năng được trình bày trong Chương 5 đều hướng tới một mục tiêu chung: giúp học sinh chủ động làm chủ quá trình học tập trong môi trường số. Công cụ tìm kiếm có thể giúp tìm tài liệu nhưng học sinh phải biết lựa chọn; AI có thể giải thích, gợi ý và hỗ trợ sáng tạo nhưng không thể thay thế việc suy nghĩ, kiểm chứng và tự học; các nền tảng trực tuyến có thể giúp làm việc nhóm thuận tiện hơn nhưng mỗi thành viên vẫn cần bảo vệ thông tin cá nhân và tôn trọng trách nhiệm chung.

Vì vậy, sử dụng Internet hiệu quả không phải là biết thật nhiều công cụ, mà là biết lựa chọn công cụ phù hợp, sử dụng đúng lúc, kiểm tra những gì mình nhận được và chịu trách nhiệm về những gì mình tạo ra hoặc chia sẻ. Kết hợp với những nguyên tắc an toàn, kỹ năng nhận diện rủi ro và cách ứng phó đã được trình bày ở các chương trước, các kỹ năng của Chương 5 giúp học sinh từng bước hình thành năng lực cần thiết của một người học trong thời đại số: *an toàn khi kết nối – tỉnh táo khi tiếp nhận – trung thực khi sử dụng – sáng tạo khi học tập – có trách nhiệm khi chia sẻ*.

CHƯƠNG 6. INFOGRAPHIC VÀ HÌNH ẢNH MINH HỌA

6.1. Giáo dục về đạo đức và pháp luật



Hình 6.1. Giáo dục về đạo đức và pháp luật

6.2. Kiến thức về tin học và an toàn thông tin



Hình 6.2. Kiến thức về tin học và an toàn thông tin

6.3. Nguy cơ về nội dung xấu trên mạng, bảo vệ thông tin cá nhân



Hình 6.3. Nguy cơ về nội dung xấu trên mạng, bảo vệ thông tin cá nhân

6.4. Nguy cơ về tương tác có hại với người khác



Hình 6.4. Nguy cơ về tương tác có hại với người khác

6.5. Nguy cơ về quảng cáo và tiêu dùng



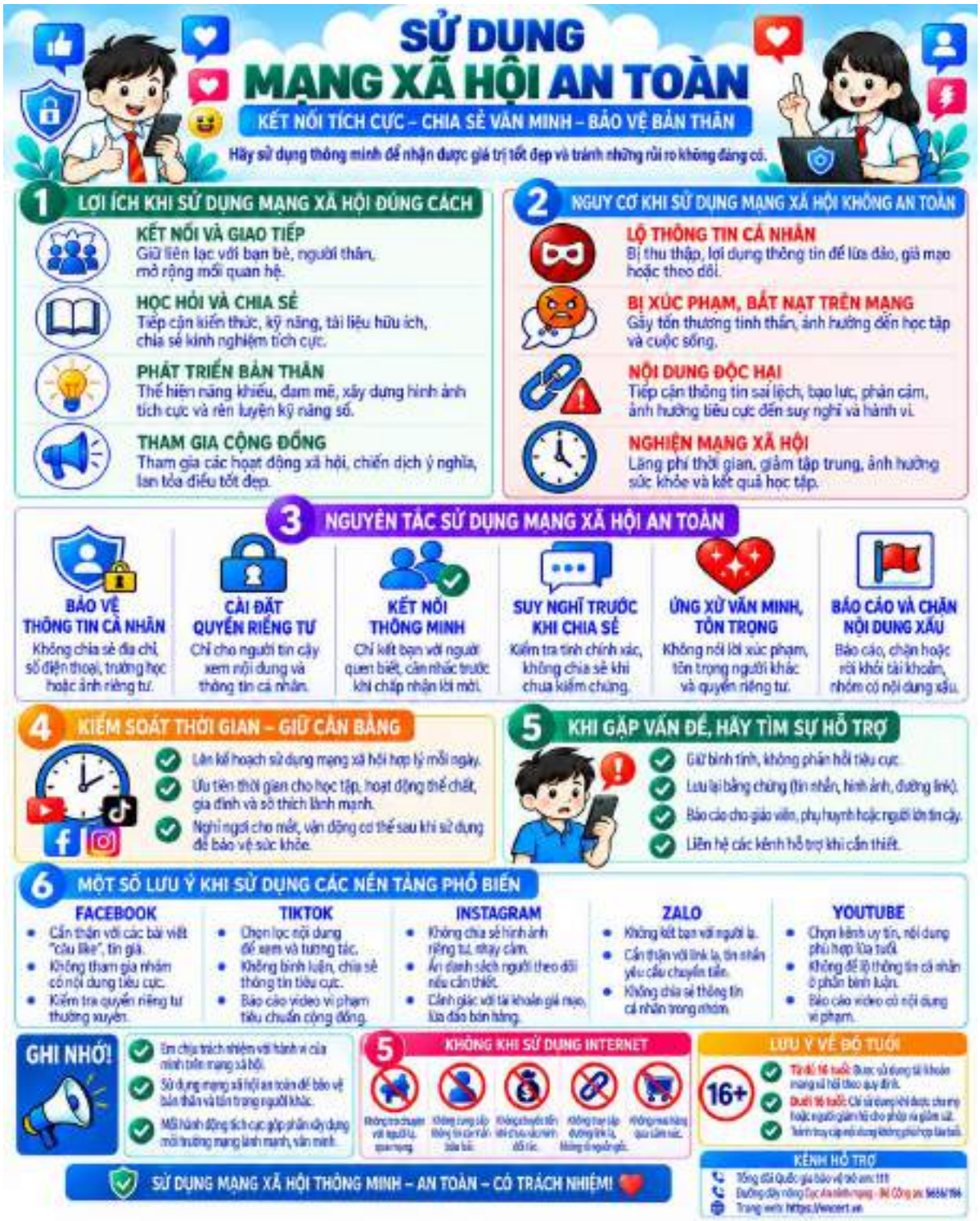
Hình 6.5. Nguy cơ về quảng cáo và tiêu dùng

6.6. Nguy cơ về an toàn thông tin



Hình 6.6. Nguy cơ về an toàn thông tin

6.7. Sử dụng mạng xã hội an toàn



Hình 6.7. Sử dụng mạng xã hội an toàn

6.8. Sử dụng an toàn thiết bị



Hình 6.8. Sử dụng an toàn thiết bị

TÀI LIỆU THAM KHẢO

[1] P. Diwanji, "'Be Internet Awesome': Helping kids make smart decisions online," Google. Accessed: Oct. 15, 2026. [Online]. Available: https://blog.google/innovation-and-ai/technology/families/be-internet-awesome-helping-kids-make-smart-decisions-online/

[2] Bộ TTTT, "Quyết định 88/QĐ-BTTTT 2025 Bộ Quy tắc ứng xử về bảo vệ trẻ em trên môi trường mạng," THƯ VIỆN PHÁP LUẬT. Accessed: Oct. 13, 2026. [Online]. Available: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Quyet-dinh-88-QD-BTTTT-2025-Bo-Quy-tac-ung-xu-ve-bao-ve-tre-em-tren-moi-truong-mang-640960.aspx

[3] Bitwarden, "Best Password Manager for Business, Enterprise & Personal," Bitwarden. Accessed: Aug. 09, 2026. [Online]. Available: https://bitwarden.com/

[4] S. Livingstone and S. Mariya, "The 4Cs: Classifying Online Risk to Children. CO:RE – Children," CO:RE Knowledge Base. Accessed: Aug. 10, 2026. [Online]. Available: https://core-evidence.eu/posts/what-are-online-risks

[5] Báo điện tử Chính phủ, "THI TỐT NGHIỆP THPT 2026: Bộ Công an khuyến nghị thí sinh, phụ huynh, giáo viên, quần chúng nhân dân," xaydungchinhsach.chinhphu.vn. Accessed: Aug. 10, 2026. [Online]. Available: https://xaydungchinhsach.chinhphu.vn/thi-tot-nghiep-thpt-2026-bo-cong-an-khuyen-nghi-thi-sinh-phu-huynh-giao-vien-va-quan-chung-nhan-dan-119260610094216595.htm

[6] T. Trang, "Từ 8h ngày 1/7, tra cứu điểm thi tốt nghiệp THPT 2026," baochinhphu.vn. Accessed: Aug. 10, 2026. [Online]. Available: https://baochinhphu.vn/tu-8h-ngay-1-7-tra-cuu-diem-thi-tot-nghiep-thpt-2026-102260630103659184.htm

[7] Báo Nhân dân, "Sở Giáo dục và Đào tạo Hà Nội hướng dẫn các kênh chính thức tra điểm thi vào lớp 10." Accessed: Aug. 10, 2026. [Online]. Available: https://phapluat.gov.vn/tin-tuc/so-giao-duc-va-dao-tao-ha-noi-huong-dan-cac-kenh-chinh-thuc-tra-diem-thi-vao-lop-10

[8] Đ.H. Thắm, "Học sinh phát tán ảnh nhạy cảm tạo bằng AI: Không chỉ là trò đùa!," muctim.tuoitre.vn. Accessed: Aug. 10, 2026. [Online]. Available: https://muctim.tuoitre.vn/hoc-sinh-phat-tan-anh-nhay-cam-tao-bang-ai-khong-chi-la-tro-dua-101260502171859118.htm

[9] S. Vosloo, "Digital misinformation/disinformation and children | Office of Strategy and Evidence Innocenti." Accessed: Aug. 10, 2026. [Online]. Available: https://www.unicef.org/innocenti/stories/digital-misinformationdisinformation-and-children

[10] VOV, "Công an cảnh báo việc thế chấp clip, hình ảnh nhạy cảm để vay tiền." Accessed: Aug. 10, 2026. [Online]. Available: https://vov.gov.vn/cong-an-canh-bao-viec-the-chap-clip-hinh-anh-nhay-cam-de-vay-tien-dtnew-1070926

[11] H. Trang and N. Anh, "Cảnh giác trước thủ đoạn "bắt cóc online"." Accessed: Oct. 13, 2026. [Online]. Available: https://bocongan.gov.vn/bai-viet/canh-giac-thu-doan-bat-coc-online-gia-danh-cong-an-co-lap-sinh-vien-de-chiem-doat-tien-1791168262

[12] T. Mỹ and N. Ngọc, "Khởi tố đối tượng cưỡng đoạt tài sản bằng video clip 'nhạy cảm,'" 2026, Accessed: Aug. 10, 2026. [Online]. Available: https://bocongan.gov.vn/bai-viet/khoi-to-doi-tuong-cuong-doat-tai-san-bang-video-clip-nhay-cam-1779624726

[13] N.H.M. An, H.T.M. Sang, L.T. Sơn, L.T.T. Anh, N.T.K. Khanh, and N.V. Tuy, "Nghiện mạng xã hội và hành vi tự gây tổn thương không tự sát ở học sinh trung học phổ thông: Phân tích trung gian nối tiếp," *Tạp Chí Nghiên Cứu Y Học*, vol. 203, no. 6, pp. 899–906, Jul. 2026, doi: 10.52852/tcncyh.v203i6.5578.

[14] S. Dodd *et al.*, "School-based peer education interventions to improve health: a global systematic review of effectiveness," *BMC Public Health*, vol. 22, no. 1, p. 2247, Dec. 2022, doi: 10.1186/s12889-022-14688-3.

[15] Báo Điện tử Chính phủ, "Trao giải cuộc thi 'Học sinh với An ninh mạng 2026' trên toàn quốc," baochinhphu.vn. Accessed: Sep. 30, 2026. [Online]. Available: https://baochinhphu.vn/trao-giai-cuoc-thi-hoc-sinh-voi-an-ninh-mang-2026-tren-toan-quoc-102260424112707066.htm

[16] Báo Điện tử Chính phủ, "Khởi tố 2 nữ sinh trong vụ bạo lực học đường ở Phú Thọ," baochinhphu.vn. Accessed: Oct. 13, 2026. [Online]. Available: https://baochinhphu.vn/khoi-to-2-nu-sinh-trong-vu-bao-luc-hoc-duong-o-phu-tho-102260523075609334.htm

[17] Cục An ninh mạng, "Hệ thống phòng, chống tin nhắn rác, cuộc gọi rác." Accessed: Oct. 13, 2026. [Online]. Available: https://nospam.vncert.vn/

[18] S. Blakeslee, "The CRAAP Test," *LOEX Q.*, vol. 31, no. 3, Oct. 2004, [Online]. Available: https://commons.emich.edu/loexquarterly/vol31/iss3/4

[19] G. M. U. Libraries, "Evaluating Resources: The CRAAP Test | University Libraries." Accessed: Aug. 11, 2026. [Online]. Available: https://library.gmu.edu/tutorials/craap_test

[20] OpenAI, "ChatGPT có an toàn cho mọi lứa tuổi không?," OpenAI Help Center. Accessed: Oct. 14, 2026. [Online]. Available: https://help.openai.com/vi-vn/articles/8313401-is-chatgpt-safe-for-all-ages

[21] Niall, "How Old Do You Have to Be to Use Claude AI? (Parent Guide)," AI Tools for Kids. Accessed: Oct. 14, 2026. [Online]. Available: https://aitoolsforkids.com/blog/how-old-to-use-claude-ai

BẢNG PHÂN LOẠI NGUỒN THAM KHẢO

Nguồn	Dành cho	Nội dung
[1] Be Internet Awesome	[HS/GV]	Nội dung giáo dục an toàn mạng cho trẻ em.
[2] Bộ Quy tắc ứng xử bảo vệ trẻ em	[GV/CMHS]	Văn bản pháp lý, ngôn ngữ tương đối khó với học sinh nhỏ.
[3] Bitwarden	[HS THCS–THPT/GV]	Công cụ kỹ thuật; không cần thiết cho tiểu học tự đọc.
[4] Khung 4C – CO:RE	[GV]	Tài liệu nghiên cứu/chuyên môn.
[5]–[7] Cảnh báo, tra cứu thi	[HS THCS–THPT/GV]	Phù hợp với học sinh lớn hơn, đặc biệt THPT.
[8] Ảnh riêng tư tạo bằng AI	[GV/CMHS]	Chủ đề nhạy cảm; không nên để học sinh nhỏ tự mở.
[9] UNICEF về thông tin sai lệch	[HS THCS–THPT/GV]	Có thể dùng cho học sinh lớn với hướng dẫn.
[10] Nội dung riêng tư dùng để vay tiền	[GV/CMHS]	Chủ đề nhạy cảm.
[11] "Bắt cóc online"	[GV/CMHS; HS THPT có hướng dẫn]	Nội dung về đe dọa, lừa đảo nghiêm trọng.

[12] Cưỡng đoạt bằng video riêng tư	[GV/CMHS]	Nội dung vụ án và thông tin nhạy cảm.
[13] Nghiên cứu về hành vi tự gây tổn thương	[GV/CBQL]	Nội dung nghiên cứu sức khỏe tâm lý không phù hợp để học sinh nhỏ tự đọc.
[14] Nghiên cứu giáo dục đồng đẳng	[GV/CBQL]	Nguồn nghiên cứu chuyên môn.
[15] Cuộc thi Học sinh với An ninh mạng	[HS/GV]	Nội dung phù hợp với học sinh.
[16] Khởi tố nữ sinh trong vụ bạo lực học đường	[GV/CMHS]	Vụ việc pháp lý liên quan học sinh, không cần học sinh nhỏ tự truy cập.
[17] Hệ thống chống tin nhắn/cuộc gọi rác	[HS THCS–THPT/GV/CMHS]	Nguồn hỗ trợ thực hành.
[18]–[19] CRAAP Test	[HS THPT/GV]	Nội dung học thuật, phù hợp học sinh lớn.
[20] Điều kiện độ tuổi ChatGPT	[HS THCS–THPT/GV/CMHS]	Liên quan trực tiếp đến việc sử dụng AI theo độ tuổi.
[21] Hướng dẫn tuổi sử dụng Claude	[GV/CMHS]	Chủ yếu phục vụ lựa chọn công cụ cho học sinh.

PHỤ LỤC

Các kênh hỗ trợ khi gặp sự cố

STT	Thông tin hỗ trợ	Mã QRCode
1	**Tổng đài 111** **Tổng đài Quốc gia Bảo vệ Trẻ em, Cục Bà mẹ và Trẻ em** **Website: https://tongdai111.vn**	
2	**Tổng đài 156/5656** **Hệ thống phòng, chống tin rác, cuộc gọi rác, Cục An ninh mạng – Bộ Công an.** **Website: https://nospam.vncert.vn/**	
3	**Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam** **thuộc Cục An ninh mạng – Bộ Công an** **Website: https://vncert.vn**	

Giải thích một số thuật ngữ

Thuật ngữ trong tài liệu	Cách gọi dễ hiểu	Giải thích dành cho học sinh	Ví dụ gần gũi
AI – Artificial Intelligence	Trí tuệ nhân tạo	Công nghệ giúp máy tính thực hiện một số công việc thường cần đến khả năng của con người như nhận diện hình ảnh, tạo văn bản hoặc trả lời câu hỏi.	AI giúp giải thích một bài toán hoặc gợi ý dàn ý bài thuyết trình.
2FA – Two-Factor Authentication	Xác thực hai lớp	Ngoài mật khẩu, tài khoản yêu cầu thêm một bước xác minh để chắc chắn người đăng nhập đúng là chủ tài khoản.	Sau khi nhập mật khẩu, em còn phải nhập mã gửi về điện thoại.
OTP – One-Time Password	Mã dùng một lần	Mã xác thực chỉ có giá trị trong thời gian ngắn và thường chỉ dùng một lần. Đây là thông tin bí mật.	Ngân hàng gửi mã 6 số để xác nhận giao dịch. Không đọc mã này cho người khác.
Trình quản lý mật khẩu	Kho giữ mật khẩu an toàn	Công cụ giúp tạo, lưu và tự động điền các mật khẩu khác nhau cho nhiều tài khoản.	Em chỉ cần nhớ mật khẩu chính để mở kho chứa các mật khẩu khác.
Report	Báo cáo	Chức năng dùng để thông báo cho nền tảng biết một tài khoản hoặc nội dung có dấu hiệu vi phạm.	Báo cáo một tài khoản giả mạo hoặc đang quấy rối.
Block	Chặn	Ngăn một tài khoản tiếp tục liên hệ hoặc tương tác với mình.	Chặn người lạ liên tục gửi tin nhắn gây khó chịu.
Phishing	Lừa đảo giả mạo	Kẻ xấu giả làm người hoặc tổ chức đáng tin để dụ người dùng bấm liên kết, nhập mật khẩu, OTP hoặc cung cấp thông tin.	Tin nhắn giả danh nhà trường: “Bấm vào đây để xem điểm thi”.
Smishing	Lừa đảo qua tin nhắn	Một dạng phishing được thực hiện qua SMS hoặc ứng dụng nhắn tin.	Tin nhắn Zalo giả danh giáo viên yêu cầu đăng nhập vào một đường link lạ.
Malware	Mã độc/phần mềm độc hại	Phần mềm được tạo ra để gây hại, đánh cắp thông tin, theo dõi hoặc chiếm quyền thiết bị.	Tải một ứng dụng lạ rồi điện thoại liên tục bật quảng cáo và tài khoản bị đăng nhập bất thường.

Virus máy tính	Phần mềm gây hại có khả năng lây lan	Một loại mã độc có thể gắn vào tệp hoặc chương trình và lan sang dữ liệu khác khi được kích hoạt.	Một tệp tải từ nguồn lạ làm nhiều tệp trong máy bị lỗi.
Antivirus	Phần mềm chống mã độc	Công cụ giúp phát hiện, cảnh báo hoặc xử lý một số phần mềm có khả năng gây hại.	Công cụ bảo mật cảnh báo khi em tải một tệp đáng ngờ.
Game mod	Bản game đã chỉnh sửa	Phiên bản trò chơi được thay đổi so với bản gốc. Có bản mod hợp lệ nhưng bản tải từ nguồn lạ có thể chứa mã độc.	Một bản mod thay giao diện hoặc thêm bản đồ mới.
Game hack	Can thiệp trái phép vào game	Sử dụng công cụ hoặc cách thức không được nhà phát hành cho phép để thay đổi trò chơi hoặc tài khoản.	Can thiệp để có thêm tiền ảo trái quy định.
Cheat	Gian lận trong trò chơi	Dùng mã hoặc công cụ để có lợi thế không công bằng so với người chơi khác.	Công cụ tự ngắm mục tiêu trong trò chơi.
Crack	Bản phần mềm bị phá cơ chế bảo vệ	Phần mềm đã bị sửa để bỏ giới hạn bản quyền hoặc mở tính năng trả phí trái phép; có nguy cơ chứa mã độc.	Tải bản "phần mềm trả phí miễn phí" từ website lạ.
Deepfake	Hình/giọng/video giả bằng AI	Nội dung được AI tạo hoặc chỉnh sửa để mô phỏng khuôn mặt, giọng nói hay hành động của người thật.	Cuộc gọi có hình và giọng giống người thân nhưng thực ra được làm giả.
Cyberbullying	Bắt nạt trên mạng	Hành vi dùng mạng xã hội, tin nhắn hoặc nền tảng số để xúc phạm, chế giễu, đe dọa hoặc cô lập người khác.	Cả nhóm cùng đăng bình luận chế giễu một bạn trong lớp.
Grooming	Dụ dỗ, tạo lòng tin để gây hại	Quá trình một người từng bước làm quen, tạo lòng tin rồi gây áp lực hoặc lợi dụng trẻ em.	Người quen qua game tặng quà, xin giữ bí mật rồi yêu cầu gửi ảnh riêng tư.

Sexual extortion (thường gọi là Sextortion)	Đe dọa, ép buộc bằng nội dung riêng tư.	Một người dùng hoặc đe dọa phát tán nội dung riêng tư, nhạy cảm để gây áp lực, buộc người khác làm theo yêu cầu, cung cấp thêm nội dung hoặc chuyển tiền.	Một người đe dọa sẽ gửi hình ảnh riêng tư của học sinh cho bạn bè nếu em không làm theo yêu cầu (ví dụ chuyển tiền).
Tin giả – Fake news	Thông tin giả	Nội dung sai hoặc gây hiểu nhầm được trình bày giống như thông tin thật.	Bài đăng giả thông báo "Ngày mai toàn trường nghỉ học".
Misinformation	Thông tin sai không chủ ý	Thông tin không chính xác được chia sẻ bởi người tưởng rằng nó là đúng.	Chia sẻ lại lịch thi cũ vì tưởng đó là lịch năm nay.
Disinformation	Thông tin sai có chủ ý	Thông tin sai được cố tình tạo và lan truyền nhằm đánh lừa người khác.	Tạo thông báo giả của nhà trường để khiến học sinh hoang mang.
Khung 4C	Bốn nhóm rủi ro trên mạng	Cách phân loại rủi ro trẻ em gặp trên mạng thành Content, Contact, Conduct và Contract.	Nội dung độc hại thuộc Content; người lạ tiếp cận trẻ thuộc Contact.
Content risk	Rủi ro từ nội dung	Nguy cơ khi trẻ nhìn thấy hoặc tiếp nhận nội dung không phù hợp hoặc gây hại.	Video bạo lực hoặc thông tin sai lệch.
Contact risk	Rủi ro từ người khác tiếp cận	Nguy cơ khi trẻ bị người khác tiếp cận trên mạng với mục đích không phù hợp.	Người lạ nhắn tin xin ảnh riêng tư.
Conduct risk	Rủi ro từ hành vi	Nguy cơ phát sinh từ hành vi của trẻ hoặc người khác trong tương tác trực tuyến.	Chia sẻ ảnh của bạn mà chưa được phép.
Contract risk	Rủi ro thương mại/giao dịch	Nguy cơ liên quan đến mua bán, dữ liệu, quảng cáo hoặc giao dịch trực tuyến.	Website dụ nhập thông tin để nhận quà miễn phí.
Sandbox	"Hộp cát" bảo vệ ứng dụng	Cơ chế tách các ứng dụng khỏi nhau để một ứng dụng khó tự ý truy cập dữ liệu của ứng dụng khác.	Một ứng dụng trên iPhone không thể tùy ý đọc dữ liệu của ứng dụng khác.

Firewall	Tường lửa	Cơ chế kiểm soát luồng dữ liệu ra vào thiết bị hoặc mạng nhằm hạn chế kết nối không mong muốn.	Máy tính chặn một chương trình lạ đang cố kết nối Internet.
VPN – Virtual Private Network	Mạng riêng ảo	Công nghệ tạo một kết nối được bảo vệ hơn giữa thiết bị và mạng Internet.	Khi dùng Wi-Fi công cộng, VPN có thể giúp bảo vệ dữ liệu truyền qua mạng.
DNS – Domain Name System	"Danh bạ" của Internet	Hệ thống giúp chuyển tên website dễ nhớ thành địa chỉ mà máy tính có thể sử dụng để kết nối.	Em gõ tên một website, DNS giúp thiết bị tìm đúng máy chủ của website đó.
Wi-Fi công cộng	Mạng Wi-Fi dùng chung	Mạng không dây ở nơi công cộng mà nhiều người có thể cùng sử dụng và cần thận trọng khi truyền thông tin quan trọng.	Wi-Fi miễn phí ở quán cà phê hoặc sân bay.
Mã hóa – Encryption	Biến dữ liệu thành dạng khó đọc	Cách biến thông tin thành dạng người không có quyền khó đọc được.	Tin nhắn được mã hóa trước khi truyền đi.
Parental control	Công cụ cha mẹ quản lý	Tính năng giúp cha mẹ giới hạn thời gian, ứng dụng hoặc nội dung phù hợp với độ tuổi của con.	Cha mẹ đặt giới hạn một giờ chơi game mỗi ngày.
Restrictive mediation	Đặt giới hạn và quy tắc	Cha mẹ thống nhất những việc con được làm, không nên làm hoặc cần giới hạn khi sử dụng Internet.	Quy định không dùng điện thoại sau 22 giờ.
Active mediation	Cùng trao đổi và hướng dẫn	Cha mẹ trò chuyện, giải thích và cùng con xử lý những điều gặp trên mạng.	Hai mẹ con cùng kiểm tra một tin nhắn đáng ngờ.
Technical mediation	Hỗ trợ bằng công cụ kỹ thuật	Cha mẹ sử dụng tính năng hoặc phần mềm để hỗ trợ bảo vệ trẻ khi dùng thiết bị.	Bật giới hạn thời gian hoặc bộ lọc nội dung.
Boolean Search	Tìm kiếm bằng cách kết hợp từ khóa	Cách dùng AND, OR, NOT và các ký hiệu khác để thu hẹp hoặc mở rộng kết quả tìm kiếm.	"an toàn mạng" AND "học sinh"
AND	Tìm cả hai	Yêu cầu kết quả có đồng thời các từ khóa cần tìm.	an toàn mạng AND học sinh

OR	Tìm một trong hai	Mở rộng kết quả để nhận các trang chứa một trong các từ khóa.	cyberbullying OR "bắt nạt mạng"
NOT / dấu trừ (-)	Loại từ không muốn tìm	Loại bỏ các kết quả chứa từ khóa gây nhiễu.	"an toàn mạng" -game
Dấu ngoặc kép "..."	Tìm đúng cụm từ	Yêu cầu công cụ tìm kiếm giữ nguyên cụm từ và thứ tự các từ.	"Bộ Quy tắc ứng xử về bảo vệ trẻ em trên môi trường mạng"
site:	Chỉ tìm trong một website/tên miền	Giới hạn kết quả vào một website hoặc một nhóm tên miền nhất định.	an toàn mạng site:moet.gov.vn
filetype:	Tìm theo loại tệp	Giới hạn kết quả ở một định dạng tệp như PDF.	an toàn mạng filetype:pdf
intitle:	Tìm từ trong tiêu đề	Tìm các trang có từ hoặc cụm từ xuất hiện trong tiêu đề.	intitle:"an toàn mạng"
CRAAP Test	Năm câu hỏi kiểm tra nguồn	Khung đánh giá nguồn dựa trên mức độ cập nhật, liên quan, thẩm quyền, chính xác và mục đích.	Trước khi dùng một bài viết, hỏi: mới không, đúng việc không, ai nói, có bằng chứng không, nói để làm gì?
Currency	Tính cập nhật	Kiểm tra thông tin được đăng hoặc cập nhật khi nào.	Một quy định pháp luật năm 2020 có thể đã được thay thế.
Relevance	Mức độ liên quan	Xem nguồn có thực sự phù hợp với câu hỏi hoặc bài học hay không.	Bài viết về sinh viên có thể không phù hợp nếu em đang nghiên cứu học sinh tiểu học.
Authority	Độ tin cậy của người/đơn vị cung cấp	Kiểm tra ai viết hoặc tổ chức nào chịu trách nhiệm về nội dung.	Thông tin tuyển sinh nên ưu tiên nguồn của Bộ, Sở hoặc trường.
Accuracy	Độ chính xác	Kiểm tra nội dung có bằng chứng, nguồn dẫn và có thể đối chiếu hay không.	Một số liệu có dẫn báo cáo gốc đáng tin hơn số liệu không ghi nguồn.
Purpose	Mục đích của nội dung	Xem nội dung được tạo để cung cấp kiến thức, quảng cáo, thuyết phục hay gây ảnh hưởng.	Một bài quảng cáo khóa học có thể nhấn mạnh lợi ích để thuyết phục người mua.

APA	Chuẩn trích dẫn tác giả – năm	Cách trình bày nguồn tham khảo thường dùng trong khoa học xã hội, giáo dục và tâm lý.	Trong bài có thể ghi (Nguyễn, 2026).
MLA	Chuẩn trích dẫn tác giả – trang	Cách trình bày nguồn thường dùng trong ngôn ngữ và văn học.	Trong bài có thể ghi (Nguyễn 25).
Prompt	Yêu cầu gửi cho AI	Câu lệnh, câu hỏi hoặc hướng dẫn người dùng đưa cho AI để AI thực hiện một nhiệm vụ.	"Giải thích vòng tuần hoàn nước cho học sinh lớp 5 bằng 5 câu."
Prompt Engineering	Cách viết yêu cầu cho AI	Kỹ năng diễn đạt yêu cầu rõ ràng, cung cấp đủ bối cảnh và nói rõ kết quả mong muốn.	Thay vì hỏi "Toán", yêu cầu: "Giải thích phân số bằng ví dụ chia bánh cho học sinh lớp 4."
Ảo giác AI – AI hallucination	AI "bịa" nhưng nói như thật	Hiện tượng AI tạo ra thông tin nghe hợp lý và tự tin nhưng thực tế sai hoặc không tồn tại.	AI đưa ra tên một cuốn sách hoặc số liệu không có thật.
Kiểm chứng đầu ra AI	Kiểm tra lại câu trả lời của AI	Đối chiếu thông tin AI cung cấp với sách, tài liệu chính thức hoặc nguồn đáng tin cậy khác trước khi sử dụng.	AI nói một ngày lịch sử; em kiểm tra lại trong SGK hoặc website chính thức.
Pomodoro	Học tập theo phiên tập trung	Cách chia thời gian học thành các khoảng tập trung ngắn, xen kẽ nghỉ.	Học 25 phút, nghỉ 5 phút; sau vài phiên thì nghỉ lâu hơn.
"Phần thưởng biến đổi"	Phần thưởng xuất hiện khó đoán	Khi nội dung thú vị, lượt thích hoặc thông báo xuất hiện không cố định, người dùng dễ muốn kiểm tra tiếp để xem điều gì sẽ xuất hiện.	Em định xem một video nhưng tiếp tục cuộn vì không biết video thú vị tiếp theo xuất hiện lúc nào.