BỘ GIÁO DỤC VÀ ĐÀO TẠO	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số3308/QĐ-BGDĐT	*Hà Nội, ngày 12 tháng 11 năm 2026*

QUYẾT ĐỊNH
Phê duyệt Tài liệu tập huấn cho giáo viên về hỗ trợ học sinh tương tác an toàn trên không gian mạng

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 Kế hoạch số 1028/KH-BGDĐT ngày 15/6/2026 của Bộ Giáo dục và Đào tạo về triển khai các nhiệm vụ thuộc Dự án Học tập và Kỹ năng cho trẻ em năm 2026;

Căn cứ Quyết định số 3104/QĐ-BGDĐT ngày 23/10/2026 của Bộ trưởng Bộ Giáo dục và Đào tạo về việc thành lập Hội đồng thẩm định Tài liệu tập huấn cho giáo viên về hỗ trợ học sinh tương tác an toàn trên không gian mạng;

Căn cứ Biên bản họp Hội đồng thẩm định tài liệu ngày 28/10/2026;

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

QUYẾT ĐỊNH:

Điều 1. Phê duyệt Tài liệu tập huấn cho giáo viên về hỗ trợ học sinh tương tác an toàn trên không gian mạng *(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./.

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.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

BỘ GIÁO DỤC ĐÀO TẠO

Nguyễn Thị Quyên Thanh

BỘ GIÁO DỤC VÀ ĐÀO TẠO

TÀI LIỆU TẬP HUẤN

CHO GIÁO VIÊN VỀ HỖ TRỢ HỌC SINH TƯƠNG TÁC AN TOÀN TRÊN KHÔNG GIAN MẠNG

Hà Nội, năm 2026



BỘ GIÁO DỤC VÀ ĐÀO TẠO

TÀI LIỆU TẬP HUẤN

CHO GIÁO VIÊN VỀ HỖ TRỢ HỌC SINH TƯƠNG TÁC AN TOÀN TRÊN KHÔNG GIAN MẠNG

Ban biên soạn:

Nguyễn Thị Nhung

Nguyễn Đức Giang

Âu Thanh Ngọc

Lê Thị Hoàng Lan

Tạ Văn Hai

Lưu Thị Nhung

Hà Nội, năm 2026

LỜI NÓI ĐẦU

Hiện nay, không gian mạng đã trở thành một môi trường sống, học tập và giao tiếp thường nhật của học sinh Việt Nam. Bên cạnh những cơ hội to lớn về tiếp cận tri thức, kết nối và sáng tạo, không gian mạng cũng đặt học sinh trước nhiều nguy cơ ngày càng đa dạng và tinh vi: lừa đảo và chiếm đoạt tài khoản, lộ lọt dữ liệu cá nhân, sử dụng thiết bị số quá mức, tin giả và thông tin xấu độc, bắt nạt trực tuyến, xâm hại và bóc lột tình dục trực tuyến, các "thử thách" nguy hiểm, cờ bạc trá hình, nội dung giả mạo do trí tuệ nhân tạo tạo ra và những tác động bất lợi đối với sức khỏe tinh thần. Những nguy cơ này không chỉ là vấn đề kỹ thuật mà là vấn đề giáo dục, gắn trực tiếp với sự phát triển nhân cách và sự an toàn của người học.

Trong bối cảnh đó, Đảng và Nhà nước đã ban hành nhiều chủ trương, chính sách về bảo vệ trẻ em trên môi trường mạng, tiêu biểu là Luật Trẻ em năm 2016, Luật An ninh mạng năm 2025, Luật Bảo vệ dữ liệu cá nhân năm 2025 và Chương trình "Bảo vệ và hỗ trợ trẻ em phát triển trên môi trường mạng giai đoạn 2026 – 2030" ban hành kèm theo Quyết định số 468/QĐ-TTg ngày 23/3/2026 của Thủ tướng Chính phủ. Ngành Giáo dục đã ban hành Khung năng lực số cho người học (Thông tư số 02/2025/TT-BGDĐT), trong đó "An toàn" là một miền năng lực, và hướng dẫn về công tác tư vấn học đường, công tác xã hội trong trường học (Thông tư số 18/2025/TT-BGDĐT).

Giáo viên là người tiếp xúc với học sinh thường xuyên nhất, có điều kiện thuận lợi nhất để giáo dục, sớm nhận ra những thay đổi bất thường và là chỗ dựa tin cậy khi học sinh gặp sự cố. Tuy nhiên, kết quả khảo sát thực tiễn cho thấy nhiều giáo viên còn lúng túng khi tổ chức các hoạt động giáo dục mang tính thực hành, khi tiếp nhận chia sẻ của học sinh về một sự cố trực tuyến và khi phối hợp với cha mẹ học sinh, các lực lượng xã hội để xử lý vụ việc.

Thực hiện Kế hoạch số 1028/KH-BGDĐT ngày 15/6/2026 của Bộ Giáo dục và Đào tạo về triển khai các nhiệm vụ thuộc Dự án Học tập và Kỹ năng cho trẻ em năm 2026, Ban biên soạn xây dựng tài liệu "Tài liệu tập huấn cho giáo viên về hỗ trợ học sinh tương tác an toàn trên không gian mạng". Trọng tâm của tài liệu là phát triển năng lực của giáo viên trên bốn phương diện: (1) giáo dục học sinh kỹ năng tương tác an toàn; (2) phát hiện sớm dấu hiệu học sinh gặp nguy cơ,

sự cố; (3) hỗ trợ ban đầu và xử lý đúng quy trình; (4) phối hợp với cha mẹ học sinh và các lực lượng liên quan.

Tài liệu được biên soạn trên cơ sở kế thừa các tài liệu tập huấn đã có, kết quả các nghiên cứu khoa học giáo dục trong nước về giáo dục kỹ năng an toàn trên không gian mạng cho học sinh và các công trình, khuyến nghị quốc tế có uy tín. Ban biên soạn đã chú trọng đảm bảo tính khoa học, cập nhật, phù hợp với bối cảnh pháp lý và thực tiễn nhà trường Việt Nam.

Dù đã rất cố gắng, tài liệu khó tránh khỏi thiếu sót. Ban biên soạn mong nhận được ý kiến góp ý của các nhà khoa học, cán bộ quản lý và giáo viên để tài liệu tiếp tục được hoàn thiện.

BAN BIÊN SOẠN

MỤC LỤC

LỜI NÓI ĐẦU 1
DANH MỤC TỪ VIẾT TẮT 8
HƯỚNG DẪN SỬ DỤNG TÀI LIỆU 9
1. Đối tượng sử dụng 9
2. Cấu trúc tài liệu 9
3. Quy ước trình bày 9
4. Cách sử dụng tài liệu 9
5. Lưu ý về đạo đức khi sử dụng tài liệu 10
MỤC TIÊU VÀ KẾ HOẠCH TẬP HUẤN 11
1. Mục tiêu tập huấn 11
1.1. Về kiến thức 11
1.2. Về năng lực 11
1.3. Về phẩm chất 11
2. Kế hoạch và phân bổ thời lượng 11
CHUYÊN ĐỀ 1. HỌC SINH TRONG MÔI TRƯỜNG SỐ VÀ KHUNG BẢO VỆ HỌC SINH TRÊN KHÔNG GIAN MẠNG Ở VIỆT NAM 13
1.1. Một số khái niệm cơ bản 14
1.1.1. Không gian mạng 14
1.1.2. An toàn trên không gian mạng và kỹ năng an toàn trên không gian mạng 14
1.1.3. Tương tác an toàn trên không gian mạng 15
1.1.4. Giáo dục kỹ năng an toàn trên không gian mạng 15
1.2. Đặc điểm phát triển tâm sinh lý của học sinh và hành vi trực tuyến 15
1.2.1. Vì sao giáo viên cần hiểu đặc điểm phát triển của học sinh? 15
1.2.2. Đặc điểm theo cấp học và hàm ý đối với giáo viên 17
1.2.3. Sự khác biệt giữa tương tác trực tuyến và trực tiếp 18
1.3. Thực trạng học sinh Việt Nam trên không gian mạng 18
1.3.1. Mức độ tiếp cận và các hoạt động trực tuyến 18
1.3.2. Nhận thức và trải nghiệm rủi ro của học sinh 19
1.3.3. Thực trạng giáo dục kỹ năng an toàn trên không gian mạng trong nhà trường 19
1.4. Khung pháp lý và trách nhiệm của nhà trường, giáo viên 20
1.4.1. Các văn bản pháp luật, chính sách chủ yếu 20
1.4.2. Trách nhiệm của nhà trường 22
1.4.3. Trách nhiệm của giáo viên (được làm gì, phải làm gì, không được làm gì) 23
CHUYÊN ĐỀ 2. NHẬN DIỆN CÁC NGUY CƠ PHỔ BIẾN ĐỐI VỚI HỌC SINH TRÊN KHÔNG GIAN MẠNG 26
2.1. Khung phân loại nguy cơ trực tuyến 4C 26

2.2. Lừa đảo trực tuyến và chiếm đoạt tài khoản 28
2.2.1. Bản chất 28
2.2.2. Biểu hiện thường gặp ở học sinh 28
2.2.3. Dấu hiệu cảnh báo 29
2.2.4. Phòng ngừa 29
2.3. Lộ lọt dữ liệu cá nhân và xâm phạm quyền riêng tư 29
2.3.1. Bản chất 29
2.3.2. Biểu hiện thường gặp ở học sinh 30
2.3.3. Phòng ngừa 30
2.4. Sử dụng thiết bị số quá mức, nghiện trò chơi điện tử và mạng xã hội 30
2.4.1. Bản chất 30
2.4.2. Dấu hiệu cảnh báo 31
2.4.3. Phòng ngừa 31
2.5. Tin giả, thông tin sai sự thật và nội dung có hại 31
2.5.1. Bản chất 31
2.5.2. Biểu hiện thường gặp ở học sinh 32
2.5.3. Phòng ngừa 32
2.6. "Thử thách" nguy hiểm, cờ bạc và cá cược trực tuyến 32
2.6.1. "Thử thách" nguy hiểm 32
2.6.2. Cờ bạc và cá cược trực tuyến, các hình thức trá hình 33
2.7. Nội dung do trí tuệ nhân tạo tạo ra 33
2.7.1. Bản chất 33
2.7.2. Phòng ngừa 34
2.8. Bắt nạt trực tuyến 34
2.8.1. Bản chất 34
2.8.2. Tác động 34
2.8.3. Dấu hiệu cảnh báo 35
2.8.4. Phòng ngừa 35
2.9. Xâm hại và bóc lột tình dục trẻ em trực tuyến 35
2.9.1. Bản chất và các hình thức 35
2.9.2. Quá trình dụ dỗ trực tuyến 36
2.9.3. Chia sẻ hình ảnh nhạy cảm ở học sinh 37
2.9.4. Dấu hiệu cảnh báo 37
2.9.5. Phòng ngừa 37
2.10. Môi trường số và sức khỏe tinh thần của học sinh 37
2.10.1. Bản chất 37
2.10.2. Các cơ chế tác động tiêu cực cần lưu ý 38

2.10.3. Mặt tích cực cần phát huy 38
2.10.4. Phòng ngừa 38
2.11. Văn hóa ứng xử trên không gian mạng – yếu tố bảo vệ chung 38
CHUYÊN ĐỀ 3. GIÁO DỤC KỸ NĂNG TƯƠNG TÁC AN TOÀN TRÊN KHÔNG GIAN MẠNG CHO HỌC SINH 41
3.1. Mục tiêu và yêu cầu cần đạt theo cấp học 41
3.2. Hệ thống kỹ năng thành phần 43
3.3. Nguyên tắc giáo dục 45
3.4. Con đường và hình thức giáo dục 45
3.4.1. Tích hợp trong các môn học 45
3.4.2. Hoạt động trải nghiệm, hướng nghiệp 46
3.4.3. Sinh hoạt lớp, sinh hoạt theo quy mô lớp/khối/toàn trường 47
3.4.4. Câu lạc bộ, ngày hội, hoạt động ngoại khóa 47
3.5. Phương pháp và kỹ thuật giáo dục 47
3.5.1. Chu trình học tập trải nghiệm 47
3.5.2. Các phương pháp, kỹ thuật chủ yếu 48
3.5.3. Lưu ý khi giáo dục các chủ đề nhạy cảm 49
3.6. Đánh giá kết quả giáo dục 49
3.6.1. Định hướng đánh giá 49
3.6.2. Các công cụ đánh giá 49
3.6.3. Ví dụ rubric đánh giá kỹ năng ứng phó 50
CHUYÊN ĐỀ 4. PHÁT HIỆN, HỖ TRỢ VÀ XỬ LÝ BAN ĐẦU KHI HỌC SINH GẶP SỰ CỐ TRÊN KHÔNG GIAN MẠNG 53
4.1. Vai trò, phạm vi và giới hạn của giáo viên 53
4.1.1. Vì sao giáo viên giữ vị trí then chốt? 53
4.1.2. Vai trò của giáo viên trong xử lý sự cố 54
4.1.3. Giới hạn của giáo viên 54
4.1.4. Các nguyên tắc nền tảng 54
4.2. Nhận biết dấu hiệu học sinh gặp nguy cơ, sự cố 54
4.2.1. Các nhóm dấu hiệu 54
4.2.2. Dấu hiệu khủng hoảng cần can thiệp khẩn cấp 55
4.2.3. Các kênh phát hiện 56
4.3. Tiếp nhận chia sẻ, tiết lộ của học sinh 56
4.3.1. Đặc điểm của việc tiết lộ 56
4.3.2. Các bước tiếp nhận 56
4.3.3. Những câu nên nói và không nên nói 57
4.3.4. Trường hợp học sinh yêu cầu giữ bí mật 57

4.4. Hỗ trợ tâm lý ban đầu 58
4.5. Quy trình xử lý chung 58
4.5.1. Phân loại mức độ sự việc 58
4.5.2. Các bước xử lý 59
4.6. Hướng dẫn xử lý theo từng loại sự cố 61
4.6.1. Bắt nạt trực tuyến 62
4.6.2. Lừa đảo, mất tài khoản, mất tiền 62
4.6.3. Lộ lọt thông tin cá nhân, hình ảnh bị phát tán (không mang tính nhạy cảm tình dục) . 63
4.6.4. Dụ dỗ, xâm hại, tống tiền tình dục trực tuyến (mức 3 – ĐỎ) 63
4.6.5. Nội dung giả mạo do AI tạo ra (deepfake) 63
4.6.6. Khủng hoảng tâm lý, ý định tự gây hại (mức 3 – ĐỎ) 64
4.6.7. Sử dụng thiết bị số quá mức 64
4.7. Ghi chép và bảo mật hồ sơ vụ việc 64
4.8. Đầu mối hỗ trợ 65
4.9. Giáo viên tự chăm sóc bản thân 65
CHUYÊN ĐỀ 5. PHỐI HỢP VỚI CHA MẸ HỌC SINH VÀ CÁC LỰC LƯỢNG TRONG HỖ TRỢ HỌC SINH TƯƠNG TÁC AN TOÀN 68
TRÊN KHÔNG GIAN MẠNG 68
5.1. Vai trò của các lực lượng 68
5.2. Nội dung và nguyên tắc phối hợp 69
5.2.1. Nội dung phối hợp 69
5.2.2. Nguyên tắc phối hợp 69
5.3. Phối hợp với cha mẹ học sinh 70
5.3.1. Phối hợp trong giáo dục phòng ngừa 70
5.3.2. Phối hợp khi xảy ra sự cố 71
5.4. Phối hợp với các lực lượng xã hội 71
5.5. Xây dựng môi trường mạng an toàn trong nhà trường 72
CHUYÊN ĐỀ 6. VÍ DỤ MINH HỌA VÀ THỰC HÀNH THIẾT KẾ 75
HOẠT ĐỘNG GIÁO DỤC 75
6.1. Các kế hoạch hoạt động mẫu 76
6.1.1. Kế hoạch mẫu cấp Tiểu học: SỬ DỤNG MẠNG XÃ HỘI AN TOÀN 76
6.1.2. Kế hoạch mẫu cấp THCS: PHÒNG TRÁNH LỪA ĐẢO VÀ BẢO VỆ TÀI KHOẢN 78
6.1.3. Kế hoạch mẫu cấp THCS: PHÒNG TRÁNH NGUY CƠ XÂM HẠI TÌNH DỤC TRÊN KHÔNG GIAN MẠNG 80
6.1.4. Kế hoạch mẫu cấp THPT: TIN GIẢ, DEEPFAKE VÀ NỘI DUNG DO AI TẠO RA ... 82
6.1.5. Kế hoạch mẫu cấp THPT: DẤU CHÂN SỐ VÀ HỒ SƠ TRỰC TUYẾN TRONG ĐỊNH HƯỚNG NGHỀ NGHIỆP 83

6.1.6. Kế hoạch mẫu cấp THPT: CÂN BẰNG ĐỜI SỐNG SỐ VÀ SỨC KHỎE TINH THẦN 85
6.2. Gợi ý lồng ghép theo môn học và khối lớp ... 86
6.3. Nghiên cứu trường hợp: giáo viên xử lý sự cố và phối hợp với cha mẹ học sinh ... 87
Trường hợp 1. Bắt nạt trực tuyến trong nhóm lớp (THCS) ... 87
Trường hợp 2. Học sinh bị lừa chuyển tiền (THPT) ... 88
Trường hợp 3. Cha mẹ học sinh phản ánh con bị người lạ nhắn tin (Tiểu học) ... 88
TÀI LIỆU THAM KHẢO ... 91
A. Văn bản quy phạm pháp luật, văn bản chỉ đạo ... 91
B. Tài liệu tiếng Việt ... 91
C. Tài liệu tiếng Anh ... 92
PHỤ LỤC ... 95
Phụ lục 1. Phiếu khảo sát trước và sau tập huấn ... 95
Phụ lục 2. Phiếu ghi nhận sự việc ... 98
Phụ lục 3. Quy trình xử lý sự cố trực tuyến của học sinh ... 100
Phụ lục 4. Danh bạ đầu mối hỗ trợ ... 101
Phụ lục 5. Mẫu thỏa thuận sử dụng thiết bị số trong gia đình ... 102
Phụ lục 6. Phiếu học tập cho học sinh ... 103
Phiếu 6.1. "Đèn giao thông an toàn" (Tiểu học) ... 103
Phiếu 6.2. "Thám tử mạng" (THCS) ... 103
Phiếu 6.3. Phiếu kiểm chứng thông tin (THPT) ... 104
Phụ lục 7. Gợi ý đáp án câu hỏi tự đánh giá ... 105
Chuyên đề 1 ... 105
Chuyên đề 2 ... 105
Chuyên đề 3 ... 105
Chuyên đề 4 ... 106
Chuyên đề 5 ... 106
Chuyên đề 6 ... 106
Phụ lục 8. Mindmaps tóm tắt cho 6 chuyên đề ... 107
Phụ lục 9. Các kênh hỗ trợ khi gặp sự cố ... 113
GIẢI THÍCH MỘT SỐ THUẬT NGỮ ... 114

DANH MỤC TỪ VIẾT TẮT

Từ viết tắt	Nghĩa đầy đủ
AI	Trí tuệ nhân tạo (Artificial Intelligence)
BGH	Ban giám hiệu
CBQL	Cán bộ quản lý
CMHS	Cha mẹ học sinh
CSAM	Tài liệu xâm hại tình dục trẻ em (Child Sexual Abuse Material)
GDPT	Giáo dục phổ thông
GV	Giáo viên
GVCN	Giáo viên chủ nhiệm
HĐTN	Hoạt động trải nghiệm
HĐTN, HN	Hoạt động trải nghiệm, hướng nghiệp
HS	Học sinh
OCSEA	Bóc lột và xâm hại tình dục trẻ em trực tuyến (Online Child Sexual Exploitation and Abuse)
OECD	Tổ chức Hợp tác và Phát triển Kinh tế
OTP	Mật khẩu dùng một lần (One-Time Password)
THCS	Trung học cơ sở
THPT	Trung học phổ thông
TPT Đội	Tổng phụ trách Đội
UNICEF	Quỹ Nhi đồng Liên hợp quốc
WHO	Tổ chức Y tế Thế giới

HƯỚNG DẪN SỬ DỤNG TÀI LIỆU

1. Đối tượng sử dụng

Tài liệu dành cho giáo viên các cấp tiểu học, trung học cơ sở và trung học phổ thông, trong đó ưu tiên giáo viên chủ nhiệm lớp, giáo viên phụ trách hoạt động trải nghiệm, hướng nghiệp, giáo viên Tin học, Giáo dục công dân, Giáo dục kinh tế và pháp luật, người làm công tác tư vấn học đường và công tác xã hội trong trường học, Tổng phụ trách Đội, Bí thư Đoàn trường.

Cán bộ quản lý cơ sở giáo dục và báo cáo viên cấp tỉnh có thể sử dụng tài liệu để tổ chức tập huấn, bồi dưỡng tại cơ sở.

2. Cấu trúc tài liệu

Tài liệu gồm phần mở đầu, sáu chuyên đề và phần phụ lục:

– Chuyên đề 1. Học sinh trong môi trường số và khung bảo vệ học sinh trên không gian mạng ở Việt Nam.

– Chuyên đề 2. Nhận diện các nguy cơ phổ biến đối với học sinh trên không gian mạng.

– Chuyên đề 3. Giáo dục kỹ năng tương tác an toàn trên không gian mạng cho học sinh.

– Chuyên đề 4. Phát hiện, hỗ trợ và xử lý ban đầu khi học sinh gặp sự cố trên không gian mạng.

– Chuyên đề 5. Phối hợp với cha mẹ học sinh và các lực lượng trong hỗ trợ học sinh tương tác an toàn trên không gian mạng.

– Chuyên đề 6. Ví dụ minh họa và thực hành thiết kế hoạt động giáo dục.

3. Quy ước trình bày

– Tài liệu dùng thống nhất cách xưng hô "thầy cô" khi hướng tới học viên tập huấn.

– Tài liệu dùng thống nhất thuật ngữ "học sinh"; thuật ngữ "trẻ em" chỉ được sử dụng khi dẫn quy định của pháp luật hoặc trích dẫn kết quả nghiên cứu sử dụng thuật ngữ này.

– Các ô "Hoạt động tập huấn" được đóng khung; phần "Gợi ý" nêu định hướng trả lời, không phải đáp án duy nhất.

– Các văn bản quy phạm pháp luật được dẫn theo hiệu lực tại thời điểm biên soạn (tháng 10/2026). Người sử dụng cần cập nhật khi văn bản được sửa đổi, bổ sung hoặc thay thế.

4. Cách sử dụng tài liệu

– **Đối với báo cáo viên:** sử dụng kế hoạch tập huấn ở mục "Mục tiêu và kế hoạch tập huấn"; tổ chức các hoạt động tập huấn theo hướng trải nghiệm, thảo luận, xử lý tình huống; sử dụng phiếu khảo sát trước và sau tập huấn (Phụ lục 1) để đánh giá hiệu quả.

– **Đối với giáo viên tự học:** đọc theo trình tự các chuyên đề; thực hiện các hoạt động tập huấn và trả lời câu hỏi tự đánh giá; vận dụng các kế hoạch hoạt động mẫu ở Chuyên đề 6 vào lớp học của mình, có điều chỉnh phù hợp với đặc điểm học sinh.

– **Đối với cán bộ quản lý:** sử dụng Chuyên đề 1, 4 và 5 để xây dựng quy trình tiếp nhận, xử lý sự cố và cơ chế phối hợp của nhà trường.

5. Lưu ý về đạo đức khi sử dụng tài liệu

Một số nội dung của tài liệu đề cập đến xâm hại, bạo lực và tự gây hại. Báo cáo viên cần thông báo trước cho học viên, tạo không khí an toàn khi thảo luận, không yêu cầu học viên chia sẻ trải nghiệm cá nhân và không sử dụng hình ảnh, thông tin thật của học sinh trong các ví dụ

MỤC TIÊU VÀ KẾ HOẠCH TẬP HUẤN

1. Mục tiêu tập huấn

1.1. Về kiến thức

Trình bày được đặc điểm phát triển tâm sinh lý của học sinh theo cấp học và ảnh hưởng của các đặc điểm đó đến hành vi trực tuyến.

Trình bày được những quy định cơ bản của pháp luật Việt Nam về bảo vệ trẻ em trên môi trường mạng và trách nhiệm của nhà trường, giáo viên.

Phân tích được các nguy cơ phổ biến đối với học sinh trên không gian mạng, dấu hiệu nhận biết và cách phòng ngừa.

1.2. Về năng lực

Thiết kế và tổ chức được hoạt động giáo dục kỹ năng tương tác an toàn trên không gian mạng thông qua môn học, hoạt động trải nghiệm, hướng nghiệp và sinh hoạt lớp.

Phối hợp được với cha mẹ học sinh, đồng nghiệp, người làm công tác tư vấn học đường và các cơ quan chức năng.

Nhận diện được dấu hiệu học sinh đang gặp nguy cơ hoặc sự cố trực tuyến.

Tiếp nhận được chia sẻ của học sinh một cách an toàn, hỗ trợ tâm lý ban đầu và xử lý sự cố theo đúng quy trình.

1.3. Về phẩm chất

Tôn trọng quyền riêng tư, quyền được bảo vệ và quyền được tham gia của học sinh trên môi trường mạng.

Không đổ lỗi, không kỳ thị học sinh là nạn nhân; ứng xử đồng cảm, kiên nhẫn và bảo mật thông tin.

Có ý thức tự cập nhật kiến thức về môi trường mạng và làm gương cho học sinh trong hành vi trực tuyến.

2. Kế hoạch và phân bổ thời lượng

Chương trình tập huấn được thiết kế cho 02 ngày (04 buổi), tương đương 14 giờ. Báo cáo viên có thể điều chỉnh thời lượng theo điều kiện thực tế, nhưng cần bảo đảm thời lượng cho 06 chuyên đề.

Bảng 1. Kế hoạch và phân bổ thời lượng tập huấn

Buổi	**Nội dung**	**Thời lượng**	**Hình thức chủ yếu**
Buổi 1 (sáng ngày 1)	Chuyên đề 1	90 phút	Trình bày, thảo luận nhóm, phân tích tình huống pháp lý
	Chuyên đề 2 (phần 1: mục 2.1 – 2.5)	90 phút	Phân tích tình huống, phân loại nguy cơ
Buổi 2 (chiều ngày 1)	Chuyên đề 2 (phần 2: mục 2.6 – 2.10)	90 phút	Thảo luận nhóm, phân tích trường hợp
	Chuyên đề 3	150 phút	Trải nghiệm, thiết kế hoạt động
Buổi 3 (sáng ngày 2)	Chuyên đề 4	180 phút	Đóng vai, xử lý tình huống, thực hành quy trình
Buổi 4 (chiều ngày 2)	Chuyên đề 5	90 phút	Đóng vai, thảo luận
	Chuyên đề 6 (thực hành thiết kế, trình bày sản phẩm)	120 phút	Làm việc nhóm theo cấp học
	Tổng kết; khảo sát cuối khóa; đánh giá tập huấn	30 phút	Cá nhân

CHUYÊN ĐỀ 1. HỌC SINH TRONG MÔI TRƯỜNG SỐ VÀ KHUNG BẢO VỆ HỌC SINH TRÊN KHÔNG GIAN MẠNG Ở VIỆT NAM

(Thời lượng: 90 phút)

MỤC TIÊU

Sau khi học xong chuyên đề này, thầy cô có thể:

– Giải thích được các khái niệm cơ bản: không gian mạng, an toàn trên không gian mạng, kỹ năng an toàn trên không gian mạng, tương tác an toàn.

– Phân tích được ảnh hưởng của đặc điểm phát triển tâm sinh lý ở từng cấp học đến hành vi trực tuyến của học sinh và rút ra hàm ý sư phạm.

– Mô tả được một số biểu hiện của thực trạng sử dụng Internet và trải nghiệm trực tuyến của học sinh Việt Nam qua các số liệu nghiên cứu.

– Phân biệt được trách nhiệm của nhà trường, giáo viên theo quy định của pháp luật Việt Nam về bảo vệ trẻ em trên môi trường mạng.

KHỞI ĐỘNG

Hoạt động khởi động: "Một ngày trực tuyến của học sinh lớp em" (10 phút)

Mỗi thầy cô viết ra 5 hoạt động trực tuyến mà học sinh lớp mình thường thực hiện trong một ngày (từ khi thức dậy đến khi đi ngủ), sau đó đánh dấu những hoạt động mà thầy cô cho rằng có thể tiềm ẩn nguy cơ. Chia sẻ trong nhóm 4 – 5 người và trả lời câu hỏi: Chúng ta biết bao nhiêu về đời sống trực tuyến thực tế của học sinh?

Gợi ý: Hoạt động giúp học viên nhận ra khoảng cách giữa hình dung của người lớn và thực tế đời sống số của học sinh (học trực tuyến, nhắn tin nhóm lớp, xem video ngắn, chơi game có trò chuyện, theo dõi người nổi tiếng, mua bán vật phẩm game, sử dụng công cụ AI để làm bài…). Báo cáo viên dẫn dắt: muốn hỗ trợ học sinh, trước hết giáo viên cần hiểu học sinh đang sống và tương tác như thế nào trên mạng.

NỘI DUNG

1.1. Một số khái niệm cơ bản

1.1.1. Không gian mạng

Luật An ninh mạng năm 2018 và Luật An ninh mạng năm 2025 (Luật số 116/2025/QH15, có hiệu lực từ ngày 01/7/2026) đều tiếp cận không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian. Từ góc độ giáo dục, không gian mạng không chỉ là một hệ thống kỹ thuật mà là một môi trường xã hội đặc thù, nơi học sinh học tập, giao tiếp, giải trí và hình thành bản sắc cá nhân.

Không gian mạng có bốn đặc điểm có ý nghĩa giáo dục quan trọng: (1) tính kết nối rộng, không giới hạn về không gian, thời gian; (2) tốc độ lan truyền thông tin nhanh và khả năng lưu trữ lâu dài; (3) tính ẩn danh tương đối và khả năng giả mạo danh tính; (4) hiệu ứng giảm ức chế hành vi, khiến con người dễ chia sẻ, bộc lộ hoặc hành xử khác so với khi giao tiếp trực tiếp (Suler, 2004). Những đặc điểm này vừa tạo cơ hội học tập, kết nối, vừa làm gia tăng nguy cơ đối với người dùng nhỏ tuổi.

1.1.2. An toàn trên không gian mạng và kỹ năng an toàn trên không gian mạng

An toàn trên không gian mạng, trong lĩnh vực giáo dục, được hiểu là trạng thái người học được bảo vệ khỏi các mối đe dọa, rủi ro và hành vi gây tổn hại về thể chất, tinh thần, tài sản, danh dự và quyền riêng tư khi tham gia môi trường số; đồng thời người học được bảo đảm các quyền tiếp cận thông tin, vui chơi, học tập và tham gia.

Kỹ năng an toàn trên không gian mạng là khả năng của cá nhân trong việc nhận diện, phòng tránh và ứng phó với các nguy cơ trong môi trường mạng, đồng thời sử dụng Internet một cách an toàn, có trách nhiệm và hiệu quả. Kỹ năng này có cấu trúc gồm ba thành tố gắn bó với nhau:

– **Nhận thức:** hiểu biết về các nguy cơ, hậu quả và nguyên tắc an toàn khi tham gia không gian mạng.

– **Thái độ:** ý thức thận trọng, trách nhiệm, tôn trọng bản thân và người khác, sẵn sàng tìm kiếm sự hỗ trợ.

– **Hành vi:** khả năng thực hiện các hành động cụ thể để bảo vệ bản thân và người khác (thiết lập quyền riêng tư, từ chối, chặn, lưu bằng chứng, báo cáo, kể với người lớn tin cậy…).

Trong Khung năng lực số cho người học (Thông tư số 02/2025/TT-BGDĐT), "An toàn" là một trong sáu miền năng lực, bên cạnh khai thác dữ liệu và thông tin; giao tiếp và hợp tác trong môi trường số; sáng tạo nội dung số; giải quyết vấn đề; ứng dụng trí tuệ nhân tạo. Điều này cho thấy kỹ năng an toàn trên không gian mạng là một bộ phận cấu thành năng lực số mà nhà trường có trách nhiệm hình thành cho học sinh.

1.1.3. Tương tác an toàn trên không gian mạng

Khái niệm "tương tác an toàn" nhấn mạnh rằng mục tiêu giáo dục không phải là hạn chế hay cấm đoán học sinh tham gia môi trường mạng, mà là giúp học sinh tham gia một cách an toàn, lành mạnh, sáng tạo và có trách nhiệm. Cách tiếp cận này phù hợp với "mục tiêu kép" của Chương trình "Bảo vệ và hỗ trợ trẻ em phát triển trên môi trường mạng giai đoạn 2026 – 2030": vừa bảo vệ trẻ em, vừa thúc đẩy trẻ em phát triển lành mạnh, nâng cao năng lực số. Nghiên cứu quốc tế cũng cho thấy rủi ro trực tuyến không đồng nghĩa với tổn hại; mức độ tổn hại phụ thuộc vào khả năng ứng phó của học sinh và sự hỗ trợ của người lớn (Livingstone & Stoilova, 2021). Trong bối cảnh hiện nay, học sinh đa số là thế hệ Gen Z/Alpha - các em có sự cập nhật, chủ động trong sử dụng công nghệ thông tin nên giải pháp cấm đoán kỹ thuật thuần túy khó đạt hiệu quả. Vì vậy, vai trò của giáo viên không chỉ là "ngăn chặn" mà là "trang bị" và "đồng hành".

1.1.4. Giáo dục kỹ năng an toàn trên không gian mạng

Giáo dục kỹ năng an toàn trên không gian mạng cho học sinh là quá trình sư phạm có mục đích, có kế hoạch, nhằm hình thành và phát triển ở học sinh hệ thống tri thức, kỹ năng, thái độ và hành vi cần thiết để nhận diện, phòng ngừa và ứng phó hiệu quả với các nguy cơ trên không gian mạng; đồng thời hình thành thói quen sử dụng không gian mạng an toàn, lành mạnh, có văn hóa. Đây là một bộ phận của giáo dục kỹ năng sống và giáo dục năng lực số, được thực hiện thông qua các môn học, hoạt động trải nghiệm, hướng nghiệp và các hoạt động giáo dục khác trong và ngoài nhà trường.

1.2. Đặc điểm phát triển tâm sinh lý của học sinh và hành vi trực tuyến

1.2.1. Vì sao giáo viên cần hiểu đặc điểm phát triển của học sinh?

Hành vi trực tuyến của học sinh chịu ảnh hưởng trực tiếp của mức độ phát triển nhận thức, cảm xúc – xã hội và thể chất. Hiểu được vì sao học sinh ở một độ tuổi nhất định dễ tin người lạ, dễ bị cuốn vào trào lưu hay khó dự đoán hậu quả hành vi giúp giáo viên lựa chọn nội dung, phương pháp phù hợp và ứng xử đúng mực khi học sinh mắc sai lầm.

Có ba hệ thống lý thuyết thường được sử dụng để lý giải vấn đề này:

– **Lý thuyết phát triển nhận thức của J. Piaget:** học sinh tiểu học chủ yếu ở giai đoạn thao tác cụ thể, tư duy gắn với sự vật cụ thể; từ khoảng 11 – 12 tuổi, học sinh bước vào giai đoạn thao tác hình thức, bắt đầu có khả năng tư duy trừu tượng, giả định (Inhelder & Piaget, 1958).

– **Lý thuyết phát triển tâm lý – xã hội của E. Erikson:** học sinh tiểu học ở giai đoạn "siêng năng – tự ti", nhu cầu được ghi nhận năng lực rất lớn; học sinh THCS, THPT ở giai đoạn "định hình cái tôi và bối rối về vai trò, gắn bó và cô lập", nhu cầu khẳng định bản thân, được thuộc về nhóm bạn và khám phá các mối quan hệ thân mật nổi trội (Erikson, 1968).

– **Nghiên cứu khoa học thần kinh về não bộ tuổi vị thành niên:** vỏ não trước trán (phụ trách kiểm soát xung động, lập kế hoạch, đánh giá rủi ro) phát triển muộn và hoàn thiện vào khoảng đầu đến giữa tuổi 20, trong khi hệ thống cảm xúc và tưởng thưởng hoạt động mạnh từ tuổi dậy thì. Sự chênh lệch này lý giải xu hướng hành động bốc đồng, tìm kiếm cảm giác mạnh và chịu ảnh hưởng mạnh của bạn bè ở lứa tuổi thiếu niên (Steinberg, 2008; Konrad và cộng sự, 2013).

Ngoài ra, Elkind (1967) chỉ ra hiện tượng "khán giả tưởng tượng" ở tuổi thiếu niên: các em tin rằng mọi người xung quanh đang chú ý đến ngoại hình và hành vi của mình. Hiện tượng này đặc biệt gắn với nhu cầu đăng tải, tìm kiếm lượt thích, bình luận trên mạng xã hội và sự nhạy cảm cao trước những đánh giá tiêu cực trực tuyến.

1.2.2. Đặc điểm theo cấp học và hàm ý đối với giáo viên

Cấp học	**Đặc điểm phát triển nổi bật**	**Biểu hiện thường gặp trên không gian mạng**	**Hàm ý đối với giáo viên**
Tiểu học (6 – 11 tuổi)	Tư duy cụ thể, ranh giới giữa tưởng tượng và thực tế còn mơ hồ (nhất là ở lớp 1 – 3); khả năng kiểm soát xung động hạn chế; tin tưởng người lớn; nhu cầu được khen ngợi, ghi nhận.	Xem video, chơi game, dùng thiết bị của cha mẹ; dễ tin quảng cáo, thông báo trúng thưởng; khó nhận ra tài khoản giả mạo; dễ vô tình tiếp xúc nội dung không phù hợp; bắt đầu tham gia nhóm trò chuyện.	Dạy bằng ví dụ cụ thể, trực quan, quy tắc ngắn gọn dễ nhớ; luyện tập hành vi "dừng lại – hỏi người lớn"; phối hợp chặt chẽ với cha mẹ vì phần lớn thiết bị do cha mẹ quản lý.
THCS (11 – 15 tuổi)	Bắt đầu tư duy trừu tượng nhưng chưa vững; dậy thì, cảm xúc thất thường; nhu cầu độc lập, được bạn bè chấp nhận rất cao; tò mò về giới tính; xu hướng thử giới hạn.	Có tài khoản mạng xã hội riêng (kể cả khi chưa đủ tuổi theo quy định của nền tảng); chơi game trực tuyến có giao tiếp; tham gia trào lưu, "thử thách"; kết bạn với người lạ; nguy cơ bị dụ dỗ, bắt nạt, lừa mua bán vật phẩm game.	Kết hợp quy tắc với giải thích lý do; tổ chức đóng vai, xử lý tình huống gần gũi; tôn trọng nhu cầu riêng tư nhưng duy trì kênh trò chuyện tin cậy; chú ý dấu hiệu thay đổi cảm xúc, hành vi.

THPT (15 – 18 tuổi)	Tư duy trừu tượng, phản biện phát triển; định hình bản sắc, giá trị, định hướng nghề nghiệp; nhu cầu các mối quan hệ thân mật; vẫn dễ bị chi phối bởi cảm xúc và áp lực nhóm.	Sử dụng mạng xã hội để thể hiện bản thân, xây dựng hình ảnh; giao dịch, mua bán, kiếm tiền trực tuyến; tham gia các mối quan hệ tình cảm qua mạng; tiếp xúc tin giả, nội dung cực đoan, cờ bạc trá hình; sử dụng công cụ AI.	Phát triển tư duy phản biện, kiểm chứng thông tin; thảo luận về đạo đức số, pháp luật, dấu chân số gắn với hướng nghiệp; trao quyền cho học sinh tham gia xây dựng quy tắc và hỗ trợ đồng đẳng.

Bảng 1.1. Đặc điểm phát triển của học sinh theo cấp học và hàm ý đối với giáo viên

Bảng trên chỉ mô tả xu hướng chung. Giáo viên cần lưu ý sự khác biệt cá nhân rất lớn trong cùng một độ tuổi, đặc biệt ở học sinh có hoàn cảnh khó khăn, học sinh khuyết tật, học sinh có vấn đề về sức khỏe tâm thần hoặc thiếu sự quan tâm của gia đình – những nhóm có nguy cơ bị tổn hại cao hơn trên môi trường mạng (ECPAT, INTERPOL & UNICEF, 2022).

1.2.3. Sự khác biệt giữa tương tác trực tuyến và trực tiếp

Môi trường trực tuyến có những đặc điểm khiến hành vi của học sinh khác với khi giao tiếp trực tiếp: khả năng tiếp cận dễ dàng, chi phí thấp; tính ẩn danh tương đối; hiệu ứng giảm ức chế hành vi; nội dung có thể bị lưu giữ, sao chép, lan truyền ngoài tầm kiểm soát; sự giám sát của người lớn giảm đi đáng kể. Ranh giới giữa đời sống trực tuyến và ngoại tuyến của học sinh ngày càng mờ nhạt: xung đột ngoài lớp học có thể tiếp tục trên mạng và ngược lại; phần lớn tương tác trực tuyến của học sinh diễn ra với những người các em đã quen biết (Saleh và cộng sự, 2014).

1.3. Thực trạng học sinh Việt Nam trên không gian mạng

1.3.1. Mức độ tiếp cận và các hoạt động trực tuyến

Theo nghiên cứu UNICEF điều tra năm 2022 tại Việt Nam (ECPAT, INTERPOL & UNICEF, 2022), 89% học sinh từ 12 đến 17 tuổi sử dụng Internet, không có sự khác biệt đáng kể theo giới; tỷ lệ ở khu vực nông thôn là 88% và đô thị là 93%. Độ tuổi có điện thoại di động riêng ngày càng giảm. Các hoạt động trực tuyến phổ biến nhất là giải trí và giao tiếp. Số liệu trên cho thấy hai điểm

đáng chú ý. Thứ nhất, mức độ tham gia mạng xã hội và nhắn tin của trẻ em tăng rất nhanh từ 12 – 13 tuổi lên 14 – 15 tuổi, tức là giai đoạn THCS là thời điểm then chốt để giáo dục. Thứ hai, gần một nửa học sinh tìm kiếm hỗ trợ tâm lý trên mạng; điều này vừa phản ánh nhu cầu chưa được đáp ứng trong đời sống thực, vừa tiềm ẩn nguy cơ học sinh tiếp cận nguồn thông tin không tin cậy và nguy cơ bị người có ý đồ xấu lợi dụng lừa đảo.

1.3.2. Nhận thức và trải nghiệm rủi ro của học sinh

Cũng theo Disrupting Harm và UNICEF Việt Nam (2022):

– Chỉ 33% trẻ em cho rằng tiếp xúc với người lạ trên mạng là rất nguy hiểm; 56% đã từng tìm kiếm bạn bè, mối quan hệ mới trên mạng và 33% đã thêm vào danh sách liên lạc người chưa từng gặp ngoài đời.

– 22% đã từng chia sẻ thông tin cá nhân với người chưa từng gặp trực tiếp; 5% đã từng gặp trực tiếp người chỉ quen qua mạng.

– 8% từng nhận những lời bình luận mang tính tình dục khiến các em khó chịu, phần lớn từ người quen; 43% học sinh nhận được lời bình luận nhưng không chia sẻ với ai.

– 5% từng nhận hình ảnh tình dục không mong muốn; gần một nửa không nói với ai, những em có chia sẻ chủ yếu nói với bạn bè, rất ít báo cáo chính thức.

Về bắt nạt trực tuyến, khảo sát U-Report của UNICEF (2019) cho thấy 21% thanh thiếu niên Việt Nam tham gia khảo sát cho biết từng là nạn nhân, và 75% không biết đến đường dây nóng hay dịch vụ hỗ trợ. Tổng quan 53 nghiên cứu cho thấy tỷ lệ bắt nạt trực tuyến ở học sinh THCS dao động khoảng 10% – 40% tùy mẫu và thang đo (Trương Thanh Long & Tô Thị Minh Tâm, 2024). Về sử dụng Internet quá mức, một nghiên cứu trên 405 học sinh THCS tại thành phố Huế ghi nhận 6,4% học sinh có khuynh hướng nghiện Internet (Hồ Văn Dũng, 2020).

Điểm chung của các số liệu trên là: học sinh gặp rủi ro không hiếm, nhưng phần lớn không tìm kiếm sự giúp đỡ từ người lớn. Đây là cơ sở thực tiễn để tài liệu đặt trọng tâm vào năng lực phát hiện, tiếp nhận và hỗ trợ của giáo viên.

1.3.3. Thực trạng giáo dục kỹ năng an toàn trên không gian mạng trong nhà trường

Các nghiên cứu khảo sát gần đây cho thấy một số đặc điểm chung:

– Giáo viên, cha mẹ học sinh và học sinh đều nhận thức được tầm quan trọng của giáo dục kỹ năng an toàn trên không gian mạng; tuy nhiên, một bộ phận chưa thấy rõ sự cần thiết của việc giáo dục thông qua hoạt động trải nghiệm.

– Học sinh đã có các kỹ năng cơ bản như bảo mật thông tin cá nhân và nhận diện nguy cơ; nhưng các kỹ năng phức hợp như đánh giá thông tin, kiểm soát hành vi sử dụng và ứng phó với tình huống trực tuyến còn hạn chế, chưa đồng đều.

– Nội dung và hình thức tổ chức giáo dục chưa thực sự hấp dẫn, chưa bám sát tình huống thực tế; việc đánh giá kết quả còn mang tính hình thức, chủ yếu kiểm tra ghi nhớ kiến thức.

– Phối hợp chủ yếu diễn ra giữa nhà trường và gia đình, sự tham gia của các lực lượng xã hội (chuyên gia, cơ quan chức năng) còn hạn chế; phối hợp chưa thường xuyên và thiếu gắn kết.

1.4. Khung pháp lý và trách nhiệm của nhà trường, giáo viên

1.4.1. Các văn bản pháp luật, chính sách chủ yếu

Văn bản	**Nội dung liên quan trực tiếp đến nhà trường, giáo viên**
Luật Trẻ em năm 2016 (Luật số 102/2016/QH13), Điều 54	Cơ quan, tổ chức, cơ sở giáo dục, gia đình, cá nhân có trách nhiệm giáo dục kiến thức, hướng dẫn kỹ năng để trẻ em biết tự bảo vệ mình khi tham gia môi trường mạng; bảo đảm an toàn và bí mật đời sống riêng tư cho trẻ em.
Nghị định số 56/2017/NĐ-CP quy định chi tiết Luật Trẻ em, Chương IV (Điều 33 – 37)	Các biện pháp bảo vệ thông tin bí mật đời sống riêng tư của trẻ em trên môi trường mạng; trách nhiệm của các chủ thể trong việc bảo vệ trẻ em trên môi trường mạng.
Luật An ninh mạng năm 2025 (Luật số 116/2025/QH15), hiệu lực từ 01/7/2026, thay thế Luật An ninh mạng 2018 và Luật An toàn thông tin mạng 2015	Trẻ em có quyền được bảo vệ, tiếp cận thông tin, tham gia hoạt động xã hội, vui chơi, giải trí, giữ bí mật cá nhân, đời sống riêng tư trên không gian mạng; doanh nghiệp, chủ quản hệ thống thông tin có trách nhiệm kiểm soát, ngăn chặn nội dung gây hại cho trẻ em; Nhà nước ưu tiên giáo dục an ninh mạng cho trẻ em; cha mẹ, giáo viên, người chăm sóc có trách nhiệm giám sát, giáo dục.

Văn bản	Nội dung liên quan trực tiếp đến nhà trường, giáo viên
Luật Bảo vệ dữ liệu cá nhân năm 2025 (Luật số 91/2025/QH15), hiệu lực từ 01/01/2026, Điều 24	Xử lý dữ liệu cá nhân của trẻ em phải bảo vệ quyền, lợi ích tốt nhất của trẻ em; việc công khai, tiết lộ thông tin về đời sống riêng tư, bí mật cá nhân của trẻ em từ đủ 07 tuổi phải có sự đồng ý của trẻ em và người đại diện theo pháp luật.
Nghị định số 147/2024/NĐ-CP về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng, Điều 39	Tài khoản trò chơi điện tử của người dưới 16 tuổi do cha, mẹ hoặc người giám hộ đăng ký và giám sát; người chơi dưới 18 tuổi bị giới hạn không quá 60 phút đối với từng trò chơi và không quá 180 phút một ngày.
Bộ luật Hình sự năm 2015 (sửa đổi, bổ sung)	Xử lý hình sự các hành vi như: dâm ô đối với người dưới 16 tuổi (Điều 146); sử dụng người dưới 16 tuổi vào mục đích khiêu dâm (Điều 147); lừa đảo chiếm đoạt tài sản (Điều 174); đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông (Điều 288); đánh bạc, tổ chức đánh bạc (Điều 321, 322).
Nghị định số 80/2017/NĐ-CP quy định về môi trường giáo dục an toàn, lành mạnh, thân thiện, phòng, chống bạo lực học đường	Trách nhiệm của nhà trường trong phòng ngừa, phát hiện, can thiệp, hỗ trợ học sinh bị bạo lực học đường, bao gồm bạo lực xảy ra qua môi trường mạng.
Thông tư số 06/2019/TT-BGDĐT quy định Quy tắc ứng xử trong cơ sở giáo dục	Chuẩn mực ứng xử của giáo viên, học sinh, kể cả ứng xử trên môi trường mạng.

Văn bản	Nội dung liên quan trực tiếp đến nhà trường, giáo viên
Thông tư số 18/2025/TT-BGDĐT hướng dẫn về công tác tư vấn học đường và công tác xã hội trong trường học (thay thế Thông tư 31/2017 và Thông tư 33/2018)	Nguyên tắc lấy người học làm trung tâm, bảo đảm an toàn và bảo mật thông tin, tự nguyện; nhiệm vụ phòng ngừa, nhận diện, hỗ trợ người học vượt qua khó khăn về học tập, tâm lý, quan hệ xã hội.
Thông tư số 02/2025/TT-BGDĐT ban hành Khung năng lực số cho người học	"An toàn" là một trong sáu miền năng lực số của người học.
Quyết định số 468/QĐ-TTg ngày 23/3/2026 phê duyệt Chương trình "Bảo vệ và hỗ trợ trẻ em phát triển trên môi trường mạng giai đoạn 2026 – 2030"	Mục tiêu kép: bảo vệ trẻ em và thúc đẩy trẻ em phát triển lành mạnh, nâng cao năng lực số; chuyển trọng tâm sang phòng ngừa chủ động; 100% cơ sở giáo dục phổ thông triển khai giải pháp bảo đảm an ninh mạng.

Bảng 1.2. Một số văn bản pháp luật, chính sách về bảo vệ học sinh trên không gian mạng

1.4.2. Trách nhiệm của nhà trường

Trên cơ sở các văn bản nêu trên, nhà trường có trách nhiệm:

– Đưa nội dung giáo dục kỹ năng an toàn trên không gian mạng vào kế hoạch giáo dục của nhà trường; tổ chức thực hiện thông qua các môn học, HĐTN, HN, sinh hoạt lớp và hoạt động ngoài giờ.

– Xây dựng và công khai quy định về sử dụng thiết bị số, Internet, nhóm trực tuyến của lớp, trường; bảo đảm an toàn hệ thống mạng của nhà trường.

– Thiết lập quy trình tiếp nhận, xử lý thông tin về sự cố trực tuyến của học sinh; phân công đầu mối; bảo đảm bảo mật thông tin.

– Tổ chức công tác tư vấn học đường, công tác xã hội trong trường học theo Thông tư số 18/2025/TT-BGDĐT.

– Phối hợp với gia đình, chính quyền địa phương, cơ quan công an, y tế và các tổ chức liên quan trong phòng ngừa, can thiệp, hỗ trợ học sinh.

– Bồi dưỡng năng lực cho giáo viên, nhân viên; bảo vệ dữ liệu cá nhân của học sinh trong mọi hoạt động của nhà trường.

1.4.3. Trách nhiệm của giáo viên (được làm gì, phải làm gì, không được làm gì)

Giáo viên CẦN làm	**Giáo viên KHÔNG được làm**
Giáo dục học sinh kỹ năng tương tác an toàn theo kế hoạch giáo dục của nhà trường.	Tự ý điều tra, thẩm vấn học sinh, đối chất học sinh với người bị nghi ngờ gây hại.
Quan sát, phát hiện dấu hiệu bất thường; lắng nghe, tiếp nhận chia sẻ của học sinh một cách tôn trọng.	Hứa với học sinh sẽ giữ bí mật tuyệt đối khi có nguy cơ đe dọa an toàn của học sinh.
Báo cáo kịp thời cho Ban Giám hiệu, người được phân công làm đầu mối theo quy trình của nhà trường.	Công khai danh tính, hình ảnh, thông tin của học sinh liên quan đến vụ việc (kể cả trong nhóm Zalo, Facebook của lớp, của trường). Trực tiếp mở file/nhận file ảnh, video nhạy cảm qua Zalo/Email cá nhân (để tránh vi phạm pháp luật về tàng trữ/vận chuyển văn hóa phẩm nhạy cảm liên quan đến trẻ em).
Ghi chép trung thực, khách quan; bảo mật thông tin; chỉ chia sẻ với người có trách nhiệm.	Yêu cầu học sinh gửi, chuyển tiếp hoặc lưu giữ hình ảnh nhạy cảm làm "bằng chứng"; tự lưu giữ, phát tán những hình ảnh này.
Phối hợp với cha mẹ học sinh, người làm tư vấn học đường, cơ quan chức năng theo phân công.	Đổ lỗi, chê trách, kỷ luật học sinh là nạn nhân; xử lý theo hướng "giải quyết nội bộ" đối với vụ việc có dấu hiệu vi phạm pháp luật.

Giáo viên CẦN làm	Giáo viên KHÔNG được làm
Làm gương trong hành vi trực tuyến; tôn trọng quyền riêng tư của học sinh (xin phép trước khi đăng ảnh học sinh, không công khai điểm số, hoàn cảnh cá nhân trên mạng).	Kết bạn, nhắn tin riêng với học sinh qua kênh cá nhân với nội dung, thời điểm không phù hợp; kiểm tra điện thoại cá nhân của học sinh trái quy định.

Bảng 1.3. Những việc giáo viên cần làm và không được làm

Lưu ý: Việc đăng tải hình ảnh, video hoạt động của học sinh lên trang thông tin của trường, lớp cần thực hiện theo quy định về bảo vệ dữ liệu cá nhân; đối với học sinh từ đủ 07 tuổi, cần có sự đồng ý của học sinh và cha mẹ học sinh khi nội dung liên quan đến đời sống riêng tư, bí mật cá nhân.

HOẠT ĐỘNG TẬP HUẤN

Hoạt động 1.1. Phân tích đặc điểm lứa tuổi (20 phút)

Nhóm thầy cô phụ trách học sinh cùng cấp học thảo luận: Những đặc điểm phát triển nào của học sinh cấp học mình phụ trách khiến các em dễ gặp rủi ro trên mạng? Hãy nêu một ví dụ thực tế và đề xuất một cách tiếp cận giáo dục phù hợp.

Gợi ý: Tiểu học – dễ tin vào thông báo trúng thưởng, nhân vật hoạt hình; cách tiếp cận: quy tắc "Dừng – Hỏi người lớn", trò chơi phân loại an toàn/không an toàn. THCS – nhu cầu được bạn bè chấp nhận khiến các em tham gia trào lưu, "thử thách"; cách tiếp cận: phân tích tình huống, thảo luận áp lực nhóm, rèn kỹ năng từ chối. THPT – nhu cầu xây dựng hình ảnh, kiếm tiền trực tuyến khiến các em dễ chia sẻ thông tin, tham gia "việc nhẹ lương cao"; cách tiếp cận: phân tích trường hợp, kiểm chứng thông tin, thảo luận về dấu chân số và nghề nghiệp tương lai.

Hoạt động 1.2. Đúng hay sai theo quy định? (20 phút)
Thầy cô nhận xét các tình huống sau là phù hợp hay không phù hợp với quy định, giải thích lý do:
a) GVCN đăng ảnh cả lớp kèm họ tên, ngày sinh từng học sinh lên trang cá nhân để chúc mừng sinh nhật tập thể.
b) Học sinh báo với cô giáo bị một tài khoản lạ đe dọa phát tán ảnh. Cô yêu cầu học sinh chuyển toàn bộ ảnh vào điện thoại của cô để làm bằng chứng.
c) Thầy giáo phát hiện một nhóm học sinh lập trang mạng chế giễu bạn cùng lớp; thầy báo cáo Ban Giám hiệu, đồng thời trao đổi riêng với học sinh bị chế giễu để hỗ trợ.
Gợi ý: (a) Không phù hợp: công khai dữ liệu cá nhân của học sinh (họ tên, ngày sinh, hình ảnh) trên trang cá nhân khi chưa có sự đồng ý, trái tinh thần Điều 24 Luật Bảo vệ dữ liệu cá nhân năm 2025. (b) Không phù hợp: giáo viên không được lưu giữ, tiếp nhận hình ảnh nhạy cảm của học sinh; cần hướng dẫn học sinh không xóa, không gửi thêm, ghi lại thông tin tài khoản và báo cáo theo quy trình (xem Chuyên đề 4). (c) Phù hợp: giáo viên báo cáo theo quy trình, ưu tiên hỗ trợ nạn nhân; cần tiếp tục phối hợp để xử lý cả học sinh có hành vi bắt nạt theo hướng giáo dục.

GHI NHỚ

– Kỹ năng an toàn trên không gian mạng gồm ba thành tố nhận thức – thái độ – hành vi; mục tiêu cuối cùng là thay đổi hành vi.

– Mục tiêu giáo dục là giúp học sinh tương tác an toàn, không phải cấm đoán học sinh tham gia môi trường mạng.

– Phần lớn học sinh gặp rủi ro không tìm đến người lớn; vì vậy năng lực phát hiện, tiếp nhận của giáo viên có ý nghĩa đặc biệt quan trọng.

– Giáo viên giáo dục, phát hiện, hỗ trợ ban đầu, báo cáo và phối hợp; giáo viên không điều tra và không xử lý thay cơ quan chức năng.

CÂU HỎI TỰ ĐÁNH GIÁ

1. Kỹ năng an toàn trên không gian mạng gồm những thành tố nào? Vì sao đánh giá kết quả giáo dục cần hướng vào thành tố hành vi?

2. Hãy giải thích vì sao học sinh THCS dễ chịu ảnh hưởng của bạn bè và trào lưu trên mạng dựa trên hiểu biết về phát triển não bộ tuổi vị thành niên.

3. Theo Luật Bảo vệ dữ liệu cá nhân năm 2025, việc công khai thông tin về đời sống riêng tư của học sinh từ đủ 07 tuổi cần điều kiện gì?

4. Nêu ba việc giáo viên không được làm khi tiếp nhận thông tin học sinh gặp sự cố trên mạng.

CHUYÊN ĐỀ 2. NHẬN DIỆN CÁC NGUY CƠ PHỔ BIẾN ĐỐI VỚI HỌC SINH TRÊN KHÔNG GIAN MẠNG

(Thời lượng: 180 phút)

MỤC TIÊU

Sau khi học xong chuyên đề này, thầy cô có thể:

– Mô tả được bản chất, biểu hiện, dấu hiệu cảnh báo và biện pháp phòng ngừa đối với chín nhóm nguy cơ phổ biến: lừa đảo, chiếm đoạt tài khoản; lộ lọt dữ liệu cá nhân; sử dụng quá mức; tin giả, nội dung có hại; "thử thách" nguy hiểm, cờ bạc; nội dung do AI tạo ra; bắt nạt trực tuyến; xâm hại, bóc lột tình dục trực tuyến; ảnh hưởng đến sức khỏe tinh thần.

– Sử dụng được khung phân loại 4C để nhận diện và phân tích các nguy cơ trực tuyến đối với học sinh.

– Nhận diện được mối liên hệ đan xen giữa các nguy cơ để có cách tiếp cận giáo dục tổng thể.

KHỞI ĐỘNG

Hoạt động khởi động: "Tin nhắn này có vấn đề gì?" (10 phút)
Báo cáo viên chiếu 4 tin nhắn giả định: (1) "Chúc mừng bạn trúng iPhone, bấm link để nhận quà"; (2) "Mình là admin game, gửi mã OTP để mình tặng skin miễn phí"; (3) "Bạn xinh quá, mình làm quen nhé, đừng nói với ai"; (4) "Thầy chủ nhiệm đây, em vào link này điền thông tin để nhận học bổng". Thầy cô xác định dấu hiệu bất thường trong từng tin nhắn.
Gợi ý: Các dấu hiệu chung: lợi ích bất ngờ, hối thúc, yêu cầu thông tin bí mật (OTP, mật khẩu), đề nghị giữ bí mật, đường link lạ, giả danh người có uy tín. Báo cáo viên dẫn dắt: nhiều nguy cơ khác nhau nhưng có chung "mẫu thao túng" – đây là điểm then chốt để giáo dục học sinh.

NỘI DUNG

2.1. Khung phân loại nguy cơ trực tuyến 4C

Để nhận diện một cách hệ thống các nguy cơ đối với học sinh, tài liệu sử dụng khung phân loại 4C do mạng lưới nghiên cứu châu Âu CO:RE đề xuất (Livingstone & Stoilova, 2021) và được OECD sử dụng trong khuyến nghị về trẻ em trong môi trường số (OECD, 2021). Khung này xác định bốn nhóm nguy cơ căn cứ vào vai trò của học sinh trong tình huống rủi ro:

Nhóm nguy cơ	**Vai trò của học sinh**	**Ví dụ**
Nội dung (Content)	Học sinh là người tiếp nhận nội dung có hại	Nội dung bạo lực, khiêu dâm, tin giả, nội dung cổ xúy tự gây hại, thù ghét, cực đoan.
Tiếp xúc (Contact)	Học sinh là đối tượng bị người khác chủ động tiếp cận	Dụ dỗ, quấy rối, lừa đảo giả danh, lôi kéo vào hoạt động phạm pháp.
Hành vi (Conduct)	Học sinh là người tham gia, thậm chí gây ra hành vi rủi ro	Bắt nạt người khác, chia sẻ hình ảnh nhạy cảm, tham gia "thử thách" nguy hiểm, phát tán tin giả.
Hợp đồng (Contract)	Học sinh là bên tham gia giao dịch, bị khai thác về tài chính, dữ liệu	Lừa đảo mua bán, cờ bạc trá hình, vật phẩm ngẫu nhiên trong game, thu thập dữ liệu cá nhân, quảng cáo nhắm mục tiêu.

Bảng 2.1. Khung phân loại nguy cơ trực tuyến 4C

Bên cạnh bốn nhóm trên, Livingstone và Stoilova (2021) chỉ ra các nguy cơ xuyên suốt: xâm phạm quyền riêng tư, ảnh hưởng đến sức khỏe thể chất và tinh thần, bất bình đẳng trong tiếp cận và bảo vệ. Cần lưu ý ba điểm khi vận dụng khung 4C:

– **Các nguy cơ đan xen và chuyển hóa:** một học sinh kết bạn với người lạ (tiếp xúc) có thể bị dẫn dắt gửi ảnh nhạy cảm (hành vi), sau đó bị tống tiền (hợp đồng) và rơi vào khủng hoảng tâm lý (sức khỏe tinh thần).

– **Rủi ro không đồng nghĩa với tổn hại:** mức độ tổn hại phụ thuộc vào yếu tố bảo vệ như kỹ năng của học sinh, sự hỗ trợ của gia đình, nhà trường.

– **Học sinh vừa có thể là nạn nhân vừa có thể là người gây hại:** giáo dục cần hướng đến cả phòng ngừa trở thành nạn nhân và phòng ngừa gây hại cho người khác.

Các mục 2.2 – 2.10 dưới đây trình bày các nguy cơ cụ thể theo cùng một cấu trúc: bản chất; biểu hiện thường gặp ở học sinh; dấu hiệu cảnh báo; biện pháp phòng ngừa. Cách xử lý khi sự cố đã xảy ra được trình bày ở Chuyên đề 4.

2.2. Lừa đảo trực tuyến và chiếm đoạt tài khoản

2.2.1. Bản chất

Lừa đảo trực tuyến là việc sử dụng thủ đoạn gian dối trên môi trường mạng nhằm chiếm đoạt tài sản, thông tin hoặc tài khoản của người khác. Các thủ đoạn lừa đảo khai thác những đặc điểm tâm lý phổ biến: lòng tin vào người có thẩm quyền, mong muốn nhận lợi ích, nỗi sợ hãi và tâm lý bị hối thúc. Theo Hiệp hội An ninh mạng quốc gia, năm 2025 các hình thức lừa đảo phổ biến nhất là mạo danh công an, thông báo trúng thưởng, mời gọi đầu tư, giả danh nhân viên giao hàng và lừa đảo qua quan hệ tình cảm; thiệt hại ước tính trên 6.000 tỷ đồng trong 11 tháng năm 2025 theo số liệu của Bộ Công an.

2.2.2. Biểu hiện thường gặp ở học sinh

– **"Bắt cóc online":** đối tượng giả danh công an, viện kiểm sát, tòa án gọi điện, gọi video cho học sinh, đe dọa rằng học sinh liên quan đến một vụ án; yêu cầu học sinh giữ bí mật, đến một nhà nghỉ, khách sạn, cắt liên lạc với gia đình, tự quay video bị "bắt cóc" để đối tượng tống tiền gia đình. Bộ Giáo dục và Đào tạo đã có văn bản cảnh báo thủ đoạn này trên cơ sở thông tin của Cục Cảnh sát hình sự, Bộ Công an.

– **Lừa đảo trong trò chơi trực tuyến:** hứa tặng vật phẩm, tài khoản cấp cao, nạp thẻ giá rẻ; yêu cầu học sinh cung cấp tài khoản, mật khẩu, mã OTP hoặc chuyển tiền trước.

– **Giả mạo nhà trường, giáo viên:** gửi đường link "đăng ký học bổng", "các suất học bổng du học", "nộp học phí", "cập nhật hồ sơ" để đánh cắp thông tin đăng nhập.

– **Chiếm đoạt tài khoản mạng xã hội:** lừa lấy mật khẩu, mã OTP, sau đó dùng tài khoản của học sinh để nhắn tin vay tiền bạn bè, người thân, phát tán nội dung xấu.

– **"Việc nhẹ lương cao", cộng tác viên online, làm nhiệm vụ nhận hoa hồng:** chủ yếu nhắm vào học sinh THPT; nạn nhân phải nạp tiền để "nhận nhiệm

vụ" và mất dần số tiền lớn hơn; một số trường hợp bị lôi kéo đi lao động trái phép ở nước ngoài.

– **Mua bán trực tuyến:** đặt cọc mua hàng, mua vé sự kiện, mua đồ cũ không có thật.

2.2.3. Dấu hiệu cảnh báo

– Lời đề nghị "quá tốt để là thật", quà tặng, lợi nhuận bất thường.

– Hối thúc phải làm ngay, đe dọa hậu quả nếu không làm.

– Yêu cầu giữ bí mật với cha mẹ, thầy cô.

– Yêu cầu cung cấp mật khẩu, mã OTP, thông tin thẻ, ảnh căn cước, hoặc cài đặt ứng dụng từ đường link lạ.

– Giả danh người có thẩm quyền làm việc qua điện thoại, mạng xã hội (cơ quan công an không làm việc, không yêu cầu chuyển tiền qua điện thoại, mạng xã hội).

2.2.4. Phòng ngừa

– Hình thành ở học sinh nguyên tắc "**Dừng lại – Kiểm tra – Hỏi người lớn**" trước mọi yêu cầu liên quan đến tiền, mật khẩu, mã OTP, thông tin cá nhân.

– Hướng dẫn học sinh thiết lập mật khẩu mạnh, không dùng chung mật khẩu, bật xác thực hai yếu tố, kiểm tra địa chỉ trang web trước khi đăng nhập.

– Thống nhất với cha mẹ học sinh "câu hỏi bí mật" hoặc cách kiểm chứng khi nhận được cuộc gọi khẩn cấp liên quan đến con.

– Nhà trường công bố rõ các kênh liên lạc chính thức; khẳng định nhà trường không yêu cầu học sinh cung cấp mật khẩu hay chuyển tiền qua đường link.

2.3. Lộ lọt dữ liệu cá nhân và xâm phạm quyền riêng tư

2.3.1. Bản chất

Theo Điều 2 Luật Bảo vệ dữ liệu cá nhân năm 2025 (Luật số 91/2025/QH15), dữ liệu cá nhân là dữ liệu số hoặc thông tin dưới dạng khác xác định hoặc giúp xác định một con người cụ thể, bao gồm: dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm. Dữ liệu cá nhân sau khi khử nhận dạng không còn là dữ liệu cá nhân. Dữ liệu cá nhân cơ bản là dữ liệu cá nhân phản ánh các yếu tố nhân thân, lai lịch phổ biến, thường xuyên sử dụng trong các giao dịch, quan hệ xã hội, thuộc danh mục do Chính phủ ban hành. Dữ liệu cá nhân nhạy cảm là dữ liệu gắn liền với quyền riêng tư mà khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp đến quyền và lợi ích hợp pháp của cá nhân.

Dữ liệu cá nhân là thông tin gắn với một người cụ thể hoặc giúp xác định một người cụ thể: họ tên, ngày sinh, địa chỉ, số điện thoại, trường lớp, hình ảnh, giọng nói, vị trí, thông tin tài khoản… Khi học sinh chia sẻ dữ liệu cá nhân thiếu kiểm soát, các em có thể bị lợi dụng để lừa đảo, theo dõi, quấy rối, dụ dỗ, giả mạo danh tính. Dữ liệu trên mạng có thể tồn tại lâu dài, tạo thành "dấu chân số" ảnh hưởng đến học tập, nghề nghiệp sau này.

2.3.2. Biểu hiện thường gặp ở học sinh

– Đăng ảnh có đồng phục, bảng tên trường, biển số nhà; chia sẻ vị trí theo thời gian thực; công khai lịch sinh hoạt.

– Tham gia các trào lưu "điền thông tin", trắc nghiệm vui yêu cầu ngày sinh, tên thú cưng, tên trường (thường là câu hỏi bảo mật của tài khoản).

– Đăng ảnh, video của bạn bè khi chưa xin phép; chụp ảnh màn hình tin nhắn riêng để đăng công khai.

– Cấp quyền truy cập danh bạ, ảnh, vị trí cho ứng dụng không rõ nguồn gốc.

2.3.3. Phòng ngừa

– Giúp học sinh phân biệt thông tin công khai được, thông tin cần hạn chế và thông tin tuyệt đối không chia sẻ.

– Hướng dẫn thiết lập quyền riêng tư, kiểm tra quyền truy cập của ứng dụng, tắt định vị không cần thiết.

– Giáo dục nguyên tắc "**xin phép trước khi đăng**" ảnh, thông tin của người khác, gắn với quyền của chủ thể dữ liệu theo Luật Bảo vệ dữ liệu cá nhân năm 2025.

– Đối với học sinh THPT: thảo luận về dấu chân số và hình ảnh cá nhân trực tuyến gắn với tuyển sinh, tuyển dụng.

– Học sinh và giáo viên cần thành thạo kỹ thuật bảo mật nền tảng: biết cách tạo mật khẩu mạnh (chuỗi câu dài) và tự thao tác bật xác thực 2 lớp (2FA) trên các tài khoản Zalo, Facebook, Gmail cá nhân và ngành.

2.4. Sử dụng thiết bị số quá mức, nghiện trò chơi điện tử và mạng xã hội

2.4.1. Bản chất

Cần phân biệt "sử dụng nhiều" với "sử dụng có vấn đề". Thời gian sử dụng không phải là tiêu chí duy nhất; điều quan trọng là việc sử dụng có ảnh hưởng tiêu cực đến học tập, giấc ngủ, sức khỏe, các mối quan hệ và khả năng tự kiểm soát hay không. Tổ chức Y tế Thế giới đưa "rối loạn chơi trò chơi" (gaming disorder) vào Bảng phân loại bệnh quốc tế ICD-11 với ba đặc điểm: (1) suy giảm khả năng

kiểm soát việc chơi; (2) ưu tiên chơi game hơn các hoạt động và mối quan tâm khác; (3) tiếp tục chơi dù đã có hậu quả tiêu cực; các biểu hiện kéo dài thường ít nhất 12 tháng và gây suy giảm đáng kể chức năng (WHO, 2019). Việc chẩn đoán thuộc thẩm quyền của chuyên gia y tế; giáo viên không "dán nhãn" nghiện cho học sinh mà chỉ nhận diện dấu hiệu để hỗ trợ, chuyển gửi.

Nhiều nền tảng số được thiết kế để tối đa hóa thời gian sử dụng (cuộn vô tận, tự động phát, thông báo liên tục, phần thưởng ngẫu nhiên). Học sinh ở tuổi vị thành niên, với hệ thống tưởng thưởng hoạt động mạnh và khả năng tự kiểm soát chưa hoàn thiện, đặc biệt dễ bị cuốn vào các cơ chế này.

2.4.2. Dấu hiệu cảnh báo

– Thường xuyên thiếu ngủ, mệt mỏi, ngủ gật trong lớp; kết quả học tập giảm sút.

– Cáu gắt, bồn chồn khi không được sử dụng thiết bị; nói dối về thời gian sử dụng.

– Từ bỏ các sở thích, hoạt động thể chất, quan hệ bạn bè trực tiếp.

– Tiêu tiền (kể cả lấy tiền của gia đình) để nạp game, mua vật phẩm.

2.4.3. Phòng ngừa

– Giáo dục học sinh tự theo dõi thời gian sử dụng bằng công cụ có sẵn trên thiết bị, tự đặt mục tiêu và kế hoạch cân bằng.

– Giúp học sinh nhận diện các "thiết kế lôi kéo" của nền tảng để chủ động kiểm soát.

– Phối hợp với cha mẹ xây dựng thỏa thuận sử dụng thiết bị trong gia đình (thời gian, không gian không dùng thiết bị, giờ đi ngủ); hướng dẫn cha mẹ sử dụng chức năng quản lý của gia đình và thực hiện quy định về tài khoản game của người dưới 16 tuổi theo Nghị định 147/2024/NĐ-CP.

– Tạo cơ hội cho học sinh tham gia hoạt động thể chất, nghệ thuật, câu lạc bộ – các hoạt động thay thế có giá trị.

2.5. Tin giả, thông tin sai sự thật và nội dung có hại

2.5.1. Bản chất

Theo Điều 3 Nghị định số 328/2026/NĐ-CP về quy định phòng, chống tin giả, tin sai sự thật, tin giả, tin sai sự thật là thông tin không có thật hoặc có một phần sự thật xâm hại đến an ninh, uy tín, hình ảnh quốc gia, trật tự, an toàn xã hội, quyền, lợi ích hợp pháp của cá nhân, tổ chức gồm các loại thông tin: thông tin giả, thông tin sai sự thật, thông tin sai lệch, thông tin giả mạo, thông tin bịa đặt, thông

tin vu khống, thông tin xuyên tạc. Nghiên cứu trên mạng xã hội cho thấy tin sai lan truyền nhanh hơn, xa hơn và rộng hơn tin đúng, chủ yếu do con người chia sẻ vì tính mới lạ và cảm xúc mạnh mà nội dung gợi ra (Vosoughi và cộng sự, 2018). Nội dung có hại đối với học sinh còn bao gồm nội dung bạo lực, khiêu dâm, thù ghét, phân biệt đối xử, cực đoan, nội dung mô tả hoặc cổ xúy hành vi tự gây hại, rối loạn ăn uống.

2.5.2. Biểu hiện thường gặp ở học sinh

– Chia sẻ tin "giật gân" về sức khỏe, thiên tai, sự kiện của trường mà không kiểm chứng; tin vào thông tin sai về thi cử, tuyển sinh.

– Vô tình tiếp xúc nội dung bạo lực, khiêu dâm qua quảng cáo bật lên, gõ sai địa chỉ, gợi ý của thuật toán.

– Bị thuật toán đề xuất liên tục cùng một loại nội dung, hình thành "buồng vang" củng cố định kiến.

– Tiếp xúc nội dung xuyên tạc lịch sử, kích động, chống phá.

2.5.3. Phòng ngừa

– Rèn luyện kỹ năng kiểm chứng: đặt câu hỏi "Ai nói? Bằng chứng ở đâu? Nguồn khác nói gì?"; kỹ thuật "đọc ngang" – rời trang đang đọc để tìm thông tin về nguồn ở các trang độc lập, kỹ thuật được chứng minh hiệu quả hơn việc chỉ xem xét bề ngoài trang web (Wineburg & McGrew, 2019).

– Hình thành thói quen "**dừng lại trước khi chia sẻ**", đặc biệt với nội dung gây cảm xúc mạnh.

– Hướng dẫn học sinh báo cáo, gắn cờ nội dung có hại và rời khỏi nội dung gây khó chịu, kể với người lớn tin cậy.

– Lồng ghép vào Ngữ văn (đọc hiểu văn bản thông tin, nghị luận), Giáo dục công dân, Giáo dục kinh tế và pháp luật, Lịch sử, Tin học.

2.6. "Thử thách" nguy hiểm, cờ bạc và cá cược trực tuyến

2.6.1. "Thử thách" nguy hiểm

"Thử thách" trực tuyến là các trào lưu kêu gọi người dùng thực hiện một hành động, ghi hình và chia sẻ. Phần lớn thử thách vô hại, nhưng một số có tính nguy hiểm (nhịn thở, ăn uống chất không an toàn, nhảy khỏi xe đang chạy, tự gây thương tích, phá hoại tài sản). Học sinh tham gia do nhu cầu được chú ý, được bạn bè công nhận, tò mò và đánh giá thấp rủi ro. Một số "thử thách" là tin đồn, câu chuyện dọa dẫm được lan truyền và thổi phồng; việc cảnh báo thiếu thận trọng

(nêu tên, mô tả chi tiết) có thể vô tình làm học sinh tò mò tìm kiếm (Praesidio Safeguarding, 2021).

Phòng ngừa: giáo viên không phổ biến tên, cách thực hiện các thử thách cụ thể; tập trung giáo dục năng lực chung: đánh giá rủi ro theo bốn bước (thử thách là gì – có thể dẫn đến điều gì tồi tệ nhất – có đáng không – hỏi ý kiến người lớn), kỹ năng từ chối áp lực nhóm và khuyến khích học sinh kể với người lớn khi thấy nội dung khiến các em lo lắng.

2.6.2. Cờ bạc và cá cược trực tuyến, các hình thức trá hình

Cờ bạc trực tuyến (cá độ bóng đá, sòng bạc trực tuyến) là hành vi vi phạm pháp luật và có thể bị xử lý hình sự theo Điều 321, 322 Bộ luật Hình sự. Học sinh có thể tiếp cận qua quảng cáo trên mạng xã hội, livestream, nhóm chat và lời rủ rê của bạn bè. Bên cạnh đó là các hình thức mang yếu tố may rủi trong trò chơi điện tử như hộp quà ngẫu nhiên (loot box), vòng quay may mắn mua bằng tiền thật. Nghiên cứu trên quy mô lớn cho thấy mức chi tiêu cho loot box có liên hệ với mức độ cờ bạc có vấn đề (Zendle & Cairns, 2018). Học sinh tham gia cờ bạc có nguy cơ nợ nần, vay nặng lãi, bị đe dọa, lôi kéo vào hoạt động phạm pháp.

Dấu hiệu cảnh báo: thường xuyên cần tiền, bán hoặc cầm cố đồ dùng, vay mượn bạn bè; căng thẳng theo kết quả trận đấu; giấu điện thoại; có giao dịch chuyển khoản bất thường.

Phòng ngừa: giáo dục bản chất "nhà cái luôn thắng" bằng các ví dụ xác suất (lồng ghép môn Toán); phân tích các kỹ thuật quảng cáo lôi kéo; giáo dục pháp luật về cờ bạc; phối hợp với cha mẹ quản lý chi tiêu, tài khoản ngân hàng, ví điện tử của học sinh.

2.7. Nội dung do trí tuệ nhân tạo tạo ra

2.7.1. Bản chất

Công nghệ trí tuệ nhân tạo tạo sinh cho phép tạo ra văn bản, hình ảnh, video, giọng nói giống thật với chi phí thấp. Công nghệ này mang lại cơ hội học tập to lớn và là một miền trong Khung năng lực số cho người học, nhưng đồng thời tạo ra các nguy cơ mới (Chesney & Citron, 2019; UNICEF, 2021):

– **Deepfake gây tổn hại danh dự và tống tiền:** ghép khuôn mặt học sinh vào hình ảnh, video nhạy cảm từ những bức ảnh công khai trên mạng xã hội hoặc trang của trường; sử dụng để bắt nạt, làm nhục hoặc tống tiền. Trong một số trường hợp, người tạo ra nội dung giả lại chính là bạn học.

– **Lừa đảo bằng giả giọng, giả hình:** gọi video, gửi tin nhắn thoại giả giọng người thân, giáo viên để yêu cầu chuyển tiền hoặc cung cấp thông tin.

– **Tài liệu xâm hại tình dục trẻ em do AI tạo ra:** dù là ảnh giả, việc tạo ra, tàng trữ, phát tán vẫn gây tổn hại nghiêm trọng cho nạn nhân và là hành vi vi phạm pháp luật (theo Điều 76 Luật An ninh mạng năm 2025).

– **Dụ dỗ được hỗ trợ bởi AI:** đối tượng xấu dùng AI phân tích dữ liệu công khai của học sinh để cá nhân hóa cách tiếp cận, tạo hồ sơ giả thuyết phục.

– **Chatbot "bạn đồng hành":** học sinh có thể gắn bó cảm xúc với chatbot, chia sẻ thông tin riêng tư hoặc nhận những phản hồi không phù hợp về các vấn đề sức khỏe tinh thần.

2.7.2. Phòng ngừa

– Giáo dục học sinh biết rằng hình ảnh, video, giọng nói có thể bị làm giả; rèn thói quen kiểm chứng qua kênh độc lập (gọi lại số điện thoại đã biết, hỏi trực tiếp).

– Hạn chế đăng tải ảnh khuôn mặt rõ nét ở chế độ công khai; nhà trường thận trọng khi đăng ảnh học sinh.

– Giáo dục đạo đức và pháp luật: tạo, chia sẻ nội dung giả mạo người khác là hành vi gây tổn hại, có thể bị xử lý theo quy định.

– Hướng dẫn sử dụng AI có trách nhiệm trong học tập; khẳng định chatbot không thay thế được sự hỗ trợ của con người khi học sinh gặp khó khăn tâm lý.

2.8. Bắt nạt trực tuyến

2.8.1. Bản chất

Bắt nạt trực tuyến là hành vi gây hấn có chủ ý, thường lặp lại, do cá nhân hoặc nhóm thực hiện thông qua phương tiện điện tử nhằm vào người khó tự bảo vệ mình (Kowalski và cộng sự, 2014). Bắt nạt trực tuyến có các hình thức: nhắn tin, bình luận xúc phạm, đe dọa; lan truyền tin đồn; đăng ảnh, video làm nhục; giả mạo tài khoản; cô lập, loại khỏi nhóm; công khai thông tin riêng tư. So với bắt nạt trực tiếp, bắt nạt trực tuyến có những đặc điểm làm tăng tổn hại: diễn ra mọi lúc, mọi nơi, nạn nhân không có "nơi an toàn"; nội dung có thể lan truyền rộng và tồn tại lâu dài; người bắt nạt có thể ẩn danh; số người chứng kiến rất lớn.

2.8.2. Tác động

Tổng hợp nghiên cứu cho thấy bắt nạt trực tuyến liên quan đến lo âu, trầm cảm, cô đơn, giảm lòng tự trọng, suy giảm kết quả học tập, các triệu chứng cơ thể và trong những trường hợp nghiêm trọng là ý nghĩ tự sát (Kowalski và cộng sự,

2014). Học sinh có hành vi bắt nạt cũng có nguy cơ cao gặp vấn đề hành vi về sau. Học sinh vừa là nạn nhân vừa là người bắt nạt là nhóm đặc biệt dễ tổn thương. Bắt nạt trực tuyến và bắt nạt trực tiếp có liên quan chặt chẽ: phần lớn học sinh bị bắt nạt trên mạng cũng bị bắt nạt ở trường và người bắt nạt thường là bạn học.

2.8.3. Dấu hiệu cảnh báo

– Đột ngột ngừng sử dụng hoặc sử dụng thiết bị một cách lo lắng, giật mình khi có thông báo.

– Né tránh đến trường, tách khỏi nhóm bạn, xuất hiện căng thẳng với một nhóm học sinh cụ thể.

– Buồn bã, cáu gắt, mất ngủ, than đau đầu, đau bụng không rõ nguyên nhân.

– Có tài khoản giả mạo, nhóm chat chế giễu một học sinh trong lớp.

2.8.4. Phòng ngừa

– Xây dựng quy tắc ứng xử trên nhóm trực tuyến của lớp, trường cùng học sinh.

– Giáo dục vai trò của người chứng kiến: không "thả tim", không chia sẻ, không im lặng; hỗ trợ bạn và báo người lớn.

– Phát triển năng lực đồng cảm, quản lý cảm xúc, giải quyết xung đột.

– Duy trì kênh báo cáo an toàn, có thể ẩn danh.

2.9. Xâm hại và bóc lột tình dục trẻ em trực tuyến

2.9.1. Bản chất và các hình thức

Xâm hại và bóc lột tình dục trẻ em trực tuyến (OCSEA) bao gồm các hành vi xâm hại tình dục được thực hiện, hỗ trợ hoặc lan truyền qua công nghệ số. Các hình thức chủ yếu gồm:

– **Dụ dỗ trực tuyến (grooming):** xây dựng mối quan hệ tin cậy, phụ thuộc cảm xúc nhằm mục đích xâm hại.

– **Sản xuất, phát tán tài liệu xâm hại tình dục trẻ em (CSAM):** bao gồm cả hình ảnh do học sinh tự chụp dưới áp lực, bị lừa hoặc bị ép buộc.

– **Tống tiền tình dục (sextortion):** đe dọa phát tán hình ảnh để ép nạn nhân gửi thêm hình ảnh, tiền hoặc thực hiện hành vi tình dục.

– **Quấy rối tình dục trực tuyến:** gửi tin nhắn, bình luận, hình ảnh mang tính tình dục không mong muốn.

– **Phát tán hình ảnh riêng tư không có sự đồng ý:** thường xảy ra sau khi một mối quan hệ tình cảm kết thúc.

Theo pháp luật Việt Nam, sử dụng người dưới 16 tuổi vào mục đích khiêu dâm là tội phạm (Điều 147 Bộ luật Hình sự). Học sinh tự chụp, gửi hình ảnh nhạy cảm trước hết cần được nhìn nhận là đối tượng cần được bảo vệ, không phải là người có lỗi.

2.9.2. Quá trình dụ dỗ trực tuyến

Các nghiên cứu về hành vi dụ dỗ trực tuyến (Webster và cộng sự, 2012; Whittle và cộng sự, 2013) mô tả quá trình này thường trải qua các giai đoạn đan xen:

Giai đoạn	**Biểu hiện**
Lựa chọn mục tiêu	"Quét" các không gian trực tuyến, ưu tiên học sinh bộc lộ cô đơn, mâu thuẫn với gia đình, thiếu tự tin, cần tiền hoặc có tên tài khoản, hình ảnh gợi ý.
Xây dựng lòng tin	Khen ngợi, đóng vai người bạn đồng trang lứa hoặc người cố vấn; thể hiện sự đồng cảm, cùng sở thích; tặng quà, thẻ nạp game, vật phẩm.
Tạo sự phụ thuộc và cô lập	Khuyến khích học sinh tin rằng chỉ có mình hiểu em; chuyển sang ứng dụng riêng tư; yêu cầu giữ bí mật với cha mẹ, thầy cô.
Bình thường hóa nội dung tình dục	Đưa dần chủ đề tình dục vào trò chuyện dưới dạng đùa, trò chơi, "bài học"; gửi hình ảnh khiêu dâm để làm giảm sự nhạy cảm.
Xâm hại và kiểm soát	Yêu cầu hình ảnh, video, gọi video; đề nghị gặp mặt; đe dọa phát tán để duy trì kiểm soát.

Bảng 2.2. Các giai đoạn của quá trình dụ dỗ trực tuyến

Quá trình này có thể diễn ra trong vài giờ hoặc kéo dài nhiều tháng. Người dụ dỗ không nhất thiết là người lạ; nhiều trường hợp là người học sinh đã quen biết. Theo cơ quan thực thi pháp luật Việt Nam, đối tượng phạm tội thường lợi dụng sự dễ tổn thương về cảm xúc, hoàn cảnh kinh tế khó khăn của nạn nhân, sử dụng vật chất, tiền và các mối quan hệ thân thiết; mạng xã hội được sử dụng rộng rãi để xác định, tiếp cận và xây dựng lòng tin với nạn nhân tiềm năng (ECPAT, INTERPOL & UNICEF, 2022).

2.9.3. Chia sẻ hình ảnh nhạy cảm ở học sinh

Phân tích tổng hợp quốc tế cho thấy khoảng 15% thanh thiếu niên từng gửi và khoảng 27% từng nhận tin nhắn, hình ảnh mang tính tình dục; khoảng 12% từng chuyển tiếp hình ảnh không có sự đồng ý của người trong ảnh (Madigan và cộng sự, 2018). Tại Việt Nam, tỷ lệ tự báo cáo về hành vi bị chia sẻ hình ảnh nhạy cảm thấp hơn thực tế do học sinh ngại tiết lộ nhưng các nhà nghiên cứu lưu ý con số thực có thể cao hơn do học sinh ngại tiết lộ (ECPAT, INTERPOL & UNICEF, 2022). Nguyên nhân dẫn đến hành vi này gồm: nhu cầu khẳng định bản thân, thân mật trong quan hệ tình cảm, tò mò, áp lực từ bạn bè hoặc người yêu, bị lừa dối, bị ép buộc. Hậu quả nghiêm trọng nhất xảy ra khi hình ảnh bị phát tán hoặc bị dùng để tống tiền.

2.9.4. Dấu hiệu cảnh báo

– Có "người bạn" trên mạng mà học sinh giấu kín; nhận quà, tiền, thẻ nạp không rõ nguồn gốc.

– Sử dụng thiết bị vào ban đêm, giấu màn hình, có tài khoản, ứng dụng ẩn.

– Có kiến thức, ngôn ngữ, hành vi tình dục không phù hợp lứa tuổi.

– Thay đổi đột ngột: sợ hãi, lo âu, xấu hổ, thu mình, tự trách bản thân, giảm sút học tập; biểu hiện hoảng loạn khi nhận tin nhắn.

2.9.5. Phòng ngừa

– Giáo dục giới tính, sức khỏe sinh sản, quyền về thân thể và ranh giới cá nhân phù hợp lứa tuổi; khái niệm đồng thuận trong các mối quan hệ.

– Nhận diện dấu hiệu dụ dỗ; khẳng định "người lớn đáng tin cậy không bao giờ yêu cầu em giữ bí mật với cha mẹ, thầy cô".

– Thông điệp then chốt: "**Nếu em bị đe dọa, đó không phải lỗi của em; đừng gửi thêm, đừng trả tiền, hãy kể với người lớn ngay**".

– Tránh cách giáo dục gây sợ hãi, đổ lỗi, xấu hổ – điều này khiến học sinh không dám tiết lộ khi gặp sự cố.

2.10. Môi trường số và sức khỏe tinh thần của học sinh

2.10.1. Bản chất

Mối quan hệ giữa sử dụng công nghệ số và sức khỏe tinh thần của thanh thiếu niên là phức tạp. Các nghiên cứu quy mô lớn cho thấy mối liên hệ trung bình giữa thời gian sử dụng công nghệ và mức độ hạnh phúc của thanh thiếu niên là có nhưng nhỏ (Orben & Przybylski, 2019); tác động phụ thuộc vào nội dung, cách sử dụng và đặc điểm cá nhân. Những học sinh vốn đã dễ tổn thương ngoài đời thực thường cũng dễ tổn thương hơn trên mạng (Odgers & Jensen, 2020). Vì vậy, giáo viên cần tránh hai thái cực: coi công nghệ là nguyên nhân của mọi vấn đề hoặc bỏ qua tác động của môi trường mạng.

2.10.2. Các cơ chế tác động tiêu cực cần lưu ý

– **So sánh xã hội và hình ảnh cơ thể:** tiếp xúc liên tục với hình ảnh đã chỉnh sửa, "cuộc sống hoàn hảo" của người khác dẫn đến không hài lòng với bản thân, cơ thể.

– **Nỗi sợ bị bỏ lỡ và áp lực phải trực tuyến liên tục,** lo âu khi không nhận được phản hồi, lượt thích.

– **Ảnh hưởng đến giấc ngủ** do sử dụng thiết bị vào ban đêm.

– **Tiếp xúc nội dung về tự gây hại, rối loạn ăn uống** và các cộng đồng trực tuyến bình thường hóa những hành vi này.

– **Hệ quả của các sự cố trực tuyến** như bắt nạt, tống tiền, lừa đảo dẫn đến khủng hoảng tâm lý.

2.10.3. Mặt tích cực cần phát huy

Môi trường số cũng là nguồn hỗ trợ: học sinh tìm kiếm thông tin sức khỏe, kết nối với bạn bè, tham gia cộng đồng có cùng sở thích, tiếp cận dịch vụ tư vấn. Giáo viên cần giúp học sinh biết tìm đến các nguồn hỗ trợ tin cậy (Tổng đài 111 (Tổng đài Quốc gia Bảo vệ Trẻ em, Cục Bà mẹ và Trẻ em), người làm tư vấn học đường, cơ sở y tế) và phân biệt với nguồn không tin cậy.

2.10.4. Phòng ngừa

– Giáo dục kỹ năng tự nhận thức, quản lý cảm xúc, tư duy phê phán về hình ảnh trên mạng.

– Khuyến khích "vệ sinh số": không dùng thiết bị trước giờ ngủ, tắt thông báo không cần thiết, chủ động lựa chọn nội dung tích cực.

– Tạo môi trường lớp học an toàn, nơi học sinh có thể nói về cảm xúc mà không bị phán xét.

– Phát hiện sớm và chuyển gửi kịp thời học sinh có dấu hiệu khủng hoảng (xem Chuyên đề 4).

2.11. Văn hóa ứng xử trên không gian mạng – yếu tố bảo vệ chung

Các nguy cơ nêu trên cho thấy học sinh không chỉ cần kỹ năng tự bảo vệ mà còn cần văn hóa ứng xử số: tôn trọng người khác, sử dụng ngôn ngữ phù hợp, không phát tán thông tin sai, không tham gia bắt nạt, tôn trọng quyền riêng tư và quyền tác giả, có trách nhiệm với nội dung mình tạo ra và chia sẻ. Văn hóa ứng xử là yếu tố bảo vệ chung cho cả cộng đồng học sinh, giúp giảm nguy cơ ở nhóm "hành vi" trong khung 4C và là nội dung xuyên suốt của Chuyên đề 3.

HOẠT ĐỘNG TẬP HUẤN

Hoạt động 2.1. Phân loại và chuỗi nguy cơ (30 phút)

Các nhóm nhận tình huống, từ đó xác định các nguy cơ theo khung 4C và vẽ "chuỗi nguy cơ" (nguy cơ này dẫn đến nguy cơ khác như thế nào):

Tình huống: "Nam (lớp 8) chơi game trực tuyến, được một tài khoản tặng vật phẩm hiếm. Sau đó tài khoản này đề nghị Nam đăng nhập vào một trang web để nhận thêm quà. Một tuần sau, tài khoản game và Facebook của Nam bị chiếm, kẻ gian nhắn tin vay tiền bạn bè Nam và đăng những hình ảnh chế giễu Nam lên nhóm lớp."

Gợi ý: Tiếp xúc (người lạ tặng quà) → Hợp đồng (lừa đảo giả mạo, chiếm đoạt tài khoản) → Hành vi (tài khoản của Nam bị dùng để lừa đảo người khác) → Nội dung/hành vi (hình ảnh chế giễu – bắt nạt) → Sức khỏe tinh thần (xấu hổ, lo âu, mất lòng tin của bạn bè). Bài học: giáo dục cần giúp học sinh nhận ra dấu hiệu ở "mắt xích đầu tiên".

Hoạt động 2.2. Phiếu nhận diện nguy cơ theo cấp học (40 phút)

Nhóm thầy cô cùng cấp học hoàn thành bảng: liệt kê 3 nguy cơ phổ biến nhất ở học sinh cấp học mình; với mỗi nguy cơ, nêu 2 dấu hiệu cảnh báo giáo viên có thể quan sát được ở trường và 1 biện pháp phòng ngừa có thể thực hiện trong tiết sinh hoạt lớp.

Gợi ý: Tiểu học: lừa đảo trúng thưởng, nội dung không phù hợp, chia sẻ thông tin cá nhân. THCS: lừa đảo trong game, bắt nạt trực tuyến, dụ dỗ trực tuyến. THPT: "việc nhẹ lương cao", tin giả và deepfake, cờ bạc trực tuyến, phát tán hình ảnh riêng tư. Dấu hiệu quan sát được ở trường: thay đổi cảm xúc, né tránh, mệt mỏi, căng thẳng với bạn, thường xuyên cần tiền.

Hoạt động 2.3. Thông điệp giáo dục không gây sợ hãi (20 phút)
Thầy cô nhận xét thông điệp sau và viết lại cho phù hợp: "Các em tuyệt đối không được gửi ảnh cho ai. Ai gửi ảnh nhạy cảm là hư hỏng và phải chịu trách nhiệm!"
Gợi ý: Thông điệp mang tính đổ lỗi, gây xấu hổ, khiến học sinh đã lỡ gửi ảnh không dám tìm kiếm giúp đỡ. Thông điệp phù hợp: "Cơ thể và hình ảnh của em là của riêng em. Em có quyền từ chối mọi yêu cầu khiến em không thoải mái. Nếu ai đó đe dọa em vì một bức ảnh, đó là lỗi của người đe dọa, không phải lỗi của em. Đừng gửi thêm, đừng trả tiền và hãy kể với thầy cô hoặc bố mẹ – chúng tôi sẽ giúp em."

GHI NHỚ

– Khung 4C (Nội dung – Tiếp xúc – Hành vi – Hợp đồng) giúp nhận diện nguy cơ một cách hệ thống; các nguy cơ thường đan xen và chuyển hóa.

– Nhiều nguy cơ có chung "mẫu thao túng": lợi ích bất ngờ, hối thúc, đe dọa, yêu cầu giữ bí mật, yêu cầu thông tin bí mật.

– Giáo viên nhận diện dấu hiệu để hỗ trợ, chuyển gửi; không chẩn đoán, không dán nhãn học sinh.

– Giáo dục phòng ngừa phải tránh gây sợ hãi, đổ lỗi; thông điệp cốt lõi là "Không phải lỗi của em – hãy kể với người lớn".

CÂU HỎI TỰ ĐÁNH GIÁ

1. Trình bày bốn nhóm nguy cơ trong khung 4C và cho mỗi nhóm một ví dụ ở học sinh cấp học thầy cô phụ trách.

2. Nêu thủ đoạn "bắt cóc online" và ba dấu hiệu giúp học sinh nhận biết.

3. Phân biệt "sử dụng nhiều" và "sử dụng có vấn đề" đối với trò chơi điện tử, mạng xã hội.

4. Vì sao giáo viên không nên phổ biến tên và cách thực hiện các "thử thách" nguy hiểm khi cảnh báo học sinh?

5. Mô tả các giai đoạn của quá trình dụ dỗ trực tuyến và dấu hiệu cảnh báo tương ứng.

CHUYÊN ĐỀ 3. GIÁO DỤC KỸ NĂNG TƯƠNG TÁC AN TOÀN TRÊN KHÔNG GIAN MẠNG CHO HỌC SINH

(Thời lượng: 150 phút)

MỤC TIÊU

Sau khi học xong chuyên đề này, thầy cô có thể:

– Nhận diện được mục tiêu, yêu cầu cần đạt về kỹ năng tương tác an toàn trên không gian mạng đối với học sinh từng cấp học.

– Trình bày được hệ thống kỹ năng thành phần và các nguyên tắc giáo dục kỹ năng an toàn trên không gian mạng.

– Lựa chọn và vận dụng được con đường, hình thức, phương pháp giáo dục phù hợp, đặc biệt là tích hợp trong môn học, HĐTN, HN và sinh hoạt lớp.

– Thiết kế và sử dụng được các công cụ đánh giá kết quả giáo dục hướng vào hành vi của học sinh.

KHỞI ĐỘNG

Hoạt động khởi động: "Biết" và "làm được" (10 phút)
Thầy cô suy nghĩ: Hầu hết học sinh đều "biết" không nên chia sẻ mật khẩu. Vậy vì sao vẫn có nhiều học sinh bị chiếm đoạt tài khoản? Viết một câu trả lời lên giấy nhớ và dán lên bảng.
Gợi ý: Khoảng cách giữa biết và làm do: tình huống thực tế phức tạp hơn (kẻ gian giả danh người quen, tạo áp lực thời gian); học sinh chưa được luyện tập phản ứng; cảm xúc lấn át lý trí; thói quen chưa được hình thành; môi trường không củng cố. Kết luận: giáo dục kỹ năng phải dựa trên trải nghiệm, luyện tập và củng cố, không dừng ở truyền đạt kiến thức.

NỘI DUNG

3.1. Mục tiêu và yêu cầu cần đạt theo cấp học

Mục tiêu giáo dục kỹ năng tương tác an toàn trên không gian mạng được xác định trên ba phương diện nhận thức, thái độ và hành vi, hướng tới năm nhóm kết quả: (1) sử dụng Internet và thiết bị số hợp lý, cân bằng; (2) nhận diện nguy cơ và tự bảo vệ; (3) đánh giá, khai thác và sử dụng thông tin hiệu quả, có trách nhiệm; (4) ứng phó với bắt nạt và các tình huống tiêu cực, biết tìm kiếm hỗ trợ; (5) giao tiếp, ứng xử văn minh, có trách nhiệm. Các mục tiêu này được cụ thể hóa theo

cấp học, phù hợp với tinh thần phát triển tăng dần của Khung năng lực số cho người học.

Nhóm yêu cầu	Tiểu học	THCS	THPT
Sử dụng hợp lý, cân bằng	Tuân thủ thời gian sử dụng do cha mẹ, thầy cô thỏa thuận; nhận biết khi mình dùng thiết bị quá lâu.	Tự theo dõi và điều chỉnh thời gian sử dụng; nhận biết một số cơ chế lôi kéo của game, mạng xã hội.	Tự lập kế hoạch cân bằng giữa học tập, nghỉ ngơi, đời sống số; phân tích được tác động của thiết kế nền tảng đến hành vi.
Bảo vệ thông tin cá nhân và tài khoản	Kể được những thông tin không được chia sẻ; không cho người khác biết mật khẩu, kể cả bạn thân.	Thiết lập mật khẩu mạnh, quyền riêng tư; bật xác thực hai yếu tố; nhận diện yêu cầu OTP là dấu hiệu lừa đảo.	Quản lý dấu chân số và hình ảnh cá nhân trực tuyến; hiểu quyền của chủ thể dữ liệu cá nhân theo pháp luật.
Nhận diện nguy cơ và tự bảo vệ	Phân biệt tình huống an toàn, cần cảnh giác, nguy hiểm; thực hiện "Dừng lại – Hỏi người lớn".	Nhận diện dấu hiệu lừa đảo, dụ dỗ, bắt nạt; thực hành từ chối, chặn, lưu bằng chứng, báo cáo.	Phân tích các thủ đoạn lừa đảo, thao túng tinh vi (giả danh cơ quan chức năng, việc làm online, deepfake); đánh giá rủi ro trước khi quyết định.
Đánh giá và sử dụng thông tin	Biết rằng không phải mọi điều trên mạng đều đúng; hỏi người lớn khi thấy thông tin lạ.	Kiểm tra nguồn, so sánh nhiều nguồn; phân biệt sự thật và ý kiến, quảng cáo.	Kiểm chứng thông tin bằng "đọc ngang"; nhận diện nội dung do AI tạo ra; sử dụng AI có trách nhiệm, trung thực trong học tập.

Nhóm yêu cầu	Tiểu học	THCS	THPT
Ứng phó và tìm kiếm hỗ trợ	Kể với người lớn tin cậy khi gặp điều khiến em sợ, khó chịu; biết tên ít nhất một người lớn có thể giúp.	Biết quy trình báo cáo trên nền tảng; biết các kênh hỗ trợ trong trường và Tổng đài 111 (Tổng đài Quốc gia Bảo vệ Trẻ em, Cục Bà mẹ và Trẻ em); hỗ trợ bạn bị bắt nạt.	Ứng phó với tình huống phức tạp (tống tiền, lừa đảo); biết quyền và nghĩa vụ pháp lý; tham gia hỗ trợ đồng đẳng.
Giao tiếp, ứng xử văn minh	Nói lời tử tế; xin phép trước khi đăng ảnh của bạn.	Kiểm soát cảm xúc khi giao tiếp trên mạng; không tham gia, không cổ vũ bắt nạt.	Tham gia xây dựng môi trường số tích cực; tôn trọng sự khác biệt; trách nhiệm pháp lý với nội dung tạo ra, chia sẻ.

Bảng 3.1. Yêu cầu cần đạt về kỹ năng tương tác an toàn trên không gian mạng theo cấp học

3.2. Hệ thống kỹ năng thành phần

Trên cơ sở tổng hợp nghiên cứu và yêu cầu của Khung năng lực số, kỹ năng tương tác an toàn trên không gian mạng của học sinh được cấu thành từ mười kỹ năng thành phần:

TT	Kỹ năng thành phần	Biểu hiện hành vi có thể quan sát
1	Bảo vệ thông tin cá nhân	Phân loại thông tin được/không được chia sẻ; thiết lập quyền riêng tư; không chia sẻ mật khẩu, OTP.

TT	Kỹ năng thành phần	Biểu hiện hành vi có thể quan sát
2	Bảo mật tài khoản và thiết bị	Tạo mật khẩu mạnh, khác nhau cho từng tài khoản; bật xác thực hai yếu tố; không cài ứng dụng không rõ nguồn gốc; khôi phục tài khoản khi bị xâm phạm.
3	Nhận diện và phòng tránh lừa đảo	Chỉ ra dấu hiệu lừa đảo trong tin nhắn, cuộc gọi, đường link; kiểm chứng qua kênh độc lập.
4	Đánh giá thông tin	Kiểm tra nguồn, đối chiếu nhiều nguồn; phân biệt sự thật, ý kiến, quảng cáo, nội dung giả mạo; dừng lại trước khi chia sẻ.
5	Giao tiếp văn minh	Sử dụng ngôn ngữ tôn trọng; kiểm soát cảm xúc; xin phép trước khi đăng nội dung liên quan đến người khác.
6	Tự kiểm soát việc sử dụng	Theo dõi, điều chỉnh thời gian sử dụng; nhận biết và chủ động thoát khỏi vòng lặp sử dụng.
7	Từ chối và thiết lập ranh giới	Nói "không" rõ ràng trước yêu cầu không an toàn; rời khỏi cuộc trò chuyện; không chịu áp lực "phải lịch sự".
8	Ứng phó với bắt nạt và quấy rối	Không đáp trả; lưu bằng chứng; chặn, báo cáo; hỗ trợ bạn với vai trò người chứng kiến tích cực.
9	Phòng tránh xâm hại trực tuyến	Nhận diện dấu hiệu dụ dỗ; không gửi hình ảnh nhạy cảm; xử lý đúng khi bị đe dọa.
10	Tìm kiếm hỗ trợ	Xác định người lớn tin cậy; biết các kênh hỗ trợ trong và ngoài nhà trường; mạnh dạn kể và nhờ giúp đỡ.

Bảng 3.2. Hệ thống kỹ năng thành phần và biểu hiện hành vi

Kỹ năng số 10 – tìm kiếm hỗ trợ – có vai trò đặc biệt, vì đây là "lưới an toàn" khi các kỹ năng khác chưa đủ để học sinh tự xử lý. Một chương trình giáo dục chỉ

dạy học sinh "tự bảo vệ" mà không xây dựng niềm tin để học sinh tìm đến người lớn là chưa đầy đủ.

3.3. Nguyên tắc giáo dục

Giáo dục kỹ năng tương tác an toàn trên không gian mạng cần tuân thủ các nguyên tắc sau:

Thứ nhất, nguyên tắc lấy học sinh làm trung tâm và tôn trọng quyền của học sinh. Học sinh vừa có quyền được bảo vệ, vừa có quyền tiếp cận thông tin, tham gia, vui chơi và có đời sống riêng tư. Giáo dục cần lắng nghe trải nghiệm thực tế của học sinh, xuất phát từ chính những tình huống các em gặp, tránh áp đặt quan điểm của người lớn.

Thứ hai, nguyên tắc trải nghiệm. Kỹ năng chỉ được hình thành khi học sinh được thực hành trong các tình huống cụ thể, được thử – sai – sửa trong môi trường an toàn. Hoạt động giáo dục cần ưu tiên đóng vai, xử lý tình huống, mô phỏng, dự án.

Thứ ba, nguyên tắc tương tác. Giáo dục cần tạo ra sự tương tác đa chiều giữa giáo viên với học sinh, giữa học sinh với học sinh và giữa nhà trường với gia đình. Đối thoại cởi mở là điều kiện để học sinh chia sẻ những vấn đề thực sự gặp phải.

Thứ tư, nguyên tắc tiến trình, liên tục và phù hợp lứa tuổi. Giáo dục được thực hiện thường xuyên, theo lộ trình từ đơn giản đến phức tạp xuyên suốt các cấp học, tránh tổ chức theo phong trào hoặc chỉ khi xảy ra sự cố.

Thứ năm, nguyên tắc hướng tới thay đổi hành vi. Mục tiêu là học sinh "làm được" và "duy trì được" hành vi an toàn; đánh giá cần dựa vào biểu hiện hành vi, không chỉ kiểm tra ghi nhớ.

Thứ sáu, nguyên tắc không gây sợ hãi, không đổ lỗi. Thông điệp giáo dục cần cân bằng giữa cơ hội và rủi ro, tránh phóng đại, tránh dùng hình ảnh, câu chuyện gây sốc; tuyệt đối không đổ lỗi cho nạn nhân. Giáo dục dựa trên sợ hãi có thể làm học sinh lo âu và không dám tiết lộ khi gặp sự cố.

Thứ bảy, nguyên tắc thống nhất giữa các lực lượng. Nhà trường, gia đình và xã hội cần thống nhất mục tiêu, thông điệp, quy tắc để học sinh nhận được tác động giáo dục nhất quán.

3.4. Con đường và hình thức giáo dục

3.4.1. Tích hợp trong các môn học

Chương trình GDPT 2018 tạo nhiều cơ hội tích hợp nội dung tương tác an toàn trên không gian mạng. Giáo viên căn cứ yêu cầu cần đạt của môn học để lồng ghép một cách tự nhiên, không làm quá tải bài học:

Môn học	**Cơ hội tích hợp tiêu biểu**
Tin học	Đạo đức, pháp luật và văn hóa trong môi trường mạng; bảo vệ thông tin, tài khoản; nhận diện phần mềm độc hại, lừa đảo; sử dụng công cụ AI có trách nhiệm.
Đạo đức (Tiểu học), Giáo dục công dân (THCS), Giáo dục kinh tế và pháp luật (THPT)	Quyền trẻ em, quyền riêng tư; tôn trọng người khác; phòng chống bạo lực; pháp luật về an ninh mạng, bảo vệ dữ liệu cá nhân, phòng chống tội phạm; quản lý tài chính cá nhân và phòng tránh lừa đảo.
Tiếng Việt, Ngữ văn	Đọc hiểu văn bản thông tin, nghị luận về vấn đề đời sống số; đánh giá độ tin cậy của thông tin; viết bài nghị luận về văn hóa ứng xử trên mạng.
Toán	Xác suất và tính "nhà cái luôn thắng" trong cờ bạc, loot box; phân tích số liệu thống kê về sử dụng Internet.
Khoa học, Sinh học	Giấc ngủ, sức khỏe và thiết bị số; dậy thì, sức khỏe sinh sản; tin giả về sức khỏe.
Lịch sử và Địa lí, Lịch sử	Nhận diện thông tin xuyên tạc, kiểm chứng nguồn sử liệu.
Ngoại ngữ	Chủ đề công nghệ, mạng xã hội, an toàn trực tuyến trong các bài đọc, thảo luận.

Bảng 3.3. Cơ hội tích hợp nội dung tương tác an toàn trên không gian mạng trong một số môn học

3.4.2. Hoạt động trải nghiệm, hướng nghiệp

HĐTN (Tiểu học) và HĐTN, HN (THCS, THPT) là con đường đặc biệt thuận lợi vì bản chất của hoạt động là học sinh trực tiếp trải nghiệm, huy động

kinh nghiệm, giải quyết vấn đề thực tiễn (Bộ Giáo dục và Đào tạo, 2018). Nội dung tương tác an toàn có thể gắn với các mạch nội dung:

– **Hoạt động hướng vào bản thân:** quản lý danh tính số, bảo vệ thông tin và hình ảnh cá nhân, quản lý cảm xúc, cân bằng thời gian sử dụng thiết bị.

– **Hoạt động hướng đến xã hội:** giao tiếp có trách nhiệm, phòng chống bắt nạt, xây dựng quy tắc lớp học số, hỗ trợ bạn bè.

– **Hoạt động hướng đến tự nhiên:** đánh giá thông tin về môi trường, thiên tai; nhận diện tin giả.

– **Hoạt động hướng nghiệp:** dấu chân số và hồ sơ trực tuyến; nhận diện lừa đảo tuyển dụng, "việc nhẹ lương cao"; nghề nghiệp trong lĩnh vực an toàn thông tin.

3.4.3. Sinh hoạt lớp, sinh hoạt theo quy mô lớp/khối/toàn trường

Tiết sinh hoạt lớp phù hợp với các hoạt động ngắn (10 – 15 phút): thảo luận một tình huống thời sự, rà soát quy tắc nhóm trực tuyến của lớp, chia sẻ "mẹo an toàn của tuần". Sinh hoạt dưới cờ phù hợp với truyền thông chủ đề, tiểu phẩm, giao lưu với chuyên gia, cán bộ công an.

3.4.4. Câu lạc bộ, ngày hội, hoạt động ngoại khóa

Các hình thức như câu lạc bộ "Công dân số", diễn đàn, hội thi, ngày hội an toàn số, dự án truyền thông do học sinh thực hiện giúp mở rộng không gian trải nghiệm và phát huy vai trò chủ động, sáng tạo của học sinh. Đặc biệt, mô hình nhóm hỗ trợ đồng đẳng – học sinh được tập huấn để lắng nghe bạn và kết nối bạn với người lớn – phù hợp với thực tế học sinh thường chia sẻ với bạn bè trước tiên.

3.5. Phương pháp và kỹ thuật giáo dục

3.5.1. Chu trình học tập trải nghiệm

Các hoạt động giáo dục kỹ năng nên được thiết kế theo chu trình học tập trải nghiệm của Kolb (1984), được cụ thể hóa thành bốn bước:

– **Bước 1 – Trải nghiệm:** học sinh tham gia một tình huống, trò chơi, mô phỏng hoặc chia sẻ trải nghiệm thực tế.

– **Bước 2 – Phản hồi, chia sẻ:** học sinh mô tả điều đã xảy ra, cảm xúc của bản thân, những lựa chọn đã đưa ra.

– **Bước 3 – Khái quát hóa:** học sinh rút ra dấu hiệu, nguyên tắc, quy tắc ứng xử; giáo viên chốt kiến thức.

– **Bước 4 – Vận dụng:** học sinh áp dụng vào tình huống mới, cam kết hành động, thực hiện nhiệm vụ tại nhà.

3.5.2. Các phương pháp, kỹ thuật chủ yếu

Phương pháp, kỹ thuật	Cách thực hiện	Lưu ý
Phân tích tình huống	Học sinh đọc, xem tình huống; xác định dấu hiệu nguy cơ, nguyên nhân, hậu quả; đề xuất cách xử lý và giải thích lựa chọn.	Tình huống gần gũi, phù hợp lứa tuổi; không sử dụng tình huống thật của học sinh trong lớp.
Đóng vai, mô phỏng	Học sinh đóng vai người nhận tin nhắn đáng ngờ, người chứng kiến, người hỗ trợ; luyện tập câu nói từ chối, cách báo cáo.	Không để học sinh đóng vai người bị xâm hại tình dục; tổ chức "thoát vai" sau hoạt động.
Thảo luận nhóm, kỹ thuật khăn trải bàn, mảnh ghép	Học sinh cùng xây dựng quy tắc, phân loại hành vi, thiết kế áp phích.	Bảo đảm mọi học sinh đều được tham gia.
Trò chơi giáo dục	Trò chơi "Đèn giao thông an toàn", "Thám tử mạng", ghép thẻ, câu đố, trò chơi trên nền tảng trực tuyến (Kahoot, Quizizz…).	Sau trò chơi phải có phần phản hồi, rút ra bài học; tránh biến thành cuộc thi thắng – thua.
Dạy học dựa trên dự án	Học sinh thực hiện sản phẩm: bộ quy tắc lớp, video, áp phích, cẩm nang, chiến dịch truyền thông.	Kiểm soát nguồn thông tin; không yêu cầu đăng sản phẩm công khai khi chưa có sự đồng ý.
Vấn đáp, đàm thoại gợi mở	Câu hỏi mở về trải nghiệm, cảm xúc, lựa chọn của học sinh.	Tạo bầu không khí không phán xét.
Thực hành trên thiết bị	Thực hành thiết lập quyền riêng tư, mật khẩu, xác thực hai yếu tố, báo cáo nội dung trên tài khoản mô phỏng.	Sử dụng tài khoản mô phỏng; bảo vệ dữ liệu thật của học sinh.

Bảng 3.4. Một số phương pháp, kỹ thuật giáo dục kỹ năng tương tác an toàn

3.5.3. Lưu ý khi giáo dục các chủ đề nhạy cảm

– Thông báo trước cho học sinh và cha mẹ học sinh về chủ đề; cho phép học sinh tạm rời hoạt động nếu thấy không thoải mái.

– Sử dụng tình huống "nhân vật thứ ba" để học sinh thảo luận mà không phải bộc lộ bản thân.

– Không sử dụng hình ảnh nhạy cảm, không mô tả chi tiết hành vi xâm hại, không nêu tên, mô tả các "thử thách" nguy hiểm cụ thể.

– Chuẩn bị sẵn phương án hỗ trợ: sau bài học về xâm hại, bắt nạt, có thể có học sinh tiết lộ; giáo viên cần biết quy trình tiếp nhận (Chuyên đề 4) và thông báo cho học sinh nơi tìm kiếm sự giúp đỡ.

3.6. Đánh giá kết quả giáo dục

3.6.1. Định hướng đánh giá

Đánh giá kết quả giáo dục kỹ năng tương tác an toàn cần chuyển trọng tâm từ kiến thức sang hành vi, thái độ; kết hợp đánh giá của giáo viên, tự đánh giá của học sinh, đánh giá đồng đẳng và thông tin từ cha mẹ; thực hiện ở nhiều thời điểm (trước, trong và sau hoạt động; sau một khoảng thời gian để đánh giá tính bền vững). Kết quả đánh giá chủ yếu dùng để phản hồi, điều chỉnh, ưu tiên nhận xét định tính, khích lệ.

3.6.2. Các công cụ đánh giá

Công cụ	Mục đích	Ví dụ
Bảng kiểm hành vi	Quan sát hành vi trong hoạt động thực hành, đóng vai.	Học sinh có từ chối lời mời kết bạn của người lạ trong tình huống mô phỏng không? Mật khẩu tạo ra có đủ độ mạnh không?
Bài tập tình huống	Đánh giá khả năng nhận diện rủi ro và lựa chọn cách ứng phó.	Đưa tình huống tống tiền giả định, yêu cầu học sinh sắp xếp các bước xử lý theo thứ tự ưu tiên và giải thích.

Công cụ	Mục đích	Ví dụ
Phiếu phản tư	Đánh giá thái độ, nhận thức, cảm xúc.	"Nếu gặp tình huống này, em sẽ làm gì? Em cảm thấy thế nào khi chia sẻ thông tin cá nhân?" (với học sinh lớp nhỏ dùng biểu tượng cảm xúc).
Rubric sản phẩm	Đánh giá sản phẩm dự án.	Tiêu chí: tính chính xác của thông điệp an toàn, tính rõ ràng, tính sáng tạo, tôn trọng quyền riêng tư.
Phiếu tự đánh giá	Học sinh tự nhận biết mức độ đạt được.	Các mức "Chưa rõ – Đã hiểu – Có thể thực hiện" đối với từng kỹ năng.
Phiếu ghi nhận của cha mẹ	Thu thập thông tin về hành vi tại nhà.	Con đã thiết lập quyền riêng tư cho tài khoản chưa? Con có tuân thủ thỏa thuận thời gian sử dụng không?

Bảng 3.5. Một số công cụ đánh giá kết quả giáo dục kỹ năng tương tác an toàn

3.6.3. Ví dụ rubric đánh giá kỹ năng ứng phó

Tiêu chí	Mức 1 – Chưa đạt	Mức 2 – Đạt	Mức 3 – Tốt
Nhận diện nguy cơ	Chưa nhận ra dấu hiệu bất thường.	Nhận ra một số dấu hiệu chính.	Nhận ra nhanh, đầy đủ dấu hiệu và giải thích được.
Lựa chọn cách ứng phó	Lựa chọn cách xử lý không an toàn (đáp trả, làm theo yêu cầu).	Lựa chọn được một số hành động an toàn.	Lựa chọn và sắp xếp hợp lý các hành động: dừng, chặn, lưu bằng chứng, báo cáo, kể với người lớn.

Tiêu chí	Mức 1 – Chưa đạt	Mức 2 – Đạt	Mức 3 – Tốt
Tìm kiếm hỗ trợ	Không xác định được người có thể giúp.	Xác định được người lớn tin cậy.	Xác định được nhiều nguồn hỗ trợ phù hợp với mức độ sự việc; sẵn sàng hỗ trợ bạn.

Bảng 3.6. Rubric đánh giá kỹ năng ứng phó với tình huống không an toàn trên mạng

HOẠT ĐỘNG TẬP HUẤN

Hoạt động 3.1. Trải nghiệm làm học sinh (30 phút)
Báo cáo viên tổ chức cho học viên tham gia trò chơi "Đèn giao thông an toàn" (Phụ lục 6) như học sinh, sau đó phân tích hoạt động theo bốn bước của chu trình học tập trải nghiệm.
Gợi ý: Học viên nhận ra vai trò của bước phản hồi và khái quát hóa: nếu chỉ chơi mà không thảo luận vì sao chọn "đỏ" hay "vàng", học sinh sẽ không hình thành được nguyên tắc để vận dụng sang tình huống mới.

Hoạt động 3.2. Thiết kế hoạt động tích hợp 15 phút (60 phút)
Nhóm thầy cô cùng môn học hoặc cùng cấp học chọn một bài học trong chương trình, thiết kế một hoạt động 15 phút tích hợp nội dung tương tác an toàn, gồm: mục tiêu (yêu cầu cần đạt); tình huống hoặc nhiệm vụ; cách tổ chức theo chu trình trải nghiệm; công cụ đánh giá. Các nhóm trình bày và góp ý chéo.
Gợi ý tiêu chí góp ý: (1) Tích hợp tự nhiên, không làm lệch mục tiêu bài học; (2) Học sinh được trải nghiệm, thực hành; (3) Thông điệp không gây sợ hãi, không đổ lỗi; (4) Có công cụ đánh giá hành vi; (5) Khả thi về thời gian, điều kiện.

GHI NHỚ

– Mục tiêu giáo dục được cụ thể hóa theo cấp học, phát triển tăng dần từ tiểu học đến THPT.

– Mười kỹ năng thành phần, trong đó kỹ năng tìm kiếm hỗ trợ là "lưới an toàn".

– Bảy nguyên tắc: lấy học sinh làm trung tâm, trải nghiệm, tương tác, tiến trình, hướng tới hành vi, không gây sợ hãi – không đổ lỗi, thống nhất các lực lượng.

– Tích hợp trong môn học, HĐTN, HN, sinh hoạt lớp là con đường chính; tổ chức theo chu trình trải nghiệm bốn bước.

– Đánh giá hướng vào hành vi, sử dụng nhiều công cụ, nhiều nguồn thông tin.

CÂU HỎI TỰ ĐÁNH GIÁ

1. Vì sao kỹ năng tìm kiếm hỗ trợ được coi là "lưới an toàn" trong hệ thống kỹ năng thành phần?

2. Trình bày bốn bước của chu trình học tập trải nghiệm và cho ví dụ áp dụng với chủ đề phòng tránh lừa đảo trực tuyến.

3. Nêu ba lưu ý khi tổ chức hoạt động giáo dục về chủ đề xâm hại tình dục trực tuyến.

4. Thiết kế một câu hỏi trong bảng kiểm hành vi để đánh giá kỹ năng bảo mật tài khoản của học sinh THCS.

CHUYÊN ĐỀ 4. PHÁT HIỆN, HỖ TRỢ VÀ XỬ LÝ BAN ĐẦU KHI HỌC SINH GẶP SỰ CỐ TRÊN KHÔNG GIAN MẠNG

(Thời lượng: 180 phút)

MỤC TIÊU

Sau khi học xong chuyên đề này, thầy cô có thể:

– Nhận diện được vai trò, phạm vi và giới hạn của giáo viên trong hỗ trợ học sinh gặp sự cố trên không gian mạng.

– Giải thích được các dấu hiệu cho thấy học sinh có thể đang gặp nguy cơ, sự cố hoặc khủng hoảng tâm lý.

– Tiếp nhận được chia sẻ, tiết lộ của học sinh một cách an toàn, tôn trọng; thực hiện được hỗ trợ tâm lý ban đầu.

– Vận dụng được quy trình xử lý chung và hướng dẫn xử lý đối với từng loại sự cố.

– Ghi chép, bảo mật thông tin và chuyển gửi đúng quy định; biết tự chăm sóc bản thân trong quá trình hỗ trợ học sinh.

KHỞI ĐỘNG

Hoạt động khởi động: "Người em sẽ kể" (10 phút)

Thầy cô nhớ lại thời học sinh: khi gặp chuyện khó khăn, thầy cô đã kể với ai? Vì sao chọn người đó? Điều gì ở người đó khiến thầy cô yên tâm? Điều gì khiến thầy cô không dám kể với người khác?

Gợi ý: Học viên thường nêu các phẩm chất: biết lắng nghe, không la mắng, không kể lại với người khác, không làm to chuyện, giúp được việc. Lý do không dám kể: sợ bị trách, sợ bị lan truyền, sợ người lớn phản ứng quá mức, sợ hậu quả. Kết luận: điều quyết định học sinh có tìm đến giáo viên hay không chính là cách giáo viên phản ứng ở lần đầu tiên.

NỘI DUNG

4.1. Vai trò, phạm vi và giới hạn của giáo viên

4.1.1. Vì sao giáo viên giữ vị trí then chốt?

Giáo viên tiếp xúc với học sinh hằng ngày, có cơ sở để so sánh hành vi hiện tại của học sinh với trước đó, quan sát học sinh trong các mối quan hệ bạn bè và thường là người lớn mà học sinh tin tưởng ngoài gia đình. Số liệu ở Chuyên đề 1 cho thấy phần lớn học sinh gặp rủi ro trực tuyến không kể với ai hoặc chỉ kể với

bạn bè. Vì vậy, sự nhạy bén và cách phản ứng phù hợp của giáo viên có thể tạo ra khác biệt quyết định đối với mức độ tổn hại mà học sinh phải chịu.

4.1.2. Vai trò của giáo viên trong xử lý sự cố

Giáo viên thực hiện năm vai trò: (1) phát hiện – nhận biết dấu hiệu bất thường; (2) tiếp nhận – lắng nghe, ghi nhận thông tin; (3) hỗ trợ ban đầu – giúp học sinh an toàn, bình tĩnh và cảm thấy được che chở; (4) báo cáo, kết nối – báo cáo đầu mối của nhà trường và kết nối học sinh với hỗ trợ chuyên sâu; (5) đồng hành, theo dõi – tiếp tục hỗ trợ học sinh trong môi trường học tập sau sự cố.

4.1.3. Giới hạn của giáo viên

Giáo viên **không** thay thế cơ quan điều tra, người làm công tác chuyên môn tâm lý hay cơ quan y tế. Cụ thể, giáo viên không tự điều tra, thẩm vấn, đối chất; không tự liên hệ, đàm phán với đối tượng đe dọa, lừa đảo; không tự quyết định "giải quyết nội bộ" đối với vụ việc có dấu hiệu vi phạm pháp luật; không chẩn đoán vấn đề sức khỏe tâm thần. Nhận thức rõ giới hạn giúp giáo viên không rơi vào tình trạng ôm đồm, gây tổn hại thêm cho học sinh hoặc làm mất chứng cứ.

4.1.4. Các nguyên tắc nền tảng

– Lợi ích tốt nhất của học sinh là ưu tiên hàng đầu trong mọi quyết định.

– An toàn trước tiên: khi học sinh đang gặp nguy hiểm trực tiếp (bị đe dọa tính mạng, có ý định tự gây hại, đang bị ép gặp mặt), ưu tiên bảo đảm an toàn ngay lập tức.

– Bảo mật có giới hạn: thông tin được giữ kín, chỉ chia sẻ với những người có trách nhiệm theo nguyên tắc "cần biết"; không hứa giữ bí mật tuyệt đối khi có nguy cơ đối với an toàn của học sinh.

– Không đổ lỗi, không kỳ thị; tiếp cận thấu hiểu sang chấn: nhận thức rằng hành vi của học sinh có thể là phản ứng với tổn thương, tránh làm học sinh bị tổn thương lặp lại (SAMHSA, 2014).

– Tôn trọng sự tham gia của học sinh: thông báo cho học sinh về các bước tiếp theo, lắng nghe mong muốn của học sinh trong phạm vi bảo đảm an toàn.

– Tuân thủ quy định: thực hiện theo quy trình của nhà trường, Thông tư 18/2025/TT-BGDĐT và quy định của pháp luật về bảo vệ trẻ em.

4.2. Nhận biết dấu hiệu học sinh gặp nguy cơ, sự cố

4.2.1. Các nhóm dấu hiệu

Không có dấu hiệu đơn lẻ nào khẳng định chắc chắn học sinh đang gặp sự cố. Giáo viên cần chú ý đến sự thay đổi so với trạng thái thường ngày, sự kết hợp của nhiều dấu hiệu và tính kéo dài của các dấu hiệu.

Nhóm dấu hiệu	**Biểu hiện cụ thể**
Cảm xúc	Lo âu, sợ hãi, căng thẳng; buồn bã, khóc; cáu gắt, bùng nổ; xấu hổ, tự trách; thờ ơ, mất hứng thú.
Hành vi	Thu mình, tách khỏi bạn bè; né tránh đến trường hoặc một số hoạt động, một số bạn; thay đổi đột ngột trong ăn mặc, ngoại hình; có hành vi gây hấn hoặc chống đối mới xuất hiện.
Sử dụng thiết bị	Giật mình, hoảng hốt khi có tin nhắn; giấu màn hình; đột ngột xóa tài khoản hoặc ngừng dùng mạng xã hội; dùng thiết bị đến khuya; có tài khoản, thiết bị, ứng dụng bí mật.
Học tập	Giảm tập trung, giảm sút kết quả học tập; ngủ gật trong lớp; nghỉ học không rõ lý do.
Tài chính, vật chất	Thường xuyên cần tiền, vay mượn, bán đồ dùng; có quà tặng, tiền, thẻ nạp không rõ nguồn gốc.
Quan hệ	Xuất hiện "người bạn" trên mạng được giấu kín; quan hệ với nhóm bạn mới, lớn tuổi hơn; căng thẳng rõ rệt với một nhóm bạn cụ thể.
Thể chất	Mất ngủ, ác mộng; đau đầu, đau bụng không rõ nguyên nhân; thay đổi thói quen ăn uống; có thương tích không giải thích được.

Bảng 4.1. Các nhóm dấu hiệu học sinh có thể đang gặp sự cố trên không gian mạng

4.2.2. Dấu hiệu khủng hoảng cần can thiệp khẩn cấp

Giáo viên cần hành động **ngay lập tức** (không để học sinh ở một mình, báo ngay Ban Giám hiệu và cha mẹ học sinh, kết nối với dịch vụ y tế) khi học sinh có một trong các biểu hiện sau:

– Nói, viết, đăng tải về ý định muốn chết, tự làm hại bản thân, cảm giác vô vọng, là gánh nặng; tìm kiếm cách thức tự gây hại.

– Có dấu hiệu tự gây thương tích.

– Chia tay, cho đi đồ vật quý giá, có lời nói mang tính "từ biệt".

– Đang bị đe dọa, ép buộc phải gặp mặt, phải rời khỏi nhà, phải chuyển tiền gấp; đang trong tình huống "bắt cóc online".

– Bị tống tiền tình dục và có biểu hiện hoảng loạn, tuyệt vọng.

Nghiên cứu cho thấy việc hỏi trực tiếp, bình tĩnh và quan tâm về ý nghĩ tự sát không làm tăng nguy cơ mà giúp người đang gặp khó khăn cảm thấy được thấu hiểu và mở ra cơ hội được giúp đỡ (WHO, 2014). Giáo viên có thể hỏi: "Thầy/cô thấy dạo này em rất buồn. Có lúc nào em nghĩ đến việc làm hại bản thân không?".

4.2.3. Các kênh phát hiện

Ngoài quan sát trực tiếp, giáo viên có thể nhận được thông tin qua: lời kể của bạn bè học sinh; phản ánh của cha mẹ; bài viết, bài vẽ, nhật ký học tập; nội dung trong nhóm trực tuyến của lớp; hộp thư góp ý hoặc kênh báo cáo ẩn danh của trường. Mọi thông tin đều cần được tiếp nhận nghiêm túc, kể cả khi chưa rõ ràng.

4.3. Tiếp nhận chia sẻ, tiết lộ của học sinh

4.3.1. Đặc điểm của việc tiết lộ

Học sinh hiếm khi kể toàn bộ sự việc ngay lần đầu. Việc tiết lộ thường diễn ra từng phần, có thể gián tiếp ("Em có một người bạn bị…"), có thể "thăm dò" phản ứng của người lớn, có thể bằng hành vi hoặc qua bài viết, bài vẽ. Học sinh có thể rút lại lời kể nếu nhận được phản ứng tiêu cực. Những rào cản thường gặp: xấu hổ, tự trách; sợ bị phạt, bị tịch thu điện thoại; sợ bị lan truyền; sợ bị trả thù; bị đối tượng đe dọa; không tin người lớn có thể giúp.

4.3.2. Các bước tiếp nhận

Bước 1. Giữ bình tĩnh và tạo không gian an toàn. Kiểm soát biểu hiện sốc, tức giận, hoảng hốt. Đưa học sinh đến nơi riêng tư nhưng không khép kín hoàn toàn (ví dụ phòng có cửa kính, phòng tư vấn); ngồi ngang tầm, giữ khoảng cách phù hợp.

Bước 2. Lắng nghe tích cực. Để học sinh kể theo cách của mình; không ngắt lời, không thúc ép. Thể hiện sự chú ý bằng ánh mắt, gật đầu, lời phản hồi ngắn.

Bước 3. Hỏi vừa đủ bằng câu hỏi mở, không dẫn dắt. Mục đích chỉ là nắm đủ thông tin để bảo đảm an toàn và quyết định bước tiếp theo, không phải điều tra chi tiết. Ví dụ: "Em có thể kể thêm cho thầy/cô được không?", "Chuyện đó xảy

ra như thế nào?", "Bây giờ em có đang an toàn không?". Tránh câu hỏi gợi ý câu trả lời như "Có phải anh A làm vậy không?".

Bước 4. Ghi nhận và trấn an. Ghi nhận sự can đảm của học sinh; khẳng định đó không phải lỗi của em; khẳng định thầy cô tin em và sẽ giúp em.

Bước 5. Giải thích trung thực về các bước tiếp theo. Cho học sinh biết thầy cô cần báo với ai, vì sao và điều gì sẽ diễn ra; hỏi ý kiến của học sinh về những điều em lo lắng.

Bước 6. Ghi chép ngay sau buổi trao đổi (xem mục 4.7) và báo cáo theo quy trình.

4.3.3. Những câu nên nói và không nên nói

Nên nói	**Không nên nói**
"Cảm ơn em đã tin tưởng kể cho thầy/cô."	"Sao bây giờ em mới nói?"
"Đây không phải lỗi của em."	"Sao em lại dại thế, ai bảo em gửi ảnh?"
"Thầy/cô tin em."	"Em có chắc không? Có khi em hiểu nhầm."
"Em đã làm đúng khi kể ra."	"Chuyện này nhỏ thôi, em đừng nghĩ nhiều."
"Thầy/cô cần báo với cô Hiệu trưởng/cô tư vấn để giúp em an toàn. Thầy/cô sẽ cho em biết từng bước."	"Thầy/cô hứa sẽ không nói với ai."
"Bây giờ điều gì khiến em lo lắng nhất?"	"Đưa điện thoại đây thầy/cô xem hết tin nhắn."
"Em không phải đối mặt chuyện này một mình."	"Bố mẹ em mà biết thì…"

Bảng 4.2. Ngôn ngữ phù hợp và không phù hợp khi tiếp nhận chia sẻ của học sinh

4.3.4. Trường hợp học sinh yêu cầu giữ bí mật

Giáo viên cần trung thực: "Thầy/cô hiểu em lo lắng. Thầy/cô sẽ chỉ chia sẻ với những người cần biết để giúp em an toàn và sẽ bàn với em trước khi làm gì tiếp theo." Nếu sự việc không liên quan đến an toàn, pháp luật (ví dụ học sinh

buồn vì một bình luận tiêu cực đơn lẻ, đã được giải quyết), giáo viên có thể tôn trọng mong muốn của học sinh và tiếp tục theo dõi, hỗ trợ.

4.4. Hỗ trợ tâm lý ban đầu

Hỗ trợ tâm lý ban đầu là sự hỗ trợ nhân văn, thiết thực dành cho người vừa trải qua sự kiện gây căng thẳng nghiêm trọng; không phải là trị liệu tâm lý chuyên sâu và có thể được thực hiện bởi người không phải chuyên gia sau khi được tập huấn (WHO, War Trauma Foundation & World Vision International, 2011). Hỗ trợ tâm lý ban đầu được thực hiện theo ba nguyên tắc hành động:

– **Quan sát:** kiểm tra an toàn của học sinh; nhận diện học sinh có nhu cầu cơ bản khẩn cấp hoặc phản ứng căng thẳng nghiêm trọng (hoảng loạn, không định hướng được, có ý định tự gây hại).

– **Lắng nghe:** tiếp cận nhẹ nhàng; hỏi về nhu cầu và mối lo lắng; lắng nghe và giúp học sinh bình tĩnh (hướng dẫn thở chậm, tập trung vào hiện tại, đưa nước uống).

– **Kết nối:** giúp học sinh đáp ứng nhu cầu cơ bản và giải quyết vấn đề trước mắt; kết nối với người thân, người làm công tác tư vấn học đường, dịch vụ hỗ trợ; cung cấp thông tin chính xác.

Một số việc cụ thể giáo viên có thể làm ngay: giúp học sinh xác định một người lớn trong gia đình có thể hỗ trợ; cùng học sinh thực hiện các bước bảo đảm an toàn trực tuyến (tạm thời rời khỏi nền tảng, nhờ người lớn quản lý tài khoản); thống nhất với học sinh cách liên lạc khi em cần; thông báo cho giáo viên bộ môn liên quan để giảm áp lực học tập trong thời gian ngắn (không tiết lộ chi tiết sự việc).

4.5. Quy trình xử lý chung

4.5.1. Phân loại mức độ sự việc

Mức độ	**Đặc điểm**	**Ví dụ**	**Hướng xử lý**
Mức 1 – XANH (Thấp)	Rủi ro chưa gây tổn hại đáng kể; học sinh an toàn; có thể giải quyết bằng biện pháp giáo dục.	Nhận lời mời kết bạn đáng ngờ nhưng chưa tương tác; một bình luận khiếm nhã đơn lẻ; vô tình xem nội dung không phù hợp.	GVCN hỗ trợ, hướng dẫn học sinh; thông tin cho cha mẹ khi cần; theo dõi.

Mức độ	Đặc điểm	Ví dụ	Hướng xử lý
Mức 2 – VÀNG (Trung bình)	Đã có tổn hại về tâm lý, tài sản, danh dự nhưng không nguy hiểm tức thời; cần phối hợp nhiều bên.	Bắt nạt trực tuyến lặp lại; mất tài khoản; bị lừa mất tiền; ảnh cá nhân (không nhạy cảm) bị phát tán; sử dụng thiết bị quá mức ảnh hưởng học tập.	Báo cáo đầu mối nhà trường; phối hợp cha mẹ học sinh, người làm tư vấn học đường; hướng dẫn báo cáo nền tảng, trình báo công an khi có thiệt hại tài sản.
Mức 3 – ĐỎ (Nghiêm trọng, khẩn cấp)	Nguy hiểm tức thời đến tính mạng, sức khỏe; có dấu hiệu tội phạm.	Ý định tự sát; tống tiền tình dục; hình ảnh nhạy cảm bị phát tán; dụ dỗ gặp mặt; "bắt cóc online"; bị đe dọa bạo lực.	Bảo đảm an toàn ngay; báo ngay Ban Giám hiệu và cha mẹ; báo cơ quan công an (113), Tổng đài 111 (Tổng đài Quốc gia Bảo vệ Trẻ em, Cục Bà mẹ và Trẻ em), cơ sở y tế; không để học sinh một mình.

Bảng 4.3. Phân loại mức độ sự việc và hướng xử lý

4.5.2. Các bước xử lý

Bước 1. Tiếp nhận thông tin. Tiếp nhận theo hướng dẫn ở mục 4.3; xác định sơ bộ mức độ sự việc.

Bước 2. Bảo đảm an toàn tức thời. Đối với mức 3: không để học sinh ở một mình; ngăn chặn nguy hiểm trước mắt (học sinh không đến điểm hẹn, không chuyển tiền, không gửi thêm hình ảnh); gọi hỗ trợ khẩn cấp khi cần.

Bước 3. Hướng dẫn bảo toàn chứng cứ. Hướng dẫn học sinh (hoặc cha mẹ học sinh) không xóa tin nhắn, tài khoản; chụp màn hình thể hiện tên tài khoản, đường dẫn trang, thời gian; ghi lại số điện thoại, số tài khoản ngân hàng của đối tượng. **Riêng đối với hình ảnh nhạy cảm của học sinh: giáo viên không xem, không lưu, không chuyển tiếp; chỉ ghi nhận thông tin mô tả và để cơ quan chức năng xử lý.**

Quy trình bảo toàn chứng cứ gián tiếp (Metadata/UID):
Giáo viên hướng dẫn học sinh hoặc cha mẹ học sinh tự thao tác:

Đối với tài khoản đối tượng đe dọa: Chụp màn hình trang cá nhân của đối tượng kèm theo đường dẫn URL đầy đủ hoặc mã ID cố định (Numeric UID) của tài khoản đối tượng (tránh chỉ chụp tên hiển thị vì đối tượng có thể đổi tên trong vài giây).

Đối với tin nhắn đe dọa: Chụp màn hình các đoạn chat thể hiện hành vi tống tiền, ép buộc, câu chữ đe dọa (không cần mở to hay chụp cận cảnh các tệp tin hình ảnh nhạy cảm).

Đối với hình ảnh nhạy cảm: Hướng dẫn cha mẹ học sinh/học sinh giữ nguyên dữ liệu gốc trên thiết bị cá nhân, sử dụng tính năng che/mờ (blur) vùng nhạy cảm nếu bắt buộc phải lập hồ sơ mô tả ban đầu, và chỉ bàn giao thiết bị chứa dữ liệu gốc trực tiếp cho cơ quan có thẩm quyền.

Bước 4. Báo cáo trong nhà trường. Báo cáo ngay cho người được phân công làm đầu mối (Phó Hiệu trưởng phụ trách công tác học sinh, người làm công tác tư vấn học đường). Đối với mức 3, báo cáo trực tiếp Hiệu trưởng.

Bước 5. Thông tin và phối hợp với cha mẹ học sinh. Nhà trường thông báo cho cha mẹ học sinh trong thời gian sớm nhất, trừ trường hợp có căn cứ cho rằng người gây hại là thành viên gia đình (khi đó báo ngay cơ quan chức năng, Tổng đài 111 – Tổng đài Quốc gia Bảo vệ Trẻ em, Cục Bà mẹ và Trẻ em). Hướng dẫn cha mẹ cách hỗ trợ con (xem Chuyên đề 5).

Bước 6. Chuyển tiếp hỗ trợ. Kết nối học sinh với dịch vụ phù hợp: tư vấn học đường; cơ sở y tế, chuyên gia sức khỏe tâm thần; cơ quan công an; Tổng đài Quốc gia Bảo vệ Trẻ em 111 (Tổng đài Quốc gia Bảo vệ Trẻ em, Cục Bà mẹ và Trẻ em); báo cáo vi phạm tới nền tảng số.

Bước 7. Hỗ trợ, theo dõi và phòng ngừa tái diễn. Lập kế hoạch hỗ trợ cá nhân (tâm lý, học tập, an toàn trực tuyến); theo dõi định kỳ; xử lý giáo dục đối với học sinh có hành vi gây hại (nếu là học sinh trong trường); rút kinh nghiệm, điều chỉnh hoạt động giáo dục phòng ngừa.

SƠ ĐỒ QUY TRÌNH XỬ LÝ SỰ CỐ TRỰC TUYẾN CỦA HỌC SINH



Sơ đồ 4.1. Quy trình xử lý sự cố trực tuyến của học sinh

4.6. Hướng dẫn xử lý theo từng loại sự cố

Các "thẻ hành động" dưới đây cụ thể hóa quy trình chung đối với từng loại sự cố thường gặp.

4.6.1. Bắt nạt trực tuyến

– **Hướng dẫn học sinh:** không đáp trả; lưu bằng chứng; chặn tài khoản; báo cáo nội dung trên nền tảng; điều chỉnh quyền riêng tư.

– **Giáo viên:** ghi nhận cảm xúc của học sinh; xác định mức độ (tần suất, quy mô lan truyền, có đe dọa hay không, có liên quan bắt nạt trực tiếp hay không); báo cáo đầu mối nhà trường.

– **Nhà trường:** yêu cầu gỡ bỏ nội dung nếu người đăng là học sinh trong trường; làm việc với học sinh có hành vi bắt nạt theo hướng giáo dục, phục hồi (nhận thức tác hại, sửa chữa, xin lỗi khi nạn nhân sẵn sàng); làm việc với học sinh chứng kiến; xử lý theo Nghị định 80/2017/NĐ-CP và Thông tư 19/2025/TT-BGDĐT.

– **Lưu ý:** không tổ chức cho nạn nhân và người bắt nạt đối mặt khi nạn nhân chưa sẵn sàng; không công khai xử lý trước tập thể làm nạn nhân bị chú ý thêm.

4.6.2. Lừa đảo, mất tài khoản, mất tiền

– **Ngay lập tức:** nếu tình huống đang diễn ra – dừng mọi giao dịch, ngắt liên lạc với đối tượng; liên hệ trực tiếp cha mẹ học sinh qua số điện thoại đã biết.

– **Tài khoản bị chiếm đoạt:** đổi mật khẩu các tài khoản liên quan (bắt đầu từ email, số điện thoại); sử dụng chức năng khôi phục của nền tảng; thông báo cho bạn bè, người thân không chuyển tiền theo tin nhắn từ tài khoản bị chiếm. Học sinh và cha mẹ học sinh có thể thực hiện theo các bước kỹ thuật cốt lõi sau đây:

Bước 1: Báo cha mẹ, thầy cô để tình hình được kiểm soát.

Bước 2: Thu hồi tất cả các phiên đăng nhập đang hoạt động (Revoke Active Sessions); bảo vệ email, số điện thoại và đổi mật khẩu.

Bước 3: Chọn tính năng "Đăng xuất khỏi tất cả các thiết bị khác" sau khi đổi mật khẩu để vô hiệu hóa Cookie/Token của kẻ gian.

Bước 4: Gỡ ứng dụng lạ khỏi thiết bị đang sử dụng.

Bước 5: Bật xác thực 2 lớp và báo nền tảng.

Bước 6: Chia sẻ thông tin cho bạn bè và người dùng khác.

– **Mất tiền:** cha mẹ học sinh liên hệ ngay với ngân hàng, ví điện tử để yêu cầu phong tỏa; trình báo cơ quan công an nơi cư trú kèm chứng cứ.

– **"Bắt cóc online":** giữ liên lạc với học sinh, không để học sinh tiếp tục làm theo yêu cầu; báo ngay cơ quan công an (113); xác minh vị trí của học sinh với gia đình.

– **Lưu ý:** không trách mắng học sinh; nhấn mạnh rằng các thủ đoạn lừa đảo được thiết kế để lừa cả người lớn có kinh nghiệm.

4.6.3. Lộ lọt thông tin cá nhân, hình ảnh bị phát tán (không mang tính nhạy cảm tình dục)

– Xác định nội dung bị phát tán, nơi phát tán, người phát tán (nếu biết).

– Hướng dẫn học sinh và cha mẹ sử dụng chức năng báo cáo vi phạm quyền riêng tư của nền tảng; yêu cầu gỡ bỏ nội dung; nếu người phát tán là học sinh trong trường, nhà trường yêu cầu gỡ bỏ và giáo dục.

– Rà soát, siết chặt quyền riêng tư các tài khoản của học sinh.

– Khi có dấu hiệu bị quấy rối, đe dọa từ việc lộ thông tin (địa chỉ, số điện thoại), báo cơ quan công an.

4.6.4. Dụ dỗ, xâm hại, tống tiền tình dục trực tuyến (mức 3 – ĐỎ)

– **Thông điệp cho học sinh:** "Em không có lỗi. Em đã làm đúng khi kể. Em không phải đối mặt chuyện này một mình."

– **Ngăn chặn tổn hại tiếp diễn:** học sinh không gửi thêm hình ảnh, không chuyển tiền (việc đáp ứng thường làm đối tượng đòi hỏi nhiều hơn), không gặp mặt; tạm ngừng trả lời nhưng **không xóa** tài khoản, tin nhắn.

– **Bảo toàn chứng cứ:** ghi nhận tên tài khoản, đường dẫn, thời gian; **giáo viên tuyệt đối không xem, lưu, chuyển tiếp hình ảnh nhạy cảm của học sinh**.

– **Báo cáo:** báo ngay Hiệu trưởng; nhà trường thông báo cho cha mẹ học sinh (trừ trường hợp nghi người gây hại là người trong gia đình); báo cơ quan công an; liên hệ Tổng đài 111 (Tổng đài Quốc gia Bảo vệ Trẻ em, Cục Bà mẹ và Trẻ em) để được tư vấn, kết nối dịch vụ.

– **Hỗ trợ tâm lý:** đánh giá nguy cơ tự gây hại (tống tiền tình dục là tình huống có nguy cơ khủng hoảng cao); kết nối người làm công tác tư vấn học đường, chuyên gia tâm lý.

– **Bảo mật tuyệt đối danh tính học sinh** trong và ngoài nhà trường.

4.6.5. Nội dung giả mạo do AI tạo ra (deepfake)

– Khẳng định với học sinh: nội dung là giả mạo, học sinh là nạn nhân.

– Bảo toàn chứng cứ (ghi nhận đường dẫn, tài khoản, thời gian); báo cáo nền tảng để gỡ bỏ.

– Nếu nội dung mang tính tình dục: xử lý như mục 4.6.4.

– Nếu người tạo ra nội dung là học sinh trong trường: nhà trường xử lý theo quy định, kết hợp giáo dục về đạo đức, pháp luật; thông tin cho cha mẹ các bên.

– Hỗ trợ học sinh đối mặt với sự chú ý của bạn bè; GVCN định hướng tập thể lớp không chia sẻ, không bàn tán.

4.6.6. Khủng hoảng tâm lý, ý định tự gây hại (mức 3 – ĐỎ)

– Không để học sinh ở một mình; đưa học sinh đến nơi an toàn, có người lớn ở cùng.

– Lắng nghe, thể hiện sự quan tâm; hỏi trực tiếp, bình tĩnh về ý định tự gây hại; không phán xét, không tranh luận, không hứa giữ bí mật.

– Báo ngay Ban Giám hiệu, người làm công tác tư vấn học đường và cha mẹ học sinh; khi có nguy cơ tức thời, gọi cấp cứu 115 hoặc đưa đến cơ sở y tế gần nhất.

– Phối hợp với gia đình hạn chế khả năng tiếp cận phương tiện có thể gây hại.

– Theo dõi sát sau khủng hoảng; phối hợp với cơ sở y tế, chuyên gia sức khỏe tâm thần.

– Khi trao đổi về sự việc trong tập thể, tuân thủ nguyên tắc truyền thông an toàn: không mô tả phương thức, không lan truyền hình ảnh, thông tin chi tiết.

4.6.7. Sử dụng thiết bị số quá mức

– Trao đổi riêng với học sinh, tìm hiểu nguyên nhân (giải trí, trốn tránh căng thẳng, áp lực bạn bè, cô đơn); tránh quy kết, dán nhãn "nghiện".

– Cùng học sinh đặt mục tiêu điều chỉnh từng bước, có thể đo lường; ghi nhận tiến bộ.

– Phối hợp với cha mẹ học sinh xây dựng thỏa thuận sử dụng thiết bị tại gia đình; tăng cường hoạt động thay thế.

– Khi có dấu hiệu suy giảm chức năng nghiêm trọng, kéo dài, kết hợp với các vấn đề tâm lý: tư vấn gia đình đưa học sinh đến cơ sở y tế có chuyên khoa tâm thần, tâm lý.

4.7. Ghi chép và bảo mật hồ sơ vụ việc

Mọi vụ việc từ mức 2 trở lên cần được ghi chép theo mẫu "Phiếu ghi nhận sự việc" (Phụ lục 2). Nội dung ghi chép gồm: thời gian, địa điểm tiếp nhận; người tiếp nhận; cách thức phát hiện; mô tả sự việc **theo đúng lời kể của học sinh** (ghi nguyên văn những câu quan trọng); những quan sát của giáo viên về trạng thái của học sinh; những việc đã làm; người đã được báo cáo, thời điểm báo cáo; chữ ký, ngày ghi chép.

Yêu cầu: ghi chép khách quan, phân biệt rõ sự kiện với nhận định của người ghi; không ghi suy đoán; lưu giữ ở nơi an toàn, chỉ người có trách nhiệm được tiếp cận; tuân thủ quy định về bảo vệ dữ liệu cá nhân của học sinh.

4.8. Đầu mối hỗ trợ

Đầu mối	**Khi nào liên hệ**
Ban Giám hiệu, người làm công tác tư vấn học đường của nhà trường	Mọi sự việc từ mức 2 trở lên; khi giáo viên cần hướng dẫn.
Tổng đài Quốc gia Bảo vệ Trẻ em, Cục Bà mẹ và Trẻ em (111 – miễn phí, 24/7)	Tư vấn, tiếp nhận thông tin về trẻ em bị xâm hại, bạo lực, bóc lột, có nguy cơ; kết nối dịch vụ bảo vệ trẻ em.
Cảnh sát 113; cơ quan công an xã, phường nơi cư trú	Sự việc có dấu hiệu tội phạm: tống tiền, xâm hại, lừa đảo chiếm đoạt tài sản, đe dọa, "bắt cóc online".
Cấp cứu 115; cơ sở y tế	Nguy cơ tự gây hại, tổn thương thể chất, khủng hoảng tâm lý cấp tính.
Chức năng báo cáo của nền tảng (Facebook, TikTok, Zalo, YouTube, nền tảng trò chơi…)	Yêu cầu gỡ bỏ nội dung vi phạm, khóa tài khoản giả mạo, khôi phục tài khoản.
Ngân hàng, ví điện tử	Yêu cầu phong tỏa giao dịch khi bị lừa chuyển tiền.

Bảng 4.4. Đầu mối hỗ trợ (nhà trường cần bổ sung số điện thoại cụ thể của địa phương vào Phụ lục 4)

4.9. Giáo viên tự chăm sóc bản thân

Hỗ trợ học sinh trong các sự việc nghiêm trọng có thể gây căng thẳng, cảm giác bất lực hoặc "sang chấn thứ cấp" ở giáo viên. Giáo viên cần: nhận biết dấu hiệu căng thẳng của bản thân (mất ngủ, ám ảnh về sự việc, cáu gắt, kiệt sức); chia sẻ với đồng nghiệp, người làm công tác tư vấn học đường trong phạm vi bảo mật; không một mình gánh vác vụ việc; duy trì ranh giới giữa công việc và đời sống cá nhân. Nhà trường cần có cơ chế hỗ trợ, ghi nhận và phân công hợp lý đối với giáo viên tham gia xử lý sự việc.

HOẠT ĐỘNG TẬP HUẤN

Hoạt động 4.1. Đóng vai tiếp nhận tiết lộ (40 phút)

Học viên làm việc theo nhóm ba người: một người đóng vai học sinh, một người đóng vai giáo viên, một người quan sát (sử dụng bảng 4.2 để nhận xét). Luân phiên đổi vai với ba tình huống:

a) Học sinh lớp 5 nói: "Cô ơi, có người trên game bảo con gửi ảnh thì cho con kim cương, con lỡ gửi rồi…"

b) Học sinh lớp 8 nói vòng vo: "Thầy ơi, nếu có một bạn bị người ta dọa đăng ảnh lên mạng thì bạn ấy có bị kỷ luật không ạ?"

c) Học sinh lớp 11 xin: "Cô hứa không nói với ai thì em mới kể."

Gợi ý: (a) Bình tĩnh, cảm ơn em đã kể, khẳng định không phải lỗi của em; hỏi em có còn liên lạc với người đó không, người đó có đe dọa gì không; không yêu cầu xem ảnh; giải thích cô sẽ báo cô Hiệu trưởng và bố mẹ để giúp em; xử lý theo mục 4.6.4. (b) Nhận ra đây có thể là tiết lộ gián tiếp; trả lời rõ: "Bạn ấy là người bị hại, bạn ấy không bị kỷ luật, và thầy có thể giúp bạn ấy"; mời học sinh kể thêm hoặc giới thiệu bạn đến gặp thầy. (c) Không hứa giữ bí mật tuyệt đối; trả lời trung thực như mục 4.3.4.

Hoạt động 4.2. Phân loại mức độ và lập kế hoạch xử lý (50 phút)

Mỗi nhóm nhận hai tình huống, xác định mức độ (xanh/vàng/đỏ), lập kế hoạch xử lý theo 7 bước, ghi rõ ai làm gì, khi nào:

Tình huống 1: Một học sinh lớp 10 bị nhóm bạn lập trang "confession" đăng ảnh chế và bình luận về ngoại hình, bài đăng có hàng trăm lượt chia sẻ. Học sinh xin nghỉ học ba ngày.

Tình huống 2: Mẹ của một học sinh lớp 7 gọi điện cho GVCN lúc 21 giờ, hoảng hốt cho biết con nhận được cuộc gọi của "công an" nói con liên quan đến đường dây ma túy, yêu cầu con đi đến một nhà nghỉ và không được nói với ai; hiện không liên lạc được với con.

Tình huống 3: GVCN phát hiện bài đăng trên mạng xã hội của một học sinh lớp 9 với nội dung "mệt mỏi quá, muốn biến mất mãi mãi".

Gợi ý: Tình huống 1 – mức vàng, có thể chuyển đỏ nếu học sinh có dấu hiệu khủng hoảng; GVCN liên hệ, hỗ trợ học sinh và gia đình, báo đầu mối nhà trường; yêu cầu gỡ trang, báo cáo nền tảng; làm việc với nhóm học sinh liên

quan; theo dõi tâm lý học sinh. Tình huống 2 – mức đỏ ("bắt cóc online"); hướng dẫn cha mẹ học sinh gọi ngay 113, báo công an nơi cư trú; tiếp tục liên lạc với học sinh qua mọi kênh, nhắn tin khẳng định đây là lừa đảo; không chuyển tiền; báo Ban Giám hiệu. Tình huống 3 – mức đỏ cho đến khi được đánh giá; liên hệ ngay với học sinh và gia đình, không trì hoãn; hỏi trực tiếp về ý định tự gây hại; báo Ban Giám hiệu, người làm tư vấn học đường; kết nối dịch vụ y tế khi cần.

GHI NHỚ

– Giáo viên phát hiện, tiếp nhận, hỗ trợ ban đầu, báo cáo, kết nối và theo dõi; giáo viên không điều tra, không đàm phán với đối tượng, không chẩn đoán.

– Phản ứng đầu tiên của giáo viên quyết định việc học sinh có tiếp tục tìm kiếm sự giúp đỡ hay không: bình tĩnh, lắng nghe, tin tưởng, không đổ lỗi.

– Không hứa giữ bí mật tuyệt đối; giải thích trung thực các bước tiếp theo.

– Phân loại mức độ xanh – vàng – đỏ; mức đỏ: bảo đảm an toàn ngay, không để học sinh một mình, báo ngay.

– Không xem, không lưu, không chuyển tiếp hình ảnh nhạy cảm của học sinh.

– Ghi chép khách quan, bảo mật; tự chăm sóc bản thân.

CÂU HỎI TỰ ĐÁNH GIÁ

1. Nêu năm vai trò của giáo viên trong xử lý sự cố trực tuyến và những việc nằm ngoài phạm vi của giáo viên.

2. Vì sao giáo viên không nên hứa giữ bí mật tuyệt đối với học sinh? Thầy cô sẽ trả lời thế nào khi học sinh yêu cầu?

3. Trình bày ba nguyên tắc hành động của hỗ trợ tâm lý ban đầu.

4. Khi học sinh bị tống tiền tình dục, giáo viên cần hướng dẫn học sinh làm gì và không làm gì?

5. Trình bày bảy bước của quy trình xử lý chung.

CHUYÊN ĐỀ 5. PHỐI HỢP VỚI CHA MẸ HỌC SINH VÀ CÁC LỰC LƯỢNG TRONG HỖ TRỢ HỌC SINH TƯƠNG TÁC AN TOÀN TRÊN KHÔNG GIAN MẠNG

(Thời lượng: 90 phút)

MỤC TIÊU

Sau khi học xong chuyên đề này, thầy cô có thể:

– Phân tích được vai trò của nhà trường, gia đình và các lực lượng xã hội; nội dung và nguyên tắc phối hợp.

– Tổ chức được các hoạt động phối hợp với cha mẹ học sinh trong giáo dục phòng ngừa và khi xảy ra sự cố.

– Phân loại được cách thức phối hợp với cơ quan công an, y tế, chính quyền, Đoàn, Đội và nền tảng số.

– Đề xuất được biện pháp xây dựng môi trường mạng an toàn trong nhà trường.

KHỞI ĐỘNG

Hoạt động khởi động: "Một thông điệp, nhiều cách nói" (10 phút)

Thầy cô liệt kê những điều cha mẹ học sinh lớp mình thường nói với con về điện thoại, mạng xã hội. So sánh với những điều nhà trường dạy học sinh. Có điểm nào mâu thuẫn không?

Gợi ý: Mâu thuẫn thường gặp: nhà trường dạy "hãy kể với người lớn khi gặp sự cố", nhưng cha mẹ phản ứng bằng cách tịch thu điện thoại khiến học sinh không dám kể; nhà trường yêu cầu không dùng thiết bị khuya, nhưng gia đình không có quy tắc. Kết luận: thiếu thống nhất làm giảm hiệu quả giáo dục; phối hợp là điều kiện bắt buộc.

NỘI DUNG

5.1. Vai trò của các lực lượng

Giáo dục và hỗ trợ học sinh tương tác an toàn trên không gian mạng là quá trình mang tính xã hội. Lý thuyết hệ sinh thái phát triển của Bronfenbrenner (1979) chỉ ra rằng sự phát triển của cá nhân chịu tác động của nhiều hệ thống môi trường đan xen; trong đó mối quan hệ giữa gia đình và nhà trường (hệ thống trung gian) có ảnh hưởng đặc biệt quan trọng. Mô hình hợp tác nhà trường – gia đình – cộng đồng của Epstein (2011) khẳng định sự tham gia có tổ chức của gia đình và cộng đồng nâng cao rõ rệt hiệu quả giáo dục học sinh.

Trong lĩnh vực này, mỗi lực lượng có vị trí riêng, không thể thay thế nhau:

– **Nhà trường giữ vai trò chủ đạo, điều phối:** xây dựng kế hoạch giáo dục có hệ thống; tổ chức giáo dục qua môn học, HĐTN, HN; tiếp nhận, xử lý sự cố; kết nối các lực lượng; đánh giá kết quả. Tuy nhiên, phần lớn hoạt động trực tuyến của học sinh diễn ra ngoài giờ học và ngoài phạm vi nhà trường.

– **Gia đình giữ vai trò nền tảng, trực tiếp:** quản lý thiết bị, thời gian sử dụng; định hướng thái độ, hình thành thói quen; là người đầu tiên nhận thấy biểu hiện bất thường tại nhà; là cầu nối giữa nhà trường và đời sống thực tế của học sinh.

– **Các lực lượng xã hội giữ vai trò hỗ trợ, mở rộng, bảo đảm:** cơ quan công an (phòng ngừa, điều tra, xử lý tội phạm), cơ quan y tế (chăm sóc sức khỏe tâm thần), chính quyền địa phương và hệ thống bảo vệ trẻ em, Đoàn Thanh niên, Đội Thiếu niên, Hội Liên hiệp Phụ nữ, cơ quan truyền thông, chuyên gia, doanh nghiệp cung cấp nền tảng số (kiểm soát nội dung, cơ chế báo cáo).

5.2. Nội dung và nguyên tắc phối hợp

5.2.1. Nội dung phối hợp

Phối hợp được thực hiện trong toàn bộ chu trình giáo dục, gồm bốn nội dung:

– **Phối hợp xây dựng kế hoạch:** nhà trường chủ trì, lấy ý kiến cha mẹ học sinh, các lực lượng liên quan; kế hoạch sát với đặc điểm học sinh và điều kiện địa phương.

– **Phối hợp tổ chức hoạt động:** cùng thực hiện các nội dung giáo dục (bảo vệ thông tin cá nhân, đánh giá thông tin, kiểm soát thời gian, ứng phó bắt nạt, nhận diện nguy cơ); tổ chức hoạt động chung.

– **Phối hợp trao đổi thông tin:** chia sẻ hai chiều về thói quen sử dụng Internet, biểu hiện bất thường của học sinh, nguy cơ mới, thủ đoạn mới.

– **Phối hợp kiểm tra, đánh giá:** cùng theo dõi sự chuyển biến về nhận thức, thái độ, hành vi của học sinh; đánh giá hiệu quả phối hợp để điều chỉnh.

5.2.2. Nguyên tắc phối hợp

– Thống nhất mục tiêu, thông điệp, quy tắc; tránh mâu thuẫn trong yêu cầu đối với học sinh.

– Tôn trọng, bình đẳng, chia sẻ trách nhiệm; không đổ lỗi giữa nhà trường và gia đình khi có sự cố.

– Đặt lợi ích tốt nhất của học sinh làm trung tâm; bảo mật thông tin của học sinh và gia đình.

– Thường xuyên, liên tục, có cơ chế cụ thể (đầu mối, kênh liên lạc, quy trình).

5.3. Phối hợp với cha mẹ học sinh

5.3.1. Phối hợp trong giáo dục phòng ngừa

a) Họp cha mẹ học sinh theo chuyên đề. Mỗi năm học, GVCN dành ít nhất một buổi họp (hoặc một phần buổi họp) về an toàn trên không gian mạng, với nội dung: nguy cơ phổ biến theo lứa tuổi; dấu hiệu cảnh báo; cách trò chuyện với con; các công cụ quản lý của gia đình; quy định về tài khoản game của người dưới 16 tuổi; quy trình của nhà trường khi xảy ra sự cố.

b) Hướng dẫn cha mẹ cách đồng hành với con. Nghiên cứu về vai trò của cha mẹ cho thấy cách tiếp cận "đồng hành tích cực" (trò chuyện, cùng sử dụng, giải thích) hiệu quả hơn so với chỉ hạn chế, cấm đoán; cấm đoán đơn thuần có thể giảm rủi ro trước mắt nhưng đồng thời giảm cơ hội phát triển kỹ năng của trẻ (Livingstone & Helsper, 2008). Giáo viên có thể khuyến nghị cha mẹ:

– Thường xuyên hỏi con về đời sống trực tuyến với thái độ quan tâm, không tra hỏi.

– Cùng con xây dựng **Thỏa thuận sử dụng thiết bị trong gia đình** (Phụ lục 5): thời gian, không gian không dùng thiết bị (bữa ăn, phòng ngủ ban đêm), ứng dụng được sử dụng, những điều cần hỏi ý kiến cha mẹ.

– Sử dụng công cụ quản lý của gia đình phù hợp với lứa tuổi, minh bạch với con; giảm dần mức kiểm soát khi con lớn và có trách nhiệm hơn.

– Làm gương trong sử dụng thiết bị; xin phép con trước khi đăng ảnh của con lên mạng.

– Cam kết với con: khi con gặp sự cố và kể với cha mẹ, cha mẹ sẽ giúp, không la mắng, không tịch thu điện thoại như một hình phạt.

c) Giao "nhiệm vụ an toàn tại nhà". Sau các hoạt động trên lớp, giáo viên giao nhiệm vụ học sinh cùng cha mẹ thực hiện: cùng kiểm tra cài đặt quyền riêng tư; cùng tạo mật khẩu mạnh, bật xác thực hai yếu tố; thống nhất "câu hỏi bí mật" của gia đình để kiểm chứng cuộc gọi khẩn cấp; cùng xây dựng thỏa thuận sử dụng thiết bị. Cách làm "trải nghiệm kép" này giúp kiến thức được củng cố ở cả hai môi trường.

d) Duy trì kênh thông tin hai chiều. Sử dụng nhóm liên lạc của lớp, sổ liên lạc điện tử để chia sẻ cảnh báo thủ đoạn mới, tài liệu hướng dẫn; thiết lập kênh để cha mẹ phản ánh các tình huống học sinh gặp phải (bảo đảm riêng tư), giúp giáo viên xây dựng tình huống giáo dục sát thực tế.

5.3.2. Phối hợp khi xảy ra sự cố

a) Thông báo cho cha mẹ học sinh.

– Thông báo kịp thời, trực tiếp (gặp mặt hoặc điện thoại), không thông báo qua nhóm chung.

– Chuẩn bị trước: nắm thông tin cơ bản, các bước nhà trường đã làm, dự kiến phản ứng của cha mẹ.

– Bắt đầu bằng sự quan tâm chung: "Nhà trường và gia đình cùng mong muốn cháu an toàn."

– Trình bày sự việc khách quan, ngắn gọn, không dùng ngôn từ quy kết; tập trung vào nhu cầu của học sinh và các bước tiếp theo.

– Hướng dẫn cha mẹ cách hỗ trợ con: lắng nghe, không trách mắng, không tự liên hệ với đối tượng, bảo toàn chứng cứ, phối hợp với cơ quan chức năng.

b) Ứng xử khi cha mẹ phản ứng tiêu cực. Cha mẹ có thể sốc, tức giận, phủ nhận, đổ lỗi cho con hoặc cho nhà trường. Giáo viên giữ bình tĩnh, ghi nhận cảm xúc của cha mẹ ("Tôi hiểu anh/chị rất lo lắng"), tránh tranh luận, đưa cuộc trao đổi trở lại trọng tâm là sự an toàn của học sinh; khi cần, mời Ban Giám hiệu hoặc người làm tư vấn học đường cùng tham gia.

c) Trường hợp đặc biệt.

– Khi có căn cứ cho rằng người gây hại là thành viên gia đình hoặc việc thông báo có thể khiến học sinh gặp nguy hiểm: không thông báo cho gia đình trước; báo ngay Hiệu trưởng, cơ quan Công an, Tổng đài 111 (Tổng đài Quốc gia Bảo vệ Trẻ em, Cục Bà mẹ và Trẻ em) để có biện pháp bảo vệ.

– Khi sự việc liên quan đến nhiều học sinh (cả nạn nhân và người gây hại là học sinh trong trường): làm việc riêng với từng gia đình; bảo mật thông tin của các bên; không tổ chức đối chất giữa các gia đình khi chưa có sự chuẩn bị.

5.4. Phối hợp với các lực lượng xã hội

Lực lượng	**Nội dung phối hợp chủ yếu**
Cơ quan công an (xã, phường; đơn vị an ninh mạng, cảnh sát hình sự)	Tuyên truyền pháp luật, cảnh báo thủ đoạn mới; tham gia ngày hội, buổi nói chuyện chuyên đề; tiếp nhận, xử lý vụ việc có dấu hiệu tội phạm.

Lực lượng	Nội dung phối hợp chủ yếu
Cơ quan y tế, chuyên gia sức khỏe tâm thần	Tư vấn, điều trị cho học sinh có vấn đề sức khỏe tâm thần; tập huấn cho giáo viên về nhận diện, hỗ trợ ban đầu.
Chính quyền địa phương, hệ thống bảo vệ trẻ em, Tổng đài 111 (Tổng đài Quốc gia Bảo vệ Trẻ em, Cục Bà mẹ và Trẻ em)	Tiếp nhận, đánh giá, can thiệp các trường hợp trẻ em bị xâm hại, có nguy cơ; kết nối dịch vụ hỗ trợ.
Đoàn Thanh niên, Đội Thiếu niên, Hội Liên hiệp Phụ nữ	Tổ chức hoạt động truyền thông, câu lạc bộ, cuộc thi; phát triển mạng lưới hỗ trợ đồng đẳng; truyền thông cho cha mẹ tại cộng đồng.
Chuyên gia giáo dục, công nghệ	Tập huấn, cung cấp học liệu; thẩm định nội dung giáo dục bảo đảm chính xác, cập nhật.
Doanh nghiệp cung cấp nền tảng số	Cơ chế báo cáo, gỡ bỏ nội dung vi phạm; công cụ bảo vệ người dùng nhỏ tuổi; tham gia chương trình giáo dục an toàn số.

Bảng 5.1. Nội dung phối hợp với các lực lượng xã hội

Để phối hợp hiệu quả, nhà trường cần xây dựng mô hình và cơ chế phối hợp theo năm bước: (1) xác định cấu trúc mô hình – các lực lượng tham gia và mối quan hệ; (2) thiết kế cơ chế – vai trò, trách nhiệm, quy trình, kênh thông tin, cách xử lý tình huống phát sinh; (3) tổ chức triển khai – phổ biến, phân công đầu mối, thiết lập kênh liên lạc trực tiếp và trực tuyến; (4) vận hành và điều phối, trong đó nhà trường giữ vai trò trung tâm; (5) đánh giá định kỳ và hoàn thiện. Kết quả khảo sát cho thấy sự tham gia của các lực lượng bên ngoài (chuyên gia, cơ quan chức năng) hiện còn hạn chế; vì vậy nhà trường cần chủ động thiết lập đầu mối liên hệ cụ thể với công an xã, phường và cơ sở y tế trên địa bàn ngay từ đầu năm học, không đợi đến khi xảy ra sự cố.

5.5. Xây dựng môi trường mạng an toàn trong nhà trường

Môi trường mạng an toàn là hình thức giáo dục gián tiếp nhưng có tác động thường xuyên, lâu dài. Nhà trường có thể thực hiện các biện pháp:

– **Quy định về sử dụng thiết bị số và Internet** trong nhà trường, được xây dựng với sự tham gia của học sinh, cha mẹ học sinh; phù hợp với từng cấp học.

– **Quy tắc ứng xử trong nhóm trực tuyến của lớp, trường** (nhóm Zalo, Messenger…): mục đích sử dụng; thời gian nhắn tin; ngôn ngữ; không đăng ảnh, thông tin của người khác khi chưa đồng ý; người quản trị nhóm; cách xử lý khi có vi phạm. GVCN là người quản trị, không để nhóm lớp do người ngoài quản lý.

– **Kênh báo cáo an toàn, có thể ẩn danh:** hộp thư, biểu mẫu trực tuyến, phòng tư vấn; được thông báo rộng rãi đến học sinh.

– **Bảo vệ dữ liệu cá nhân của học sinh** trong hoạt động của nhà trường: xin sự đồng ý trước khi đăng ảnh học sinh; hạn chế công bố họ tên kèm hình ảnh, ngày sinh; bảo mật hồ sơ học sinh.

– **Mạng lưới hỗ trợ đồng đẳng:** lựa chọn, tập huấn học sinh có uy tín làm đồng đẳng viên, biết lắng nghe bạn và kết nối bạn với người lớn; có giáo viên phụ trách giám sát, hỗ trợ.

– **Truyền thông tích cực:** lan tỏa các tấm gương ứng xử đẹp trên mạng, sản phẩm sáng tạo của học sinh về an toàn số.

HOẠT ĐỘNG TẬP HUẤN

Hoạt động 5.1. Đóng vai trao đổi với cha mẹ học sinh (40 phút)

Nhóm ba người (GVCN, cha mẹ học sinh, người quan sát) đóng vai tình huống: GVCN mời mẹ của học sinh lớp 9 đến trường để thông báo con bị một tài khoản lạ tống tiền bằng hình ảnh nhạy cảm (con đã kể với GVCN sáng nay; nhà trường đã báo công an). Người mẹ phản ứng: "Con tôi không thể như thế được! Chắc chắn là do bạn bè ở trường rủ rê. Về nhà tôi sẽ đập điện thoại của nó."

Gợi ý: GVCN chuẩn bị nơi riêng tư, có thể mời người làm tư vấn học đường cùng tham gia; mở đầu bằng mục tiêu chung là sự an toàn của con; ghi nhận cảm xúc của mẹ; trình bày khách quan, không mô tả chi tiết hình ảnh; nhấn mạnh con là nạn nhân, con đã rất dũng cảm khi kể; giải thích các thủ đoạn tống tiền tinh vi nhắm vào học sinh; khuyến nghị không trách phạt, không đập điện thoại (vừa làm mất chứng cứ, vừa khiến con không dám chia sẻ lần sau), không tự liên lạc với đối tượng; thống nhất các bước phối hợp với công an và kế hoạch hỗ trợ tâm lý; hẹn lịch trao đổi tiếp.

Hoạt động 5.2. Xây dựng quy tắc nhóm lớp trực tuyến (30 phút)
Mỗi nhóm thầy cô soạn thảo bộ quy tắc ứng xử (5 – 7 điều) cho nhóm trực tuyến của một lớp học (nhóm học sinh hoặc nhóm cha mẹ học sinh) và đề xuất cách tổ chức để học sinh, cha mẹ cùng tham gia xây dựng.
Gợi ý: Quy tắc tham khảo: (1) Nhóm dùng cho thông tin học tập, hoạt động của lớp; (2) Nhắn tin trong khung giờ quy định; (3) Dùng ngôn ngữ lịch sự, tôn trọng; (4) Không đăng ảnh, thông tin cá nhân của người khác khi chưa được đồng ý; (5) Không chia sẻ đường link lạ, tin chưa kiểm chứng; (6) Vấn đề riêng trao đổi riêng với GVCN; (7) Khi thấy nội dung không phù hợp, báo ngay cho GVCN. Cách tổ chức: thảo luận trong tiết sinh hoạt lớp, biểu quyết, công bố công khai, rà soát định kỳ.

GHI NHỚ

– Nhà trường chủ đạo, điều phối; gia đình nền tảng, trực tiếp; xã hội hỗ trợ, mở rộng – không lực lượng nào có thể thay thế lực lượng khác.

– Phối hợp trong cả chu trình: kế hoạch – tổ chức – thông tin – đánh giá.

– Cha mẹ đồng hành tích cực hiệu quả hơn cấm đoán; cam kết "không phạt khi con kể" là điều kiện để học sinh tìm kiếm sự giúp đỡ.

– Thông báo sự cố cho cha mẹ cần trực tiếp, riêng tư, khách quan; trường hợp nghi người gây hại trong gia đình phải báo cơ quan chức năng trước.

– Thiết lập đầu mối với công an, y tế từ đầu năm học; xây dựng môi trường số an toàn trong nhà trường.

CÂU HỎI TỰ ĐÁNH GIÁ

1. Trình bày bốn nội dung phối hợp giữa các lực lượng trong giáo dục và hỗ trợ học sinh tương tác an toàn.

2. Vì sao cách tiếp cận "đồng hành tích cực" của cha mẹ hiệu quả hơn cách tiếp cận chỉ cấm đoán?

3. Nêu các bước chuẩn bị và tiến hành thông báo cho cha mẹ học sinh khi con gặp sự cố.

4. Trong trường hợp nào nhà trường không thông báo cho gia đình trước? Khi đó cần làm gì?

5. Đề xuất ba biện pháp xây dựng môi trường số an toàn phù hợp với trường của thầy cô.

CHUYÊN ĐỀ 6. VÍ DỤ MINH HỌA VÀ THỰC HÀNH THIẾT KẾ HOẠT ĐỘNG GIÁO DỤC

(Thời lượng: 120 phút)

MỤC TIÊU

Sau khi học xong chuyên đề này, thầy cô có thể:

– Phân tích được cấu trúc, cách tổ chức các kế hoạch hoạt động mẫu ở ba cấp học.

– Điều chỉnh, vận dụng được kế hoạch mẫu vào điều kiện lớp học của mình.

– Thiết kế được một kế hoạch hoạt động giáo dục tương tác an toàn trên không gian mạng tích hợp trong môn học, HĐTN, HN hoặc sinh hoạt lớp.

– Phân tích được các trường hợp giáo viên xử lý sự cố và phối hợp với cha mẹ học sinh.

HƯỚNG DẪN SỬ DỤNG CÁC KẾ HOẠCH MẪU

Các kế hoạch dưới đây được thiết kế theo chu trình học tập trải nghiệm (Chuyên đề 3), có thời lượng 35 phút. Thầy cô có thể sử dụng nguyên vẹn, rút gọn thành hoạt động trong tiết sinh hoạt lớp hoặc tách thành các hoạt động tích hợp trong môn học. Các tình huống, tên nhân vật là giả định; thầy cô nên điều chỉnh cho gần gũi với học sinh địa phương nhưng không sử dụng tình huống thật của học sinh trong lớp.

Kế hoạch	Cấp học	Chủ đề	Con đường tổ chức
6.1.1	Tiểu học (lớp 4, 5)	Sử dụng mạng xã hội an toàn	HĐTN (hoạt động hướng đến xã hội), sinh hoạt lớp
6.1.2	THCS (lớp 7, 8)	Phòng tránh lừa đảo và bảo vệ tài khoản	Tích hợp môn Tin học; HĐTN, HN
6.1.3	THCS (lớp 8, 9)	Phòng tránh nguy cơ xâm hại tình dục trên không gian mạng	HĐTN, HN; giáo dục kỹ năng sống

Kế hoạch	Cấp học	Chủ đề	Con đường tổ chức
6.1.4	THPT (lớp 10, 11)	Tin giả, deepfake và nội dung do AI tạo ra	Tích hợp Ngữ văn, Giáo dục kinh tế và pháp luật; HĐTN, HN
6.1.5	THPT (lớp 11, 12)	Dấu chân số và hồ sơ trực tuyến trong định hướng nghề nghiệp	HĐTN, HN (hoạt động hướng nghiệp)
6.1.6	THPT (lớp 10 – 12)	Cân bằng đời sống số và sức khỏe tinh thần	Sinh hoạt lớp; HĐTN, HN

Bảng 6.1. Danh mục kế hoạch hoạt động mẫu

6.1. Các kế hoạch hoạt động mẫu

6.1.1. Kế hoạch mẫu cấp Tiểu học: SỬ DỤNG MẠNG XÃ HỘI AN TOÀN

Đối tượng: Học sinh lớp 4, 5. **Thời lượng:** 35 phút. **Hình thức:** HĐTN, sinh hoạt lớp.

1. Yêu cầu cần đạt

– Phân biệt được thông tin có thể chia sẻ và thông tin cần giữ kín trên mạng.

– Nhận diện được một số dấu hiệu nguy hiểm: người lạ hỏi thông tin riêng tư, tin nhắn trúng thưởng, đường link lạ, lời chế giễu.

– Thực hiện được quy tắc "Dừng lại – Hỏi người lớn" và nói tên được ít nhất một người lớn tin cậy có thể giúp đỡ.

– Thể hiện thái độ tử tế, tôn trọng bạn bè khi giao tiếp trên mạng.

2. Chuẩn bị

– Giáo viên: thẻ màu xanh – vàng – đỏ; Phiếu "Đèn giao thông an toàn" (Phụ lục 6); 4 thẻ tình huống; giấy A0, bút màu.

– Học sinh: bút, giấy.

3. Tiến trình hoạt động

Thời gian	Hoạt động	Phương pháp	Sản phẩm
5 phút	Khởi động: Trò chơi "Đăng hay không đăng?"	Trò chơi	Học sinh nhận diện ban đầu
10 phút	Khám phá: "Đèn giao thông an toàn"	Thảo luận nhóm, phân loại	Phiếu đã hoàn thành
10 phút	Thực hành: "Em sẽ làm gì?"	Đóng vai	Cách xử lý tình huống
10 phút	Vận dụng: "5 nguyên tắc an toàn của em"; vé ra khỏi lớp	Làm việc cá nhân, cả lớp	Bộ quy tắc, phiếu cá nhân

Hoạt động 1. Khởi động – "Đăng hay không đăng?" Giáo viên đọc lần lượt các tình huống, học sinh giơ thẻ xanh (an toàn), vàng (cần hỏi người lớn), đỏ (không được làm): đăng bức tranh em tự vẽ; đăng ảnh vé xem phim có mã QR; một người hỏi địa chỉ nhà em; đăng ảnh của bạn khi chưa hỏi bạn; gửi mật khẩu cho người tự nhận là nhân viên hỗ trợ. Giáo viên hỏi lý do lựa chọn và kết luận: "Có những điều chúng ta có thể chia sẻ để kết nối với bạn bè, nhưng có những thông tin cần được bảo vệ."

Hoạt động 2. Khám phá – "Đèn giao thông an toàn". Nhóm 4 học sinh hoàn thành Phiếu "Đèn giao thông an toàn" với 10 tình huống. Các nhóm trình bày, giáo viên tổ chức tranh luận những tình huống có ý kiến khác nhau. Giáo viên chốt các "tín hiệu đỏ": người lạ xin thông tin riêng tư; yêu cầu mật khẩu, mã OTP; tin nhắn trúng thưởng, quà miễn phí; đường link lạ; yêu cầu giữ bí mật với bố mẹ; hình ảnh, video làm em sợ.

Hoạt động 3. Thực hành – "Em sẽ làm gì?" Mỗi nhóm nhận một tình huống, thảo luận và đóng vai cách xử lý: (1) người lạ kết bạn và xin số điện thoại; (2) tin nhắn trúng điện thoại mới, bấm link để nhận; (3) bạn trong lớp bị chế giễu trong nhóm chat; (4) em thấy một video làm em sợ. Giáo viên nhận xét, nhấn

mạnh: không trả lời người lạ, không bấm link lạ, không hùa theo chế giễu, động viên bạn và báo người lớn; "**Dừng lại – Hỏi người lớn**".

Hoạt động 4. Vận dụng. Cả lớp cùng hoàn thiện bảng "5 nguyên tắc an toàn của em": (1) SUY NGHĨ trước khi đăng; (2) GIỮ KÍN thông tin riêng tư; (3) CẢNH GIÁC với người lạ và đường link lạ; (4) TỬ TẾ khi giao tiếp; (5) KỂ VỚI NGƯỜI LỚN khi có điều bất thường. Mỗi học sinh hoàn thành "vé ra khỏi lớp": một điều em sẽ không chia sẻ trên mạng; một việc em sẽ làm khi gặp tin nhắn đáng ngờ; tên một người lớn em có thể tìm đến.

4. Đánh giá: Quan sát lựa chọn và cách giải thích của học sinh trong hoạt động 1 – 3; phân tích phiếu "vé ra khỏi lớp" theo ba mức: Hoàn thành tốt – nhận diện đúng nguy cơ, giải thích được, biết tìm người hỗ trợ; Hoàn thành – nhận diện được phần lớn nguy cơ; Cần hỗ trợ – còn chia sẻ thông tin riêng tư, chưa biết tìm người lớn hỗ trợ.

5. Nhiệm vụ tại nhà: Học sinh cùng bố mẹ đọc "5 nguyên tắc an toàn của em" và cùng chọn một "câu hỏi bí mật" của gia đình.

6.1.2. Kế hoạch mẫu cấp THCS: PHÒNG TRÁNH LỪA ĐẢO VÀ BẢO VỆ TÀI KHOẢN

Đối tượng: Học sinh lớp 7, 8. **Thời lượng:** 45 phút. **Hình thức:** tích hợp môn Tin học (chủ đề đạo đức, pháp luật và văn hóa trong môi trường số) hoặc HĐTN, HN.

1. Yêu cầu cần đạt

– Nhận diện được các dấu hiệu chung của thủ đoạn lừa đảo trực tuyến (lợi ích bất ngờ, hối thúc, đe dọa, yêu cầu bí mật, yêu cầu thông tin bí mật).

– Tạo được mật khẩu mạnh; trình bày được cách bật xác thực hai yếu tố và xử lý khi tài khoản bị chiếm đoạt.

– Vận dụng được quy tắc "Dừng lại – Kiểm tra – Hỏi người lớn" trong tình huống mô phỏng.

2. Chuẩn bị: 6 "tin nhắn mô phỏng" in trên giấy (trúng thưởng; "admin game" xin OTP; tài khoản bạn thân bị chiếm nhắn vay tiền; "công an" gọi điện đe dọa; trang đăng nhập giả mạo; tin nhắn bình thường của giáo viên); phiếu "Thám tử mạng"; máy chiếu.

3. Tiến trình hoạt động

Hoạt động 1. Khởi động – "Ai là người thật?" (5 phút). Giáo viên chiếu hai trang đăng nhập (một thật, một giả có địa chỉ sai một ký tự). Học sinh dự đoán trang thật. Giáo viên dẫn dắt: kẻ lừa đảo tạo ra những thứ rất giống thật.

Hoạt động 2. Khám phá – "Thám tử mạng" (15 phút). Nhóm 4 học sinh nhận bộ 6 tin nhắn, xác định tin nhắn lừa đảo và gạch chân "dấu hiệu nghi vấn". Các nhóm báo cáo; giáo viên tổng hợp thành "5 dấu hiệu lừa đảo": (1) lợi ích quá tốt; (2) hối thúc làm ngay; (3) đe dọa, gây sợ hãi; (4) yêu cầu giữ bí mật; (5) yêu cầu mật khẩu, OTP, tiền hoặc bấm link lạ. Giáo viên giới thiệu thủ đoạn "bắt cóc online" và khẳng định: công an không làm việc, không yêu cầu chuyển tiền qua điện thoại hay mạng xã hội.

Hoạt động 3. Thực hành – "Pháo đài tài khoản" (15 phút).

– Học sinh thực hành tạo mật khẩu mạnh theo phương pháp "câu dài dễ nhớ" (ví dụ ghép 4 từ ngẫu nhiên kèm số và ký hiệu) và tự đánh giá độ mạnh theo tiêu chí: độ dài, không chứa thông tin cá nhân, không dùng lại.

– Giáo viên trình chiếu thao tác bật xác thực hai yếu tố trên một tài khoản mô phỏng.

– Thảo luận: "Nếu tài khoản bị chiếm, em làm gì theo thứ tự nào?" Đáp án hướng tới:

Bước 1: Báo cha mẹ, thầy cô để tình hình được kiểm soát.

Bước 2: Thu hồi tất cả các phiên đăng nhập đang hoạt động (Revoke Active Sessions); bảo vệ email, số điện thoại và đổi mật khẩu.

Bước 3: Chọn tính năng "Đăng xuất khỏi tất cả các thiết bị khác" sau khi đổi mật khẩu để vô hiệu hóa Cookie/Token của kẻ gian.

Bước 4: Gỡ ứng dụng lạ khỏi thiết bị đang sử dụng.

Bước 5: Bật xác thực 2 lớp và báo nền tảng.

Bước 6: Chia sẻ thông tin cho bạn bè và người dùng khác.

Hoạt động 4. Vận dụng – "Dừng lại – Kiểm tra – Hỏi người lớn" (10 phút). Học sinh đóng vai theo cặp: một bạn đóng vai kẻ lừa đảo dùng kịch bản có sẵn, một bạn thực hành từ chối và kiểm chứng. Giáo viên nhận xét, chốt quy tắc.

4. Đánh giá: bảng kiểm khi đóng vai (có nhận ra dấu hiệu, có từ chối, có đề xuất kiểm chứng/hỏi người lớn); kiểm tra độ mạnh mật khẩu học sinh tạo (không ghi lại mật khẩu thật).

5. Nhiệm vụ tại nhà: Cùng bố mẹ bật xác thực hai yếu tố cho một tài khoản của gia đình và kiểm tra cài đặt quyền riêng tư; chia sẻ "5 dấu hiệu lừa đảo" với người thân.

6.1.3. Kế hoạch mẫu cấp THCS: PHÒNG TRÁNH NGUY CƠ XÂM HẠI TÌNH DỤC TRÊN KHÔNG GIAN MẠNG

Đối tượng: Học sinh lớp 8, 9. **Thời lượng:** 45 phút. **Hình thức:** HĐTN, HN hoặc giáo dục kỹ năng sống. **Lưu ý:** thông báo trước cho học sinh và cha mẹ học sinh; giáo viên nắm vững quy trình tiếp nhận ở Chuyên đề 4; có người làm tư vấn học đường sẵn sàng hỗ trợ.

1. Yêu cầu cần đạt

– Nhận diện được dấu hiệu của cuộc trò chuyện, mối quan hệ trực tuyến không an toàn và các hành vi dụ dỗ, thao túng, đe dọa.

– Thực hành được quy trình tự bảo vệ DỪNG – LƯU – CHẶN – BÁO – KỂ.

– Tôn trọng cơ thể, ranh giới cá nhân của bản thân và người khác; chủ động tìm kiếm sự giúp đỡ khi bản thân hoặc bạn bè gặp nguy cơ.

2. Chuẩn bị: thẻ AN TOÀN – CẢNH GIÁC – NGUY HIỂM; phiếu tình huống; phiếu "3 điều em sẽ nhớ". Không sử dụng hình ảnh nhạy cảm, không mô tả trực tiếp hành vi xâm hại.

3. Tiến trình hoạt động

Thời gian	Hoạt động	Phương pháp	Sản phẩm
5 phút	Khởi động "An toàn hay nguy cơ?"	Trò chơi nhanh	Nhận diện ban đầu
8 phút	Nhận diện nguy cơ "Điều gì đang xảy ra?"	Phân tích tình huống	Danh sách dấu hiệu
12 phút	Xử lý tình huống "Nếu là em, em sẽ làm gì?"	Thảo luận nhóm, đóng vai	Phương án xử lý
10 phút	Thực hành "5 bước tự bảo vệ"	Cá nhân, nhóm	Quy trình ứng phó
10 phút	Cam kết hành động	Viết nhanh, chia sẻ tự nguyện	Phiếu cá nhân

Hoạt động 1. Khởi động (5 phút). Học sinh giơ thẻ với 4 tình huống: (1) bạn cùng lớp nhắn hỏi bài tập; (2) tài khoản lạ kết bạn, nói cùng tuổi và liên tục khen ngợi; (3) người quen trên mạng xin ảnh riêng tư, hứa "chỉ mình xem"; (4) tài khoản đe dọa đăng tin nhắn cũ nếu không gửi ảnh. Giáo viên kết luận: không phải mọi người trên mạng đều có ý xấu, nhưng cần nhận diện dấu hiệu bất thường và biết dừng lại.

Hoạt động 2. Nhận diện nguy cơ (8 phút). Nhóm thảo luận tình huống: "Minh, 13 tuổi, chơi game trực tuyến. Một tài khoản mới quen thường xuyên trò chuyện, nói mình 14 tuổi và rất hiểu Minh, tặng Minh vật phẩm game. Sau một thời gian, người đó hỏi về trường học, địa chỉ nhà, đề nghị chuyển sang ứng dụng nhắn tin khác và xin ảnh. Khi Minh ngần ngại, người đó nói: 'Nếu coi nhau là bạn thì phải tin nhau.'" Câu hỏi: Dấu hiệu nào khiến em cần cảnh giác? Người đó đang cố tạo ra điều gì? Minh nên làm gì? Giáo viên chốt các dấu hiệu: tạo thân thiết rất nhanh; hỏi nhiều thông tin cá nhân; muốn chuyển sang kênh riêng; yêu cầu giữ bí mật; xin ảnh, video riêng tư; tặng quà để đổi lấy lòng tin; dùng lời khen, tình cảm để gây ảnh hưởng; gây áp lực, đe dọa khi bị từ chối. Thông điệp: "Một người nói họ cùng tuổi với em trên mạng không có nghĩa là họ thực sự cùng tuổi."

Hoạt động 3. Xử lý tình huống (12 phút). Mỗi nhóm nhận một tình huống: (1) yêu cầu gửi ảnh riêng tư kèm lời hứa giữ bí mật; (2) người quen qua mạng hẹn gặp ở nơi vắng, dặn không nói với bố mẹ; (3) tài khoản đe dọa đăng ảnh đã có nếu em không gửi thêm; (4) em phát hiện bạn cùng lớp thường xuyên nhắn tin với một người lớn trên mạng, người đó yêu cầu bạn giữ bí mật và gửi ảnh. Nhóm thảo luận 4 phút, trình bày 1 phút. Giáo viên nhấn mạnh với tình huống 3: "Đừng gửi thêm, đừng trả tiền, đó không phải lỗi của em, hãy kể với người lớn ngay"; với tình huống 4: đây không phải "chuyện riêng của bạn", cần nói với người lớn để bảo vệ bạn.

Hoạt động 4. Thực hành "5 bước tự bảo vệ" (10 phút). Giáo viên giới thiệu quy trình: **DỪNG – không đáp lại** yêu cầu khiến em sợ, khó chịu ("Mình không muốn làm việc này. Mình dừng cuộc trò chuyện."); **CHẶN** – chặn, hạn chế liên hệ, không tranh luận với người đe dọa; **LƯU** – không xóa tin nhắn, ghi lại tên tài khoản; không gửi thêm ảnh, tiền để "đổi lấy việc xóa ảnh"; **BÁO** – dùng chức năng báo cáo của nền tảng; **KỂ** – nói với cha mẹ, thầy cô, người làm tư vấn học đường, người thân tin cậy hoặc gọi 111 (Tổng đài Quốc gia Bảo vệ Trẻ em, Cục

Bà mẹ và Trẻ em). Học sinh viết nhanh 5 hành động tương ứng cho một tình huống đe dọa; 2 – 3 học sinh trình bày.

Hoạt động 5. Cam kết (10 phút). Học sinh hoàn thành phiếu "3 điều em sẽ nhớ": khi người lạ hỏi thông tin riêng tư, em sẽ…; khi có người yêu cầu gửi hình ảnh khiến em không thoải mái, em sẽ…; khi em hoặc bạn gặp nguy cơ, em sẽ tìm sự giúp đỡ từ… Giáo viên kết thúc: "Không im lặng khi có nguy cơ. Không tự trách mình khi bị lừa hoặc bị đe dọa. Thầy cô luôn sẵn sàng giúp em." Giáo viên thông báo cách học sinh có thể gặp riêng giáo viên hoặc người làm tư vấn học đường sau buổi học.

4. Đánh giá: phiếu tự đánh giá (Chưa đạt – Đạt – Tốt) về: nhận biết dấu hiệu nguy cơ; bảo vệ thông tin cá nhân; từ chối yêu cầu không phù hợp; chặn, báo cáo; tìm người lớn hỗ trợ. Giáo viên đánh giá theo bốn tiêu chí: nhận diện nguy cơ, bảo vệ bản thân, ứng phó, tìm kiếm hỗ trợ (rubric ở Bảng 3.6).

6.1.4. Kế hoạch mẫu cấp THPT: TIN GIẢ, DEEPFAKE VÀ NỘI DUNG DO AI TẠO RA

Đối tượng: Học sinh lớp 10, 11. **Thời lượng:** 45 phút. **Hình thức:** tích hợp Ngữ văn (đọc hiểu văn bản thông tin), Giáo dục kinh tế và pháp luật; hoặc HĐTN, HN.

1. Yêu cầu cần đạt

– Phân biệt được thông tin sai lệch, thông tin cố ý gây hiểu lầm; giải thích được vì sao tin giả lan truyền nhanh.

– Vận dụng được kỹ thuật kiểm chứng "đọc ngang" và bộ câu hỏi "Ai nói? Bằng chứng ở đâu? Nguồn khác nói gì?".

– Nhận diện được một số dấu hiệu của nội dung do AI tạo ra; nêu được cách xử lý khi bản thân hoặc bạn bè bị làm giả hình ảnh.

– Có thái độ trách nhiệm trước khi chia sẻ; nhận thức được hậu quả pháp lý, đạo đức của việc tạo và phát tán nội dung giả mạo người khác.

2. Chuẩn bị: 4 "bài đăng mô phỏng" (tin sức khỏe giật gân; thông báo tuyển sinh giả mạo; ảnh do AI tạo về một sự kiện thiên tai; trích dẫn bịa đặt của người nổi tiếng); thiết bị có kết nối Internet cho các nhóm; phiếu kiểm chứng.

3. Tiến trình hoạt động

Hoạt động 1. Khởi động – "Thật hay giả?" (7 phút). Giáo viên chiếu 6 hình ảnh (3 ảnh thật, 3 ảnh do AI tạo); học sinh bình chọn. Công bố kết quả; thảo

luận: em dựa vào đâu để đoán? Kết luận: mắt thường ngày càng khó phân biệt, cần phương pháp kiểm chứng thay vì cảm giác.

Hoạt động 2. Khám phá – Vì sao tin giả lan nhanh? (8 phút). Giáo viên giới thiệu ngắn kết quả nghiên cứu: tin sai lan truyền nhanh và rộng hơn tin đúng, chủ yếu do con người chia sẻ vì tính mới lạ, gây cảm xúc mạnh (Vosoughi và cộng sự, 2018). Học sinh liên hệ: lần gần nhất em chia sẻ một tin mà chưa kiểm tra là khi nào, vì sao?

Hoạt động 3. Thực hành – "Phòng kiểm chứng" (20 phút). Mỗi nhóm nhận một bài đăng mô phỏng, thực hiện kiểm chứng theo phiếu: (1) Ai đăng? Tài khoản này là ai? (tìm thông tin về nguồn ở trang khác – "đọc ngang"); (2) Bằng chứng nào được đưa ra? Có thể kiểm tra không? (3) Các nguồn chính thống nói gì? (4) Hình ảnh có dấu hiệu chỉnh sửa, do AI tạo không? (tìm kiếm ngược hình ảnh, kiểm tra chi tiết bất thường); (5) Kết luận và quyết định: chia sẻ, không chia sẻ hay báo cáo? Các nhóm trình bày.

Hoạt động 4. Vận dụng – Khi chính em bị làm giả (10 phút). Thảo luận tình huống: "Một học sinh lớp 11 phát hiện ảnh khuôn mặt mình bị ghép vào một video phản cảm, đang được chia sẻ trong nhóm chat của khối." Câu hỏi: Bạn ấy nên làm gì? Những người nhận được video nên làm gì? Người tạo video có thể phải chịu trách nhiệm gì? Giáo viên chốt: nạn nhân không có lỗi; không chia sẻ tiếp; lưu thông tin, báo cáo nền tảng; báo thầy cô, cha mẹ, cơ quan chức năng; tạo và phát tán nội dung giả mạo gây tổn hại người khác là hành vi vi phạm pháp luật, có thể bị xử lý.

4. Đánh giá: rubric đánh giá phiếu kiểm chứng (xác định nguồn, sử dụng bằng chứng, đối chiếu nguồn chính thống, lập luận kết luận); phiếu phản tư cá nhân: "Một thói quen em sẽ thay đổi trước khi chia sẻ thông tin".

5. Mở rộng: học sinh thực hiện dự án nhóm "Chiến dịch dừng lại trước khi chia sẻ" trên bảng tin của trường (không đăng công khai trên mạng nếu chưa có sự đồng ý).

6.1.5. Kế hoạch mẫu cấp THPT: DẤU CHÂN SỐ VÀ HỒ SƠ TRỰC TUYẾN TRONG ĐỊNH HƯỚNG NGHỀ NGHIỆP

Đối tượng: Học sinh lớp 11, 12. **Thời lượng:** 45 phút. **Hình thức:** HĐTN, HN (hoạt động hướng nghiệp).

1. Yêu cầu cần đạt

– Giải thích được khái niệm dấu chân số và tác động của dấu chân số đến cơ hội học tập, nghề nghiệp.

– Tự rà soát được dấu chân số của bản thân; lập được kế hoạch xây dựng hồ sơ trực tuyến tích cực.

– Nhận diện được các thủ đoạn lừa đảo tuyển dụng, "việc nhẹ lương cao" nhắm vào học sinh, sinh viên.

2. Chuẩn bị: hồ sơ mạng xã hội giả định của hai ứng viên; phiếu "Tự rà soát dấu chân số"; 3 tin tuyển dụng mô phỏng (1 thật, 2 lừa đảo).

3. Tiến trình hoạt động

Hoạt động 1. Khởi động – "Nhà tuyển dụng chọn ai?" (8 phút). Học sinh đóng vai nhà tuyển dụng, xem hồ sơ trực tuyến giả định của hai ứng viên có năng lực tương đương (một người có nhiều bài đăng xúc phạm người khác, chia sẻ tin sai; một người có các bài viết về hoạt động tình nguyện, sản phẩm học tập). Thảo luận lựa chọn và lý do. Giáo viên dẫn dắt: dấu chân số trở thành một phần "hồ sơ" của mỗi người.

Hoạt động 2. Khám phá – Dấu chân số của em (12 phút). Học sinh tự rà soát theo phiếu (không cần chia sẻ kết quả): các tài khoản đang sử dụng; thông tin công khai; nội dung mình sẽ không muốn thầy cô, nhà tuyển dụng tương lai nhìn thấy; quyền riêng tư đã thiết lập. Thảo luận theo cặp: điều em ngạc nhiên nhất khi rà soát.

Hoạt động 3. Thực hành – Nhận diện "việc nhẹ lương cao" (12 phút). Nhóm phân tích 3 tin tuyển dụng, chỉ ra dấu hiệu lừa đảo: thu nhập cao bất thường, không yêu cầu kỹ năng; yêu cầu nạp tiền, đặt cọc, mua hàng để "nhận nhiệm vụ"; giao tiếp chỉ qua ứng dụng nhắn tin; yêu cầu ảnh căn cước, thông tin tài khoản ngân hàng; lời mời làm việc ở nước ngoài "bao trọn gói". Giáo viên liên hệ với các vụ việc học sinh, sinh viên bị lừa, bị lôi kéo đi lao động trái phép đã được cơ quan chức năng cảnh báo.

Hoạt động 4. Vận dụng – Kế hoạch hồ sơ trực tuyến tích cực (13 phút). Mỗi học sinh lập kế hoạch 3 bước gắn với định hướng nghề nghiệp của mình: (1) dọn dẹp – điều chỉnh quyền riêng tư, xóa nội dung không phù hợp; (2) xây dựng – chia sẻ sản phẩm học tập, hoạt động tình nguyện, sở thích liên quan đến nghề; (3) duy trì – nguyên tắc trước khi đăng. Một số học sinh chia sẻ tự nguyện.

4. Đánh giá: chất lượng kế hoạch cá nhân (tính cụ thể, khả thi, gắn với định hướng nghề nghiệp); kết quả nhận diện tin tuyển dụng lừa đảo của nhóm.

6.1.6. Kế hoạch mẫu cấp THPT: CÂN BẰNG ĐỜI SỐNG SỐ VÀ SỨC KHỎE TINH THẦN

Đối tượng: Học sinh lớp 10 – 12. **Thời lượng:** 35 phút (tiết sinh hoạt lớp) hoặc 45 phút (HĐTN, HN).

1. Yêu cầu cần đạt

– Nhận biết được tác động hai chiều của mạng xã hội đến cảm xúc, giấc ngủ, hình ảnh bản thân.

– Nhận diện được một số thiết kế lôi kéo của nền tảng số; tự theo dõi và lập kế hoạch điều chỉnh thói quen sử dụng.

– Biết các nguồn hỗ trợ tin cậy khi bản thân hoặc bạn bè gặp khó khăn về tâm lý.

2. Chuẩn bị: phiếu "Nhật ký 3 ngày" (giao trước buổi học: học sinh tự ghi thời gian sử dụng theo dữ liệu trên thiết bị và cảm xúc sau khi sử dụng); thang cảm xúc; danh sách nguồn hỗ trợ.

3. Tiến trình hoạt động

Hoạt động 1. Khởi động – "Sau khi lướt mạng, em cảm thấy…" (5 phút). Học sinh dán giấy nhớ ghi một cảm xúc thường có sau khi dùng mạng xã hội lên bảng "tích cực – trung tính – tiêu cực". Giáo viên nhận xét sự đa dạng: mạng xã hội không tốt cũng không xấu tuyệt đối, phụ thuộc vào cách chúng ta sử dụng.

Hoạt động 2. Khám phá – "Ai đang điều khiển ai?" (10 phút). Nhóm thảo luận các tính năng: cuộn vô tận, tự động phát, thông báo đỏ, chuỗi ngày liên tục, đề xuất theo thuật toán. Câu hỏi: tính năng này khiến em làm gì? Ai được lợi? Em có thể kiểm soát lại như thế nào? Giáo viên giới thiệu ngắn về cơ chế phần thưởng ngẫu nhiên và vì sao não bộ tuổi vị thành niên đặc biệt nhạy cảm với cơ chế này.

Hoạt động 3. Thực hành – Phân tích "Nhật ký 3 ngày" (10 phút). Học sinh tự phân tích nhật ký: thời điểm sử dụng nhiều nhất, nội dung khiến em cảm thấy tốt hơn hoặc tệ hơn, ảnh hưởng đến giấc ngủ. Mỗi học sinh chọn một thay đổi nhỏ trong tuần tới (ví dụ: không dùng điện thoại 30 phút trước khi ngủ; tắt thông báo của một ứng dụng; bỏ theo dõi tài khoản khiến mình tự ti).

Hoạt động 4. Vận dụng – "Khi bạn không ổn" (10 phút). Thảo luận: Những dấu hiệu nào cho thấy một người bạn đang không ổn (qua bài đăng, cách nhắn tin)? Em có thể làm gì? Giáo viên hướng dẫn: hỏi thăm, lắng nghe, không phán xét; không giữ bí mật khi bạn có ý định làm hại bản thân; cùng bạn tìm đến

người lớn tin cậy, người làm tư vấn học đường, Tổng đài 111 (Tổng đài Quốc gia Bảo vệ Trẻ em, Cục Bà mẹ và Trẻ em). Giới thiệu danh sách nguồn hỗ trợ.

4. Đánh giá: phiếu cam kết thay đổi thói quen; tự đánh giá sau một tuần (đã thực hiện được không, cảm nhận thế nào).

Lưu ý: hoạt động không yêu cầu học sinh công khai thời gian sử dụng hoặc cảm xúc cá nhân; giáo viên chú ý những học sinh có biểu hiện cảm xúc tiêu cực trong hoạt động để hỗ trợ riêng.

6.2. Gợi ý lồng ghép theo môn học và khối lớp

Khối lớp	**Môn học, hoạt động**	**Gợi ý nội dung lồng ghép (5 – 15 phút)**
Lớp 1 – 3	Đạo đức; HĐTN	Thông tin nào là của riêng em; "Dừng lại – Hỏi người lớn" khi thấy điều lạ trên màn hình; thời gian dùng thiết bị hợp lý.
Lớp 4 – 5	Tin học và Công nghệ; Tiếng Việt; HĐTN	Mật khẩu là bí mật; nhận diện tin nhắn trúng thưởng; lời nói tử tế khi bình luận; viết đoạn văn về một quy tắc an toàn.
Lớp 6 – 7	Tin học; Giáo dục công dân; HĐTN, HN	Bảo vệ thông tin cá nhân; nhận diện lừa đảo trong game; ứng xử với bắt nạt trực tuyến; vai trò người chứng kiến.
Lớp 8 – 9	Tin học; Giáo dục công dân; Khoa học tự nhiên; Ngữ văn; HĐTN, HN	Dấu hiệu dụ dỗ trực tuyến; dậy thì và ranh giới cá nhân; kiểm chứng thông tin; nghị luận về văn hóa ứng xử trên mạng.
Lớp 10	HĐTN, HN; Ngữ văn; Giáo dục kinh tế và pháp luật; Tin học	Đọc hiểu, đánh giá văn bản thông tin trên mạng; pháp luật về an ninh mạng; quản lý tài chính cá nhân, phòng tránh lừa đảo đầu tư.

Khối lớp	Môn học, hoạt động	Gợi ý nội dung lồng ghép (5 – 15 phút)
Lớp 11	HĐTN, HN; Giáo dục kinh tế và pháp luật; Tin học; Toán	Quyền về dữ liệu cá nhân; đạo đức trong sử dụng AI; xác suất và cờ bạc, loot box.
Lớp 12	HĐTN, HN; Giáo dục kinh tế và pháp luật	Dấu chân số và nghề nghiệp; lừa đảo tuyển dụng; trách nhiệm pháp lý của công dân trên không gian mạng.
Mọi khối lớp	Sinh hoạt lớp	"Mẹo an toàn của tuần"; rà soát quy tắc nhóm lớp; thảo luận một tình huống thời sự; giới thiệu kênh báo cáo của trường.

Bảng 6.2. Gợi ý lồng ghép nội dung tương tác an toàn theo khối lớp

6.3. Nghiên cứu trường hợp: giáo viên xử lý sự cố và phối hợp với cha mẹ học sinh

Trường hợp 1. Bắt nạt trực tuyến trong nhóm lớp (THCS)

Mô tả: Cô Lan, GVCN lớp 7, nhận được tin nhắn ẩn danh qua hộp thư của lớp: một nhóm học sinh lập nhóm chat riêng, gắn biệt danh chế giễu và đăng ảnh chỉnh sửa của bạn H. Cô quan sát thấy H gần đây hay ngồi một mình, xin nghỉ hai buổi. Cô gặp riêng H; ban đầu H phủ nhận, sau đó khóc và kể lại. H xin cô đừng nói với ai vì "sẽ bị các bạn ghét hơn".

Câu hỏi phân tích: (1) Cô Lan đã làm đúng những gì? (2) Cô nên trả lời đề nghị của H thế nào? (3) Kế hoạch xử lý tiếp theo?

Phân tích, gợi ý: (1) Cô Lan tiếp nhận nghiêm túc thông tin ẩn danh, kết hợp quan sát dấu hiệu, gặp riêng học sinh – phù hợp mục 4.2, 4.3. (2) Cô ghi nhận nỗi lo của H, không hứa giữ bí mật tuyệt đối; giải thích cô sẽ xử lý khéo léo để bảo vệ H, cùng H bàn cách làm. (3) Sự việc ở mức vàng: báo đầu mối nhà trường; hướng dẫn H lưu bằng chứng (hoặc nhờ cha mẹ hỗ trợ); thông báo trực tiếp cho cha mẹ H; làm việc riêng với từng học sinh trong nhóm, yêu cầu xóa nội dung, giáo dục về tác hại; thông báo cho cha mẹ các học sinh liên quan; tổ chức hoạt động giáo dục chung cho cả lớp về vai trò người chứng kiến mà không nêu tên vụ việc; theo dõi H trong các tuần tiếp theo, phối hợp người làm tư vấn học đường.

Trường hợp 2. Học sinh bị lừa chuyển tiền (THPT)

Mô tả: Học sinh K, lớp 11, nhận việc "làm nhiệm vụ đánh giá sản phẩm" qua ứng dụng nhắn tin. Ban đầu K nhận được hoa hồng nhỏ, sau đó được yêu cầu nạp tiền để nhận nhiệm vụ lớn. K đã dùng tiền học phí của gia đình và vay bạn tổng cộng 12 triệu đồng, hiện không rút lại được. K hoảng loạn, nói với thầy chủ nhiệm: "Bố mẹ em mà biết thì em chết mất."

Câu hỏi phân tích: (1) Mức độ sự việc? (2) Thầy chủ nhiệm cần ưu tiên làm gì? (3) Thông báo cho gia đình thế nào?

Phân tích, gợi ý: (1) Mức vàng về thiệt hại tài sản, nhưng câu nói của K cần được đánh giá như một dấu hiệu khủng hoảng – thầy cần hỏi trực tiếp, bình tĩnh về ý nghĩ tự gây hại; nếu có, chuyển sang mức đỏ. (2) Trấn an, khẳng định đây là thủ đoạn lừa đảo có tổ chức nhắm vào cả người lớn; K không nạp thêm tiền, không xóa tin nhắn; báo Ban Giám hiệu. (3) Thầy cùng K chuẩn bị nội dung, cùng có mặt khi thông báo cho cha mẹ; nhấn mạnh K là nạn nhân, nhu cầu được hỗ trợ; hướng dẫn gia đình liên hệ ngân hàng, trình báo công an; thống nhất cách gia đình ứng xử để K không bị áp lực quá mức; theo dõi tâm lý K; cảnh báo thủ đoạn cho toàn trường (không nêu tên học sinh).

Trường hợp 3. Cha mẹ học sinh phản ánh con bị người lạ nhắn tin (Tiểu học)

Mô tả: Mẹ của học sinh lớp 4 nhắn tin cho GVCN: phát hiện con dùng điện thoại của mẹ chơi game, có một tài khoản lạ thường nhắn tin khen con, hứa tặng thẻ game nếu con gửi ảnh "mặc đồ ngủ". Con chưa gửi. Người mẹ hỏi cô có nên đăng thông tin tài khoản này lên nhóm cha mẹ học sinh của lớp để cảnh báo không.

Câu hỏi phân tích: (1) Đánh giá mức độ? (2) Cô giáo tư vấn cho cha mẹ học sinh thế nào? (3) Nhà trường cần làm gì?

Phân tích, gợi ý: (1) Đây là dấu hiệu dụ dỗ trực tuyến có mục đích tình dục, cần xử lý ở mức đỏ dù con chưa gửi ảnh. (2) Cảm ơn và ghi nhận sự quan tâm của người mẹ; hướng dẫn không xóa tin nhắn, chụp lại tên tài khoản, nội dung; ngừng liên lạc với tài khoản; không tự nhắn tin với đối tượng; khen ngợi con vì đã không gửi ảnh, trò chuyện nhẹ nhàng, không làm con sợ hãi; trình báo cơ quan công an, có thể liên hệ Tổng đài 111 (Tổng đài Quốc gia Bảo vệ Trẻ em, Cục Bà mẹ và Trẻ em) để được tư vấn; báo cáo tài khoản với nền tảng trò chơi. Không đăng thông tin cụ thể lên nhóm cha mẹ học sinh vì có thể làm lộ thông tin của học sinh và ảnh hưởng đến việc xử lý của cơ quan chức năng. (3) Báo Ban Giám hiệu; nhà trường

gửi cảnh báo chung về thủ đoạn dụ dỗ qua trò chơi đến cha mẹ học sinh (không nêu tên, không nêu tài khoản cụ thể); tổ chức hoạt động giáo dục phòng ngừa cho học sinh khối 4, 5.

HOẠT ĐỘNG TẬP HUẤN

Hoạt động 6.1. Thiết kế và trình bày kế hoạch hoạt động (90 phút)
Học viên làm việc theo nhóm cùng cấp học, lựa chọn một nguy cơ trong Chuyên đề 2 chưa có kế hoạch mẫu (ví dụ: bắt nạt trực tuyến ở THCS; cờ bạc trực tuyến ở THPT; sử dụng thiết bị hợp lý ở Tiểu học), thiết kế một kế hoạch hoạt động 35 – 45 phút theo cấu trúc: yêu cầu cần đạt; chuẩn bị; tiến trình theo chu trình trải nghiệm; đánh giá; nhiệm vụ phối hợp với gia đình. Mỗi nhóm trình bày 7 phút; các nhóm góp ý theo tiêu chí ở Hoạt động 3.2.
Gợi ý: Báo cáo viên lưu ý các nhóm: tình huống phải gần gũi; học sinh được thực hành, không chỉ nghe; thông điệp không gây sợ hãi; có công cụ đánh giá hành vi; có kết nối với gia đình; dự kiến cách xử lý nếu có học sinh tiết lộ sự cố trong giờ học.

Hoạt động 6.2. Phân tích trường hợp (30 phút)
Mỗi nhóm phân tích một trường hợp ở mục 6.3 trước khi đọc phần gợi ý, sau đó so sánh với phần gợi ý và bổ sung.
Gợi ý: Báo cáo viên hướng học viên đối chiếu với quy trình 7 bước và phân loại mức độ ở Chuyên đề 4; chú ý các chi tiết thường bị bỏ qua: đánh giá nguy cơ tự gây hại, bảo mật danh tính học sinh, cách thông báo cho cha mẹ.

GHI NHỚ

– Kế hoạch hoạt động mẫu được thiết kế theo chu trình trải nghiệm, có đánh giá hành vi và nhiệm vụ phối hợp với gia đình.

– Lồng ghép ngắn, thường xuyên trong môn học và sinh hoạt lớp hiệu quả hơn tổ chức một lần theo phong trào.

– Mọi hoạt động về chủ đề nhạy cảm cần được chuẩn bị phương án hỗ trợ học sinh tiết lộ sự cố.

CÂU HỎI TỰ ĐÁNH GIÁ

1. Phân tích cách kế hoạch mẫu 6.1.3 vận dụng chu trình học tập trải nghiệm bốn bước.

2. Lựa chọn một bài học trong môn thầy cô giảng dạy và đề xuất một hoạt động lồng ghép 10 phút.

3. Trong Trường hợp 2, vì sao câu nói "Bố mẹ em mà biết thì em chết mất" cần được đánh giá nghiêm túc?

TÀI LIỆU THAM KHẢO

A. Văn bản quy phạm pháp luật, văn bản chỉ đạo

Bộ Giáo dục và Đào tạo (2018). Thông tư số 32/2018/TT-BGDĐT ban hành Chương trình giáo dục phổ thông.

Bộ Giáo dục và Đào tạo (2019). Thông tư số 06/2019/TT-BGDĐT quy định Quy tắc ứng xử trong cơ sở giáo dục mầm non, cơ sở giáo dục phổ thông, cơ sở giáo dục thường xuyên.

Bộ Giáo dục và Đào tạo (2025). Thông tư số 02/2025/TT-BGDĐT quy định Khung năng lực số cho người học.

Bộ Giáo dục và Đào tạo (2025). Thông tư số 18/2025/TT-BGDĐT hướng dẫn về công tác tư vấn học đường và công tác xã hội trong trường học.

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

Chính phủ (2017). Nghị định số 80/2017/NĐ-CP quy định về môi trường giáo dục an toàn, lành mạnh, thân thiện, phòng, chống bạo lực học đường.

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

Quốc hội (2015). Bộ luật Hình sự số 100/2015/QH13 (sửa đổi, bổ sung năm 2017 và các năm tiếp theo).

Quốc hội (2016). Luật Trẻ em số 102/2016/QH13.

Quốc hội (2025). Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15.

Quốc hội (2025). Luật An ninh mạng số 116/2025/QH15.

Thủ tướng Chính phủ (2026). Quyết định số 468/QĐ-TTg ngày 23/3/2026 phê duyệt Chương trình "Bảo vệ và hỗ trợ trẻ em phát triển trên môi trường mạng giai đoạn 2026 – 2030".

B. Tài liệu tiếng Việt

Hồ Văn Dũng (2020). Thực trạng sử dụng và nghiện Internet của học sinh trung học cơ sở thành phố Huế. Tạp chí Khoa học – Trường Đại học Sư phạm Hà Nội: Khoa học Giáo dục, 65(1), tr. 103.

Phan Diệu Mai (2024). Một số vấn đề về nghiện Internet ở thanh thiếu niên. Tạp chí Giáo dục, 24(Số đặc biệt 12), 287–293.

Trương Thanh Long, Tô Thị Minh Tâm (2024). Bắt nạt trực tuyến ở học sinh trung học cơ sở: Tổng quan các nghiên cứu trên thế giới và Việt Nam. Tạp chí Khoa học Trường Đại học Quy Nhơn, 18(2).

C. Tài liệu tiếng Anh

Bronfenbrenner, U. (1979). The ecology of human development: Experiments by nature and design. Harvard University Press.

Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753–1820.

ECPAT, INTERPOL, & UNICEF (2022). Disrupting Harm in Viet Nam: Evidence on online child sexual exploitation and abuse. Global Partnership to End Violence against Children.

Elkind, D. (1967). Egocentrism in adolescence. Child Development, 38(4), 1025–1034.

Epstein, J. L. (2011). School, family, and community partnerships: Preparing educators and improving schools (2nd ed.). Westview Press.

Erikson, E. H. (1968). Identity: Youth and crisis. W. W. Norton.

Inhelder, B., & Piaget, J. (1958). The growth of logical thinking from childhood to adolescence, The International Library of Psychology.

Kolb, D. A. (1984). Experiential learning: Experience as the source of learning and development. Prentice Hall.

Konrad, K., Firk, C., & Uhlhaas, P. J. (2013). Brain development during adolescence: Neuroscientific insights into this developmental period. Deutsches Ärzteblatt International, 110(25), 425–431.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. Psychological Bulletin, 140(4), 1073–1137.

Livingstone, S., & Helsper, E. J. (2008). Parental mediation of children's internet use. Journal of Broadcasting & Electronic Media, 52(4), 581–599.

Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying online risk to children. CO:RE Short Report Series on Key Topics. Leibniz-Institut für Medienforschung | Hans-Bredow-Institut. https://doi.org/10.21241/ssoar.71817

Madigan, S., Ly, A., Rash, C. L., Van Ouytsel, J., & Temple, J. R. (2018). Prevalence of multiple forms of sexting behavior among youth: A systematic review and meta-analysis. JAMA Pediatrics, 172(4), 327–335.

Odgers, C. L., & Jensen, M. R. (2020). Annual Research Review: Adolescent mental health in the digital age: Facts, fears, and future directions. Journal of Child Psychology and Psychiatry, 61(3), 336–348.

OECD (2021). Children in the digital environment: Revised typology of risks. OECD Digital Economy Papers, No. 302. OECD Publishing.

Orben, A., & Przybylski, A. K. (2019). The association between adolescent well-being and digital technology use. Nature Human Behaviour, 3(2), 173–182.

Praesidio Safeguarding (2021). Exploring effective prevention education responses to dangerous online challenges.

Saleh, F. M., Grudzinskas, A., & Judge, A. (Eds.) (2014). Adolescent sexual behavior in the digital age: Considerations for clinicians, legal professionals, and educators. Oxford University Press.

SAMHSA (2014). SAMHSA's concept of trauma and guidance for a trauma-informed approach. HHS Publication No. (SMA) 14-4884. Substance Abuse and Mental Health Services Administration.

Steinberg, L. (2008). A social neuroscience perspective on adolescent risk-taking. Developmental Review, 28(1), 78–106.

Suler, J. (2004). The online disinhibition effect. CyberPsychology & Behavior, 7(3), 321–326.

UNICEF (2019). UNICEF poll: More than a third of young people in 30 countries report being a victim of online bullying. UNICEF.

UNICEF (2021). Policy guidance on AI for children (Version 2.0). UNICEF.

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. Science, 359(6380), 1146–1151.

Webster, S., Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T., & Grove-Hills, J. (2012). European Online Grooming Project: Final report. European Commission Safer Internet Plus Programme.

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. Aggression and Violent Behavior, 18(1), 62–70.

Wineburg, S., & McGrew, S. (2019). Lateral reading and the nature of expertise: Reading less and learning more when evaluating digital information. Teachers College Record, 121(11).

World Health Organization (2014). Preventing suicide: A global imperative. WHO.

World Health Organization (2019). International Classification of Diseases, 11th Revision (ICD-11): 6C51 Gaming disorder. WHO.

World Health Organization, War Trauma Foundation, & World Vision International (2011). Psychological first aid: Guide for field workers. WHO.

Zendle, D., & Cairns, P. (2018). Video game loot boxes are linked to problem gambling: Results of a large-scale survey. PLoS ONE, 13(11), e0206767.

PHỤ LỤC

Phụ lục 1. Phiếu khảo sát trước và sau tập huấn

(Dùng chung cho khảo sát đầu vào và cuối khóa; học viên không ghi tên, chỉ ghi mã số để đối chiếu)

Mã số học viên: …… Cấp học giảng dạy: ☐ Tiểu học ☐ THCS ☐ THPT. Vai trò: ☐ GVCN ☐ GV bộ môn ☐ Tư vấn học đường ☐ CBQL ☐ Khác

Phần A. Tự đánh giá năng lực (1 – Rất thấp; 2 – Thấp; 3 – Trung bình; 4 – Khá; 5 – Cao)

TT	Nội dung	1	2	3	4	5
A1	Hiểu đặc điểm tâm sinh lý của học sinh ảnh hưởng đến hành vi trực tuyến					
A2	Nắm được quy định pháp luật về bảo vệ trẻ em trên môi trường mạng và trách nhiệm của giáo viên					
A3	Nhận diện được các nguy cơ trực tuyến phổ biến (lừa đảo, dữ liệu cá nhân, sử dụng quá mức, tin giả, cờ bạc, AI, bắt nạt, xâm hại, sức khỏe tinh thần)					
A4	Thiết kế, tổ chức được hoạt động giáo dục kỹ năng tương tác an toàn qua môn học, HĐTN, HN, sinh hoạt lớp					
A5	Nhận biết được dấu hiệu học sinh đang gặp sự cố, khủng hoảng					
A6	Tiếp nhận được chia sẻ, tiết lộ của học sinh một cách phù hợp					

TT	Nội dung	1	2	3	4	5
A7	Thực hiện được hỗ trợ tâm lý ban đầu					
A8	Xử lý được sự cố theo quy trình; biết chuyển gửi đúng nơi					
A9	Phối hợp được với cha mẹ học sinh khi xảy ra sự cố					
A10	Đánh giá được kết quả giáo dục theo hướng hành vi					

Phần B. Câu hỏi kiến thức (chọn một đáp án đúng nhất)

B1. Khung 4C phân loại nguy cơ trực tuyến gồm:

a) Nội dung – Tiếp xúc – Hành vi – Hợp đồng;

b) Nội dung – Công nghệ – Cộng đồng – Chi phí;

c) Tiếp xúc – Kiểm soát – Hợp tác – Cam kết.

B2. Khi học sinh xin giáo viên hứa giữ bí mật trước khi kể, giáo viên nên:

a) Hứa để học sinh yên tâm kể;

b) Giải thích trung thực rằng sẽ chỉ chia sẻ với người cần biết để giúp em an toàn;

c) Từ chối nghe nếu học sinh không đồng ý cho báo cáo.

B3. Học sinh bị tống tiền bằng hình ảnh nhạy cảm, giáo viên hướng dẫn học sinh:

a) Xóa ngay tài khoản;

b) Chuyển tiền để đối tượng xóa ảnh;

c) Không gửi thêm, không trả tiền, không xóa tin nhắn, kể với người lớn và báo cơ quan chức năng.

B4. Theo Luật Bảo vệ dữ liệu cá nhân năm 2025, công khai thông tin đời sống riêng tư của học sinh từ đủ 07 tuổi cần:

a) Đồng ý của nhà trường;

b) Đồng ý của học sinh và người đại diện theo pháp luật;

c) Không cần đồng ý nếu vì mục đích giáo dục.

B5. Theo Nghị định 147/2024/NĐ-CP, tài khoản trò chơi điện tử của người dưới 16 tuổi:

a) Do học sinh tự đăng ký;

b) Do cha, mẹ hoặc người giám hộ đăng ký;

c) Do nhà trường đăng ký.

B6. Câu hỏi trực tiếp về ý nghĩ tự sát đối với học sinh có dấu hiệu khủng hoảng:

a) Làm tăng nguy cơ, cần tránh;

b) Không làm tăng nguy cơ và giúp học sinh được hỗ trợ;

c) Chỉ bác sĩ mới được hỏi.

Phần C. Câu hỏi mở

C1. Điều thầy cô lo lắng nhất khi phải hỗ trợ học sinh gặp sự cố trên mạng là gì?

C2. (Chỉ trả lời ở khảo sát cuối khóa) Một việc cụ thể thầy cô sẽ thực hiện trong tháng tới sau tập huấn.

Đáp án phần B: B1 – a; B2 – b; B3 – c; B4 – b; B5 – b; B6 – b.

Phụ lục 2. Phiếu ghi nhận sự việc

(Chỉ người có trách nhiệm được tiếp cận)

Mục	**Nội dung ghi chép**
1. Thời gian, địa điểm tiếp nhận	
2. Người tiếp nhận (họ tên, chức vụ)	
3. Học sinh liên quan (họ tên, lớp)	
4. Cách thức phát hiện	☐ Học sinh tự kể ☐ Bạn bè báo ☐ Cha mẹ báo ☐ Giáo viên quan sát ☐ Kênh ẩn danh ☐ Khác
5. Loại sự việc	☐ Bắt nạt ☐ Lừa đảo/mất tài khoản ☐ Lộ thông tin ☐ Xâm hại/tống tiền tình dục ☐ Nội dung giả mạo AI ☐ Khủng hoảng tâm lý ☐ Sử dụng quá mức ☐ Khác
6. Mức độ đánh giá ban đầu	☐ Xanh ☐ Vàng ☐ Đỏ
7. Mô tả sự việc theo lời kể của học sinh (ghi nguyên văn các câu quan trọng)	
8. Quan sát của giáo viên về trạng thái học sinh	
9. Thông tin chứng cứ đã được ghi nhận (tên tài khoản, đường dẫn, thời gian – KHÔNG lưu hình ảnh nhạy cảm)	
10. Những việc đã làm ngay	
11. Đã báo cáo cho (họ tên, thời gian)	

Mục	Nội dung ghi chép
12. Đã thông báo cha mẹ học sinh (thời gian, hình thức, người thông báo)	
13. Chuyển gửi (đơn vị, thời gian)	
14. Kế hoạch theo dõi, hỗ trợ	
15. Chữ ký người ghi, ngày ghi	

Phụ lục 3. Quy trình xử lý sự cố trực tuyến của học sinh

Bước	Nội dung	Người thực hiện	Thời hạn
1. Tiếp nhận	Lắng nghe, ghi nhận; xác định sơ bộ mức độ	Giáo viên tiếp nhận	Ngay khi phát hiện
2. An toàn tức thời	Ngăn nguy hiểm trước mắt; không để học sinh một mình (mức đỏ); gọi 113, 115 khi cần	Giáo viên tiếp nhận, Ban Giám hiệu	Ngay lập tức
3. Bảo toàn chứng cứ	Không xóa; ghi nhận tài khoản, đường dẫn, thời gian; không lưu hình ảnh nhạy cảm	Học sinh, cha mẹ học sinh dưới sự hướng dẫn của giáo viên	Trong ngày
4. Báo cáo nhà trường	Báo đầu mối được phân công; mức đỏ báo Hiệu trưởng	Giáo viên tiếp nhận	Mức đỏ: ngay; mức vàng: trong ngày
5. Phối hợp cha mẹ	Thông báo trực tiếp, hướng dẫn hỗ trợ con (trừ trường hợp nghi người gây hại trong gia đình)	GVCN, Ban Giám hiệu	Mức đỏ: ngay; mức vàng: trong ngày
6. Chuyển gửi	Tư vấn học đường, y tế, công an, Tổng đài 111 (Tổng đài Quốc gia Bảo vệ Trẻ em, Cục Bà mẹ và Trẻ em), nền tảng số	Đầu mối nhà trường	Theo mức độ
7. Theo dõi, hỗ trợ	Kế hoạch hỗ trợ cá nhân; xử lý giáo dục học sinh gây hại; rút kinh nghiệm	GVCN, tư vấn học đường, Ban Giám hiệu	Định kỳ hằng tuần trong ít nhất 1 tháng

Phụ lục 4. Danh bạ đầu mối hỗ trợ

(Nhà trường điền thông tin cụ thể và niêm yết tại phòng giáo viên, phòng tư vấn)

Đầu mối	**Số điện thoại, địa chỉ**
Tổng đài Quốc gia Bảo vệ Trẻ em, Cục Bà mẹ và Trẻ em	111 (miễn phí, 24/7)
Cảnh sát	113
Cấp cứu	115
Hiệu trưởng	
Phó Hiệu trưởng phụ trách công tác học sinh	
Người làm công tác tư vấn học đường, công tác xã hội của trường	
Công an xã, phường nơi trường đóng	
Trạm y tế, bệnh viện gần nhất	
Cơ sở khám, điều trị sức khỏe tâm thần trên địa bàn	
Cán bộ phụ trách bảo vệ trẻ em cấp xã, phường	

Phụ lục 5. Mẫu thỏa thuận sử dụng thiết bị số trong gia đình

THỎA THUẬN SỬ DỤNG THIẾT BỊ SỐ CỦA GIA ĐÌNH ……

Chúng tôi – cha mẹ và con – cùng thống nhất:

1. **Thời gian:** Ngày học, con sử dụng thiết bị để giải trí không quá …… phút; cuối tuần không quá …… phút. Không sử dụng thiết bị sau …… giờ tối.

2. **Không gian không thiết bị:** bữa ăn gia đình; phòng ngủ vào ban đêm (thiết bị được sạc ở ……).

3. **Ứng dụng, trò chơi:** con sử dụng các ứng dụng, trò chơi phù hợp lứa tuổi đã được cha mẹ đồng ý: ……; cài ứng dụng mới cần hỏi ý kiến cha mẹ.

4. **Bảo vệ thông tin:** con không chia sẻ mật khẩu, mã OTP, địa chỉ nhà, trường học, số điện thoại với người chưa quen biết ngoài đời; cha mẹ xin phép con trước khi đăng ảnh của con.

5. **Kết bạn và gặp mặt:** con không gặp mặt người chỉ quen qua mạng khi chưa có sự đồng ý và đi cùng của cha mẹ.

6. **Tiền và giao dịch:** con không nạp tiền, mua vật phẩm, chuyển tiền khi chưa hỏi ý kiến cha mẹ.

7. **Khi gặp chuyện không an toàn:** con sẽ kể với cha mẹ hoặc thầy cô. **Cha mẹ cam kết lắng nghe, giúp con và không la mắng, không tịch thu thiết bị vì con đã kể.**

8. **Câu hỏi bí mật của gia đình** (để kiểm chứng khi có cuộc gọi khẩn cấp): ……

9. Thỏa thuận được xem xét lại sau …… tháng.

Chữ ký của con …… Chữ ký của cha mẹ ……

Phụ lục 6. Phiếu học tập cho học sinh

Phiếu 6.1. "Đèn giao thông an toàn" (Tiểu học)

Hướng dẫn: Đọc từng tình huống và đánh dấu vào một trong ba mức: XANH – có thể làm; VÀNG – cần suy nghĩ, hỏi người lớn; ĐỎ – không được làm.

STT	Tình huống	XANH	VÀNG	ĐỎ
1	Đăng bức tranh em tự vẽ lên nhóm lớp.	☐	☐	☐
2	Gửi mật khẩu tài khoản cho bạn thân.	☐	☐	☐
3	Chia sẻ địa chỉ nhà trên mạng xã hội.	☐	☐	☐
4	Đăng ảnh của bạn khi chưa xin phép.	☐	☐	☐
5	Bấm vào đường link lạ để nhận quà.	☐	☐	☐
6	Hỏi ý kiến bố mẹ trước khi tham gia một nhóm lạ.	☐	☐	☐
7	Trả lời tin nhắn của người lạ hỏi số điện thoại.	☐	☐	☐
8	Bình luận động viên bạn trên mạng.	☐	☐	☐
9	Báo với thầy cô, bố mẹ khi thấy nội dung đáng sợ.	☐	☐	☐
10	Chia sẻ mã OTP cho người khác.	☐	☐	☐

Gợi ý đáp án: 1 – Xanh; 2 – Đỏ; 3 – Đỏ; 4 – Đỏ; 5 – Đỏ; 6 – Xanh; 7 – Đỏ; 8 – Xanh; 9 – Xanh; 10 – Đỏ.

Phiếu 6.2. "Thám tử mạng" (THCS)

Với mỗi tin nhắn, em hãy: (1) đánh dấu tin nhắn là ☐ An toàn ☐ Đáng ngờ ☐ Lừa đảo; (2) gạch chân các dấu hiệu nghi vấn; (3) viết cách em sẽ xử lý.

Dấu hiệu	Có trong tin nhắn số
Lợi ích quá tốt để là thật	
Hối thúc làm ngay	

Dấu hiệu	Có trong tin nhắn số
Đe dọa, gây sợ hãi	
Yêu cầu giữ bí mật	
Yêu cầu mật khẩu, OTP, tiền, bấm link lạ	

Phiếu 6.3. Phiếu kiểm chứng thông tin (THPT)

Câu hỏi kiểm chứng	Ghi chép của nhóm
1. Ai đăng? Tìm thông tin về nguồn này ở các trang khác (đọc ngang).	
2. Bằng chứng nào được đưa ra? Có kiểm tra được không?	
3. Các nguồn chính thống, nguồn độc lập nói gì?	
4. Hình ảnh, video có dấu hiệu chỉnh sửa hoặc do AI tạo không? (tìm kiếm ngược hình ảnh, chi tiết bất thường)	
5. Kết luận: ☐ Đáng tin ☐ Chưa đủ căn cứ ☐ Sai lệch. Quyết định: ☐ Chia sẻ ☐ Không chia sẻ ☐ Báo cáo	

Phụ lục 7. Gợi ý đáp án câu hỏi tự đánh giá

Chuyên đề 1

1. Ba thành tố: nhận thức, thái độ, hành vi. Đánh giá cần hướng vào hành vi vì mục tiêu cuối cùng là học sinh thực hiện và duy trì được hành vi an toàn; học sinh có thể biết nhưng chưa làm được.

2. Vỏ não trước trán (kiểm soát xung động, đánh giá rủi ro) phát triển muộn, trong khi hệ thống cảm xúc, tưởng thưởng hoạt động mạnh từ tuổi dậy thì; ảnh hưởng của bạn bè và triển vọng phần thưởng (lượt thích, sự công nhận) chi phối mạnh quyết định.

3. Cần có sự đồng ý của học sinh và người đại diện theo pháp luật (Điều 24 Luật Bảo vệ dữ liệu cá nhân năm 2025).

4. Ví dụ: tự điều tra, đối chất; hứa giữ bí mật tuyệt đối; công khai thông tin học sinh; tiếp nhận, lưu giữ hình ảnh nhạy cảm; đổ lỗi cho nạn nhân.

Chuyên đề 2

1. Nội dung – học sinh tiếp nhận nội dung có hại; Tiếp xúc – học sinh bị người khác tiếp cận; Hành vi – học sinh tham gia hoặc gây ra hành vi rủi ro; Hợp đồng – học sinh bị khai thác về tài chính, dữ liệu. Ví dụ tùy cấp học.

2. Đối tượng giả danh công an, viện kiểm sát, tòa án, đe dọa học sinh liên quan vụ án, yêu cầu giữ bí mật, cô lập học sinh, ép quay video để tống tiền gia đình. Dấu hiệu: làm việc qua điện thoại, mạng xã hội; đe dọa, hối thúc; yêu cầu giữ bí mật, cắt liên lạc với gia đình, chuyển tiền.

3. "Sử dụng nhiều" chỉ thời lượng; "sử dụng có vấn đề" khi suy giảm khả năng kiểm soát, ưu tiên hơn các hoạt động khác, tiếp tục dù có hậu quả tiêu cực, gây suy giảm chức năng.

4. Vì có thể khơi gợi tò mò khiến học sinh tìm kiếm, làm theo; một số thử thách là tin đồn được thổi phồng; nên giáo dục năng lực đánh giá rủi ro chung.

5. Lựa chọn mục tiêu – xây dựng lòng tin – tạo phụ thuộc, cô lập – bình thường hóa nội dung tình dục – xâm hại, kiểm soát; dấu hiệu tương ứng theo Bảng 2.2 và mục 2.9.4.

Chuyên đề 3

1. Vì khi các kỹ năng tự bảo vệ chưa đủ, việc học sinh tìm đến người lớn giúp ngăn tổn hại tiếp diễn và được hỗ trợ kịp thời.

2. Trải nghiệm – Phản hồi – Khái quát hóa – Vận dụng; ví dụ theo kế hoạch mẫu 6.1.2.

3. Thông báo trước; dùng tình huống "nhân vật thứ ba"; không dùng hình ảnh nhạy cảm, không mô tả chi tiết; chuẩn bị phương án hỗ trợ khi học sinh tiết lộ.

4. Ví dụ: “Học sinh có tạo được mật khẩu dài từ 12 ký tự trở lên, không chứa thông tin cá nhân không?”; “Học sinh có nêu được bước bật xác thực hai yếu tố không?”.

Chuyên đề 4

1. Phát hiện, tiếp nhận, hỗ trợ ban đầu, báo cáo – kết nối, đồng hành – theo dõi. Ngoài phạm vi: điều tra, đàm phán với đối tượng, “giải quyết nội bộ” vụ việc có dấu hiệu vi phạm pháp luật, chẩn đoán.

2. Vì giáo viên có trách nhiệm báo cáo để bảo đảm an toàn; hứa rồi phá vỡ lời hứa làm mất lòng tin. Trả lời theo mục 4.3.4.

3. Quan sát – Lắng nghe – Kết nối.

4. Làm: dừng liên lạc, lưu thông tin (không xóa), kể với người lớn, báo cơ quan chức năng. Không làm: gửi thêm hình ảnh, chuyển tiền, gặp mặt, tự xóa tài khoản.

5. Tiếp nhận – An toàn tức thời – Bảo toàn chứng cứ – Báo cáo nhà trường – Phối hợp cha mẹ – Chuyển tiếp hỗ trợ – Theo dõi, hỗ trợ.

Chuyên đề 5

1. Phối hợp xây dựng kế hoạch; tổ chức hoạt động; trao đổi thông tin; kiểm tra, đánh giá.

2. Vì vừa giảm rủi ro vừa phát triển kỹ năng, duy trì kênh trò chuyện, giúp học sinh sẵn sàng kể khi gặp sự cố; cấm đoán đơn thuần làm giảm cơ hội học kỹ năng và khiến học sinh giấu giếm.

3. Theo mục 5.3.2.a.

4. Khi có căn cứ cho rằng người gây hại là thành viên gia đình hoặc việc thông báo có thể khiến học sinh gặp nguy hiểm; báo ngay Hiệu trưởng, cơ quan công an, Tổng đài 111 (Tổng đài Quốc gia Bảo vệ Trẻ em, Cục Bà mẹ và Trẻ em).

5. Theo mục 5.5.

Chuyên đề 6

1. Trải nghiệm (hoạt động 1, 2, 3) – Phản hồi (thảo luận, trình bày) – Khái quát hóa (giáo viên chốt dấu hiệu, quy trình 5 bước) – Vận dụng (thực hành 5 bước, cam kết).

2. Tùy môn học, tham khảo Bảng 6.2.

3. Vì có thể là dấu hiệu khủng hoảng, ý nghĩ tự gây hại; giáo viên cần hỏi trực tiếp, bình tĩnh và xử lý theo mục 4.6.6 nếu có nguy cơ.

Phụ lục 8. Mindmaps tóm tắt cho 6 chuyên đề




CHUYÊN ĐỀ 2
NHẬN DIỆN CÁC NGUY CƠ PHỔ BIẾN ĐỐI VỚI HỌC SINH TRÊN KHÔNG GIAN MẠNG
CÁC NGUY CƠ PHỔ BIẾN
1. Lừa đảo trực tuyến
Chiếm đoạt tài khoản
2. Lộ lọt dữ liệu cá nhân
Xâm phạm quyền riêng tư
3. Sử dụng thiết bị số quá mức
Nghiện game, mạng xã hội
4. Tin giả, nội dung xấu độc
Có hại
5. "Thử thách" nguy hiểm
Cờ bạc, cá cược trực tuyến
6. Nội dung AI tạo ra
Giả mạo, lừa đảo
7. Bắt nạt trực tuyến
(Cyberbullying)
8. Xâm hại, bóc lột tình dục trẻ em trực tuyến
9. Tác động đến sức khỏe tinh thần
10. Văn hóa ứng xử
Trên không gian mạng


CHUYÊN ĐỀ 3
GIÁO DỤC KỸ NĂNG TƯƠNG TÁC AN TOÀN TRÊN KHÔNG GIAN MẠNG CHO HỌC SINH
MỤC TIÊU & YÊU CẦU
Theo cấp học
Phù hợp lứa tuổi
Hình thành thói quen tốt
HỆ THỐNG KỸ NĂNG
Nhận thức
Ứng xử
Tự bảo vệ
Hợp tác, hỗ trợ
KỸ NĂNG TƯƠNG TÁC AN TOÀN TRÊN MẠNG
NGUYÊN TẮC
Lấy HS làm trung tâm
Phù hợp tâm lý lứa tuổi
Phù hợp pháp luật
HÌNH THỨC & CON ĐƯỜNG
Tích hợp môn học
Hoạt động trải nghiệm
Trực tuyến, ngoại khóa
PHƯƠNG PHÁP & KỸ THUẬT
Thảo luận, tình huống
Trò chơi, dự án
Phương pháp tích cực
ĐÁNH GIÁ KẾT QUẢ
Quan sát, sản phẩm
Tự đánh giá, đồng đẳng
Bộ tiêu chí rõ ràng


CHUYÊN ĐỀ 4
PHÁT HIỆN, HỖ TRỢ VÀ XỬ LÝ BAN ĐẦU KHI HỌC SINH GẶP SỰ CỐ TRÊN KHÔNG GIAN MẠNG
VAI TRÒ, PHẠM VI
Đồng hành, hỗ trợ
Không thay thế chuyên gia
Giữ giới hạn chuyên môn
NHẬN BIẾT DẤU HIỆU
Thay đổi tâm lý, hành vi
Sụt giảm học tập
Bất thường trên mạng
HỖ TRỢ & XỬ LÝ SỰ CỐ
TIẾP NHẬN CHIA SẺ
Lắng nghe, tôn trọng
Bảo mật thông tin
Không phán xét
HỖ TRỢ TÂM LÝ BAN ĐẦU
Trấn an, đồng hành
Kết nối chuyên gia
Tăng cường kỹ năng
QUY TRÌNH XỬ LÝ CHUNG
Đánh giá – Can thiệp – Theo dõi
Phối hợp các bên liên quan
XỬ LÝ THEO TỪNG LOẠI SỰ CỐ
Lừa đảo, xâm hại, bắt nạt...
Hướng dẫn, hỗ trợ cụ thể
GHI CHÉP, BẢO MẬT & ĐẦU MỐI
Lưu hồ sơ
Bảo mật thông tin
Liên hệ hỗ trợ
Giáo viên – Người đồng hành tin cậy của học sinh


CHUYÊN ĐỀ 5
PHỐI HỢP VỚI CHA MẸ HỌC SINH VÀ CÁC LỰC LƯỢNG TRONG HỖ TRỢ HỌC SINH TƯƠNG TÁC AN TOÀN TRÊN KHÔNG GIAN MẠNG
CHA MẸ HỌC SINH
Quan tâm, đồng hành
Giao tiếp thường xuyên
Làm gương, định hướng
NHÀ TRƯỜNG
Tổ chức giáo dục
Kết nối gia đình
Xây dựng môi trường an toàn
PHỐI HỢP ĐỒNG HÀNH
LỰC LƯỢNG XÃ HỘI
Cơ quan chức năng
Tổ chức đoàn thể
Doanh nghiệp, chuyên gia
PHỐI HỢP HIỆU QUẢ
Chia sẻ thông tin
Phân công trách nhiệm
Hành động thống nhất
Cùng chung tay vì môi trường mạng an toàn cho học sinh!


Mục tiêu
Sau khi học xong, thầy cô có thể:
Phân tích, vận dụng kế hoạch mẫu
Thiết kế hoạt động giáo dục an toàn trên mạng
Xử lý tình huống, phối hợp hiệu quả
Hướng dẫn sử dụng kế hoạch mẫu
Dựa trên chu trình học tập trải nghiệm (35 – 45 phút).
Linh hoạt: tiết HĐTN, sinh hoạt lớp hoặc tích hợp trong môn học.
Điều chỉnh tình huống gần gũi với HS.
CHUYÊN ĐỀ 6
Ví dụ minh họa và thực hành thiết kế hoạt động giáo dục
Tương tác an toàn trên không gian mạng
Danh mục kế hoạch mẫu
Tiểu học
Sử dụng mạng xã hội an toàn
THCS
Phòng tránh lừa đảo, bảo vệ tài khoản
THCS
Phòng tránh xâm hại trên không gian mạng
THPT
Tin giả, deepfake và nội dung do AI tạo ra
THPT
Dấu chân số, định hướng nghề nghiệp
THPT
Cân bằng đời sống số, sức khỏe tinh thần
Kế hoạch hoạt động mẫu (Cấp Tiểu học)
Chủ đề: Sử dụng mạng xã hội an toàn (35 phút, HĐTN, sinh hoạt lớp)
Yêu cầu cần đạt
Nhận diện rủi ro, biết cách xử lý
Thực hiện "Dừng lại – Hỏi người lớn"
Các hoạt động chính
Khởi động
Khám phá
Thực hành
Vận dụng
Quy trình thiết kế hoạt động
1 Xác định mục tiêu
2 Lựa chọn nội dung, tình huống
3 Thiết kế hoạt động phù hợp
4 Dự kiến phương pháp, phương tiện
5 Đánh giá kết quả
Một số lưu ý thực hành
Gần gũi, thực tế
Phát huy tính tích cực của HS
Kết nối gia đình – nhà trường
Lan tỏa thông điệp an toàn trên mạng
Cùng chung tay vì môi trường mạng an toàn cho học sinh!

Phụ lục 9. Các kênh hỗ trợ khi gặp sự cố

TT	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

STT	Thuật ngữ	Cách hiểu trong tài liệu
1	*AI – Artificial Intelligence (*Trí tuệ nhân tạo)	Trí tuệ nhân tạo là việc thực hiện bằng điện tử các năng lực trí tuệ của con người, bao gồm học tập, suy luận, nhận thức, phán đoán và hiểu ngôn ngữ tự nhiên.
2	Không gian mạng	"Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian".
3	Tương tác an toàn trên không gian mạng	Việc học sinh tham gia các hoạt động trên không gian mạng (tìm kiếm, tiếp nhận, tạo lập, chia sẻ thông tin; giao tiếp, kết bạn, vui chơi, giao dịch) theo cách bảo vệ được bản thân, tôn trọng người khác, tuân thủ pháp luật và biết tìm kiếm sự hỗ trợ khi cần.
4	Dấu chân số	Toàn bộ dấu vết mà một người để lại trên môi trường mạng (bài đăng, bình luận, hình ảnh, lịch sử tìm kiếm, dữ liệu vị trí…), có thể được lưu trữ, sao chép và truy xuất lâu dài. Dấu chân số không chỉ là thông tin người dùng chủ động chia sẻ mà còn bao gồm dữ liệu kỹ thuật thụ động bị thu thập ngầm: địa chỉ IP, nhận dạng thiết bị, cookies, hành vi di chuột, thông tin vị trí.
5	Dụ dỗ trực tuyến (grooming)	Quá trình một người từng bước làm quen, tạo lòng tin rồi gây áp lực hoặc lợi dụng học sinh.
6	Tống tiền tình dục (sextortion)	Hành vi đe dọa phát tán hình ảnh, video nhạy cảm (thật hoặc giả mạo) để ép buộc nạn nhân gửi thêm hình ảnh, tiền hoặc thực hiện yêu cầu khác.

STT	Thuật ngữ	Cách hiểu trong tài liệu
7	Deepfake	Nội dung được AI tạo hoặc chỉnh sửa để mô phỏng khuôn mặt, giọng nói hay hành động của người thật.
8	Lừa đảo giả mạo (phishing)	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.
9	Tiết lộ	Việc học sinh kể lại, chia sẻ (bằng lời hoặc không bằng lời, trực tiếp hoặc gián tiếp) về việc bản thân hoặc người khác đang gặp nguy cơ, bị tổn hại.
10	Chuyển tiếp hỗ trợ	Việc giới thiệu, kết nối học sinh với dịch vụ, cơ quan có chức năng hỗ trợ chuyên sâu (tư vấn tâm lý, y tế, công an, dịch vụ bảo vệ trẻ em) theo quy định.
11	Khung 4C	Bốn nhóm rủi ro trên mạng: cách phân loại rủi ro trẻ em gặp trên mạng thành Nội dung – Tiếp xúc – Hành vi – Hợp đồng.