

Số: 6206 /BGDĐT-GDPT

V/v hướng dẫn triển khai thực hiện giáo
dục an toàn mạng toàn diện trong các cơ
sở giáo dục phổ thông năm học 2026-2027

Hà Nội, ngày 14 tháng 09 năm 2026

Kính gửi: Các Sở Giáo dục và Đào tạo

Thực hiện Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia; Kế hoạch số 04-KH/BCĐTW ngày 05/01/2026 của Ban Chỉ đạo Trung ương về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị; Thông tư số 02/2025/TT-BGDĐT ngày 24/01/2025 của Bộ Giáo dục và Đào tạo (GDĐT) quy định Khung năng lực số cho người học, Bộ GDĐT hướng dẫn triển khai thực hiện giáo dục an toàn mạng toàn diện trong các cơ sở giáo dục phổ thông như sau:

I. MỤC ĐÍCH, YÊU CẦU

Giáo dục an toàn mạng toàn diện là quá trình giáo dục có hệ thống nhằm hình thành và phát triển ở học sinh năng lực sử dụng môi trường số an toàn, lành mạnh, có trách nhiệm và có đạo đức; biết bảo vệ bản thân, người khác và dữ liệu cá nhân; nhận diện, phòng ngừa, ứng phó với các nguy cơ trên mạng; tuân thủ pháp luật; duy trì sức khỏe thể chất, tinh thần; đồng thời khai thác hiệu quả môi trường số phục vụ học tập, giao tiếp và phát triển bản thân.

Thực hiện việc giáo dục an toàn mạng toàn diện trong các cơ sở giáo dục phổ thông nhằm các mục đích, yêu cầu sau đây:

1. Mục đích

a) Giúp học sinh sử dụng Internet, mạng xã hội, nền tảng học tập trực tuyến, dữ liệu số và công cụ trí tuệ nhân tạo (AI) một cách an toàn, lành mạnh, nhân văn và có trách nhiệm.

b) Hình thành, phát triển cho học sinh các năng lực thiết yếu của công dân số, gồm: nhận diện và phòng tránh rủi ro trên môi trường mạng; bảo vệ dữ liệu cá nhân, quyền riêng tư và danh tính số; giao tiếp, ứng xử văn minh; kiểm chứng thông tin; phòng tránh tin giả, lừa đảo trực tuyến, bắt nạt mạng; quản lý thời gian sử dụng thiết bị số; bảo vệ sức khỏe thể chất, tinh thần; sử dụng AI trong học tập và đời sống một cách trung thực, minh bạch, an toàn và có trách nhiệm.

c) Nâng cao trách nhiệm và năng lực phối hợp của nhà trường, giáo viên, cán bộ tư vấn học đường, cha mẹ học sinh và các lực lượng liên quan trong phòng ngừa, phát hiện, tiếp nhận, hỗ trợ ban đầu, xử lý và phục hồi sau sự cố trên môi trường số; góp phần xây dựng môi trường giáo dục số an toàn, lành mạnh và phù hợp với đặc điểm lứa tuổi học sinh phổ thông.

2. Yêu cầu

Việc tổ chức thực hiện giáo dục an toàn mạng cho học sinh phổ thông cần bảo đảm các yêu cầu sau:

a) Phù hợp với điều kiện thực tiễn của địa phương và cơ sở giáo dục; bảo đảm tính thiết thực, khả thi, hiệu quả.

b) Nội dung giáo dục an toàn mạng toàn diện được lồng ghép, tích hợp trong các môn học, hoạt động giáo dục và trong hệ thống kế hoạch, hồ sơ hiện hành của nhà trường, không làm phát sinh hồ sơ mới; không tổ chức thành môn học, tiết học riêng.

c) Lấy học sinh làm trung tâm; bảo đảm an toàn tâm lý, quyền riêng tư và bảo mật thông tin cá nhân của học sinh trong quá trình dạy học, khảo sát, đánh giá và hỗ trợ triển khai thực hiện.

d) Chú trọng thực hành, trải nghiệm, xử lý tình huống và tạo sản phẩm học tập; giúp học sinh biết nhận diện, phòng ngừa, ứng phó và tìm kiếm hỗ trợ khi gặp rủi ro trên môi trường số.

đ) Không biến giáo dục an toàn mạng toàn diện thành hoạt động tuyên truyền hình thức hoặc nội dung kỹ thuật chuyên sâu vượt quá yêu cầu của Chương trình giáo dục phổ thông.

e) Phát huy vai trò nòng cốt của môn Tin học trong cung cấp kiến thức nền tảng, kỹ năng số cốt lõi và nguyên tắc sử dụng công nghệ an toàn, có trách nhiệm; đồng thời khuyến khích lồng ghép/tích hợp nội dung giáo dục an toàn mạng toàn diện trong các môn học/hoạt động giáo dục khác và các lực lượng giáo dục trong nhà trường có trách nhiệm phối hợp thực hiện.

f) Tăng cường phối hợp giữa nhà trường, gia đình, cơ quan quản lý giáo dục, cơ quan chuyên môn, tổ chức bảo vệ trẻ em, cơ quan công an, y tế, đoàn thể, doanh nghiệp công nghệ và các lực lượng liên quan theo quy định của pháp luật.

II. NỘI DUNG, HÌNH THỨC TỔ CHỨC THỰC HIỆN

1. Nội dung giáo dục an toàn mạng toàn diện

Cơ sở giáo dục phổ thông lựa chọn, sắp xếp nội dung giáo dục an toàn mạng toàn diện phù hợp với cấp học, môn học, hoạt động giáo dục, điều kiện triển khai và đặc điểm tâm sinh lý học sinh. Trong đó, nội dung tập trung vào 08 chủ đề chính (*Chi tiết tại phụ lục*)

2. Xây dựng và thực hiện Kế hoạch giáo dục

Cơ sở giáo dục phổ thông xây dựng kế hoạch và thực hiện nội dung giáo dục an toàn mạng toàn diện, cụ thể như sau:

a) *Kế hoạch giáo dục nhà trường*: Nhà trường xây dựng và thực hiện kế hoạch giáo dục hằng năm gắn với phát triển năng lực số và giáo dục an toàn mạng toàn diện; xác định mục tiêu, nội dung, yêu cầu cần đạt theo cấp học, khối lớp và phân công trách nhiệm cụ thể. Nội dung được lồng ghép, tích hợp phù hợp trong các môn học, hoạt động giáo dục. Nhà trường từng bước bảo đảm học liệu số, hạ

tăng và nguồn lực; phối hợp với cha mẹ học sinh, cộng đồng để theo dõi, đánh giá kết quả và sự phát triển năng lực số, kỹ năng an toàn mạng của học sinh.

b) *Kế hoạch tổ chức dạy học môn học/hoạt động giáo dục*: rà soát yêu cầu cần đạt của môn học, hoạt động giáo dục để xác định nội dung tích hợp giáo dục an toàn mạng toàn diện và phát triển năng lực số; lựa chọn hoạt động học tập, tình huống thực hành phù hợp; xác định sản phẩm học tập, minh chứng đánh giá và biện pháp hỗ trợ học sinh trong quá trình thực hiện.

c) *Kế hoạch bài dạy*: Căn cứ nội dung của môn học/hoạt động giáo dục trong chương trình, xác định mục tiêu, yêu cầu cần đạt của nội dung giáo dục an toàn mạng toàn diện (nếu có) để lồng ghép, tích hợp vào quá trình tổ chức dạy học môn học; thiết kế hoạt động học tập, nhiệm vụ thực hành phù hợp; xác định sản phẩm học tập, minh chứng và tiêu chí đánh giá; lưu ý các yêu cầu về bảo vệ dữ liệu cá nhân và bảo đảm an toàn cho học sinh trong quá trình tổ chức dạy học.

d) *Quy tắc ứng xử số của nhà trường, lớp học*: Ban hành quy tắc ứng xử trên môi trường số, quy định việc sử dụng mạng xã hội trong nhà trường, nhóm trao đổi trực tuyến, chia sẻ thông tin và hình ảnh, bảo vệ dữ liệu cá nhân, sử dụng AI; đồng thời quy định trách nhiệm của người dạy, người học và quy trình báo cáo, xử lý các sự cố an toàn mạng.

đ) *Đánh giá định kỳ*: các cơ sở giáo dục tổ chức tự đánh giá hằng năm về mức độ triển khai, mức độ đạt được của học sinh về giáo dục an toàn mạng toàn diện, khó khăn, nhu cầu hỗ trợ; sử dụng kết quả để điều chỉnh kế hoạch giáo dục và báo cáo cơ quan quản lý.

3. Hình thức tổ chức

a) Tổ chức dạy học môn Tin học theo Chương trình giáo dục phổ thông; đồng thời tăng cường lồng ghép, tích hợp các nội dung về an toàn thông tin, bảo vệ dữ liệu cá nhân, đạo đức số, sử dụng công nghệ và AI an toàn, phù hợp với đặc điểm tâm sinh lý và yêu cầu cần đạt của môn học theo từng cấp học.

b) Lồng ghép nội dung giáo dục an toàn mạng toàn diện trong các môn học và hoạt động giáo dục có liên quan theo hướng phù hợp, thiết thực, tránh quá tải, khiên cưỡng hoặc hình thức.

c) Tổ chức hoạt động trải nghiệm, sinh hoạt lớp, sinh hoạt dưới cờ, diễn đàn học sinh, cuộc thi truyền thông, dự án nhỏ, câu lạc bộ công nghệ số, STEM/STEAM, AI, diễn tập xử lý tình huống số; hoạt động của buổi thứ hai đối với cơ sở giáo dục tổ chức dạy học 2 buổi/ngày; không tổ chức thêm ngoài kế hoạch giáo dục nhà trường đã được phê duyệt.

d) Triển khai tư vấn học đường và hỗ trợ cá nhân/nhóm đối với học sinh gặp rủi ro số; thiết lập kênh báo cáo thân thiện, bí mật, dễ tiếp cận; tổ chức hoạt động phục hồi, hỗ trợ tâm lý và phòng ngừa tái diễn.

đ) Phối hợp với gia đình học sinh để hướng dẫn quản lý thiết bị, dữ liệu, thời gian sử dụng Internet, sử dụng AI và xử lý khi con gặp sự cố số.

e) Khuyến khích xã hội hóa, hợp tác với cơ sở giáo dục đại học, cơ sở nghiên

cứu, doanh nghiệp công nghệ, chuyên gia an toàn thông tin, chuyên gia tâm lý, cơ quan công an, y tế, đoàn thể, tổ chức bảo vệ trẻ em theo các quy định của pháp luật.

III. TỔ CHỨC THỰC HIỆN

1. Các đơn vị thuộc Bộ Giáo dục và Đào tạo

a) Vụ Giáo dục Phổ thông

- Chủ trì tham mưu hướng dẫn việc triển khai giáo dục an toàn mạng toàn diện trong các cơ sở giáo dục phổ thông.

- Chủ trì theo dõi, hướng dẫn, kiểm tra, tổng hợp tình hình khó khăn, vướng mắc của địa phương, đơn vị; kịp thời tham mưu điều chỉnh, bổ sung nội dung triển khai phù hợp.

- Chủ trì xây dựng tài liệu hướng dẫn; tổ chức tập huấn cho cán bộ quản lý, giáo viên, cán bộ tư vấn học đường về Khung năng lực số và giáo dục an toàn mạng toàn diện.

b) Cục Khoa học, Công nghệ và Thông tin

- Chủ trì tham mưu xây dựng tiêu chí lựa chọn, rà soát và khuyến nghị nền tảng, công cụ hỗ trợ triển khai nội dung giáo dục AI đáp ứng yêu cầu an toàn thông tin, bảo vệ dữ liệu cá nhân, phù hợp lứa tuổi để các cơ sở giáo dục.

- Chủ trì hướng dẫn các yêu cầu kỹ thuật về bảo đảm an toàn thông tin, bảo vệ dữ liệu cá nhân, dữ liệu học sinh trong quá trình dạy học, quản lý và hỗ trợ học sinh.

- Chủ trì tham mưu các giải pháp bảo đảm an toàn thông tin cho hạ tầng số, nền tảng số, kho học liệu số dùng chung phục vụ triển khai nội dung giáo dục an toàn mạng toàn diện.

2. Sở Giáo dục và Đào tạo

- Ban hành kế hoạch triển khai phát triển năng lực số và giáo dục an toàn mạng toàn diện tại địa phương theo từng năm học, xác định rõ mục tiêu, nhiệm vụ, lộ trình, sản phẩm đầu ra, nguồn lực và trách nhiệm, cơ chế phối hợp của các đơn vị liên quan.

- Tham mưu Ủy ban nhân dân cấp tỉnh bố trí kinh phí, cơ sở vật chất, hạ tầng công nghệ thông tin và điều kiện bảo đảm an toàn thông tin; ưu tiên cơ sở giáo dục vùng khó khăn, vùng sâu, vùng xa, biên giới, hải đảo và nơi còn hạn chế về hạ tầng, thiết bị, đội ngũ.

- Chỉ đạo, hướng dẫn cơ sở giáo dục: rà soát thực trạng giáo dục năng lực số, an toàn mạng, bảo vệ dữ liệu cá nhân và bảo vệ học sinh trên môi trường số; đưa nội dung này vào kế hoạch giáo dục nhà trường phù hợp điều kiện thực tiễn.

- Chỉ đạo cơ sở giáo dục ban hành, phổ biến công khai quy tắc ứng xử số và quy định về nhóm trao đổi trực tuyến, chia sẻ hình ảnh, bảo vệ dữ liệu cá nhân, sử dụng thiết bị số và công cụ AI trong học tập, bảo đảm học sinh, giáo viên, nhân viên và cha mẹ học sinh thực hiện thống nhất.

- Hướng dẫn thiết lập kênh báo cáo an toàn, thân thiện, bảo mật, dễ tiếp cận và quy trình tiếp nhận, hỗ trợ ban đầu, phối hợp xử lý, theo dõi sau sự cố theo nguyên tắc không kỳ thị, không đổ lỗi, không lan truyền thông tin nhạy cảm.

- Tổ chức tập huấn, bồi dưỡng theo từng nhóm đối tượng; tăng cường phối hợp nhà trường – gia đình trong quản lý thời gian sử dụng thiết bị số, bảo vệ dữ liệu cá nhân, phòng tránh lừa đảo trực tuyến, bắt nạt mạng, tin giả và hỗ trợ học sinh khi gặp sự cố.

- Kiểm tra, giám sát, sơ kết, tổng kết việc thực hiện; tổng hợp kết quả, khó khăn, vướng mắc, đề xuất giải pháp và báo cáo Bộ Giáo dục và Đào tạo khi kết thúc năm học hoặc khi có yêu cầu.

Bộ Giáo dục và Đào tạo yêu cầu các Sở Giáo dục và Đào tạo, các đơn vị có cơ sở GDPT chỉ đạo các cơ sở giáo dục triển khai thực hiện đầy đủ, nghiêm túc hướng dẫn này. Trong quá trình triển khai, nếu có vấn đề vướng mắc, đề nghị các Sở Giáo dục và Đào tạo phản ánh kịp thời về Bộ Giáo dục và Đào tạo (qua Vụ Giáo dục Phổ thông) để được hướng dẫn, giải quyết.

Nơi nhận:

- Như trên;
- Bộ trưởng (để b/c);
- Các Thứ trưởng (để p/h chỉ đạo);
- Các Cục, Vụ thuộc Bộ GDĐT (để t/h);
- Lưu: VT, Vụ GDPT.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG THƯỜNG TRỰC



Phạm Ngọc Thường
Phạm Ngọc Thường

PHỤ LỤC

(Kèm theo Công văn số **6106**/BGDDĐT-GDPT ngày **14** tháng **9** năm 2026
của Bộ Giáo dục và Đào tạo)

Khung nội dung giáo dục an toàn mạng toàn diện

TT	Chủ đề	Nội dung chi tiết
1	Khai thác, đánh giá thông tin số và nhận diện rủi ro thông tin	Tìm kiếm, đánh giá, kiểm chứng nguồn tin; nhận diện tin giả, quảng cáo trá hình, thao túng cảm xúc, link lạ, mã QR giả, tin nhắn trúng thưởng, giả danh, lừa đảo trực tuyến.
2	Giao tiếp, hợp tác, ứng xử và công dân số	Ứng xử văn minh trong nhóm chat, mạng xã hội, trò chơi trực tuyến; tôn trọng danh dự, nhân phẩm, quyền riêng tư; phòng chống bắt nạt trên môi trường mạng, dụ dỗ trực tuyến và hành vi lan truyền nội dung gây hại
3	Quản lý danh tính số, dữ liệu cá nhân và quyền riêng tư	Nhận biết dữ liệu cá nhân, dữ liệu nhạy cảm; quản lý hồ sơ, hình ảnh, dấu vết số; xin phép trước khi chia sẻ hình ảnh, thông tin của người khác; kiểm soát quyền truy cập ứng dụng.
4	An toàn thiết bị, tài khoản và ứng phó sự cố	Mật khẩu mạnh, xác thực nhiều lớp, cập nhật phần mềm, nhận diện mã độc, bảo vệ thiết bị dùng chung; lưu bằng chứng, chặn, báo cáo, tìm kiếm hỗ trợ khi bị lừa đảo, chiếm tài khoản, quấy rối, phát tán thông tin.
5	Sức khỏe số, an sinh số và cân bằng đời sống số	Quản lý thời gian sử dụng thiết bị, giấc ngủ, thị lực, tư thế, vận động, cảm xúc, áp lực mạng xã hội, lệ thuộc trò chơi trực tuyến, mạng xã hội và hình thành thói quen số lành mạnh.
6	Sáng tạo nội dung số, bản quyền và trách nhiệm số	Tạo lập, chia sẻ các sản phẩm số an toàn; tôn trọng bản quyền, trích dẫn nguồn, không sao chép, không phát tán nội dung vi phạm pháp luật hoặc gây tổn hại đến bản thân và người khác.
7	Sử dụng AI an toàn trong học tập và sinh hoạt	Hiểu được AI có thể sai, thiên lệch hoặc tạo nội dung giả mạo; không cung cấp dữ liệu cá nhân/dữ liệu học sinh vào công cụ AI khi chưa được phép; sử dụng AI minh bạch, trung thực, có đạo đức, có kiểm chứng, không phụ thuộc và không dùng AI để gian lận hoặc gây hại.
8	Tìm kiếm hỗ trợ, phục hồi và đóng góp cộng đồng số	Biết cung cấp thông tin với người tin cậy, giáo viên, cán bộ tư vấn, tổng đài hoặc cơ quan chức năng; biết hỗ trợ bạn bè đúng cách; góp phần xây dựng môi trường số tích cực, nhân văn trong lớp học và nhà trường, gia đình và xã hội.