UBND XÃ NÚA NGAM
TRƯỜNG THCS NÚA NGAM

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 59 /QĐ-THCSNN

Núa Ngam, ngày 24 tháng 10 năm 2025

QUYẾT ĐỊNH
Quy chế bảo vệ dữ liệu cá nhân và an toàn thông tin mạng Trường THCS Núa Ngam

HIỆU TRƯỞNG TRƯỜNG THCS NÚA NGAM

Căn cứ Luật An toàn thông tin mạng 2015, Luật An ninh mạng 2018;

Căn cứ Nghị định 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định 73/2019/NĐ-CP ngày 05/9/2019 quy định quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn nhà nước; Nghị định số 82/2024/ND-CP ngày 10/7/2024 sửa đổi bổ sung một số điều Nghị định 73/2019/NĐ-CP ngày 05/9/2019 quy định quản lý đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn nhà nước;

Căn cứ Thông tư 42/2021/TT-BGDĐT ngày 30/12/2021 quy định về cơ sở dữ liệu giáo dục và đào tạo;

Căn cứ Công văn số 3946/BGDĐT-KHCNTT ngày 30/6/2025 của Bộ Giáo dục và Đào tạo về tăng cường công tác quản lý công tác bảo vệ dự liệu cá nhân và an toàn thông tin mạng liên quan đến chuyển đổi số trong giáo dục;

Xét đề nghị bộ phận phụ trách công nghệ thông tin nhà trường.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế bảo vệ dữ liệu cá nhân và an toàn thông tin mạng của Trường THCS Núa Ngam.

Điều 2. Quyết định này có hiệu lực thi hành từ ngày ký. Viên chức nhà trường và tổ chức, cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- UBND xã Núa Ngam (b/c);
- Phòng Văn hóa - Xã hội (b/c);
- Như Điều 2 (t/h);
- Lưu: VT.

HIỆU TRƯỞNG

Phạm Trung Thành

QUY CHẾ
Bảo vệ dữ liệu cá nhân và an toàn thông tin mạng

(Ban hành kèm theo Quyết định số: 59 /QĐ-THCSNN ngày 24 tháng 10 năm 2025 của Hiệu trưởng của Trường THCS Núa Ngam)

Chương I. Nguyên tắc chung

Điều 1. Nguyên tắc bảo vệ dữ liệu cá nhân và ATTT mạng

Toàn bộ hoạt động thu thập, lưu trữ và xử lý dữ liệu cá nhân trong Trường THCS Núa Ngam phải tuân thủ quy định của pháp luật về bảo vệ dữ liệu cá nhân. Dữ liệu cá nhân chỉ được thu thập đúng mục đích đã đăng ký, giới hạn ở phạm vi cần thiết, không được mua bán dưới mọi hình thức.

Mọi cá nhân có quyền biết, truy cập, chỉnh sửa hoặc yêu cầu xóa dữ liệu cá nhân của mình, trừ trường hợp pháp luật quy định khác. Mỗi dữ liệu cá nhân thu thập phải được cập nhật, bảo đảm chính xác và chỉ lưu trữ trong thời gian phù hợp với mục đích.

Nhà trường áp dụng các biện pháp nhằm bảo vệ dữ liệu cá nhân, bao gồm biện pháp bảo mật, phòng ngừa mất mát, phá hủy do sự cố và các vi phạm quy định về bảo vệ dữ liệu cá nhân. Các cá nhân, tổ chức liên quan chịu trách nhiệm tuân thủ các nguyên tắc này.

Chương II. Phạm vi và đối tượng áp dụng

Điều 2. Phạm vi áp dụng và đối tượng

Quy chế này áp dụng cho cán bộ quản lý, giáo viên, nhân viên và học sinh của nhà trường, nhà cung cấp dịch vụ CNTT và mọi cá nhân, đơn vị tham gia thu thập, xử lý hoặc quản lý dữ liệu cá nhân, sử dụng các hệ thống thông tin mạng.

Đối tượng của quy chế gồm: **Chủ thể dữ liệu** (người mà dữ liệu cá nhân phản ánh – như học sinh, phụ huynh, CBGVNV), **Bên kiểm soát dữ liệu** (Nhà trường và các cá nhân được chỉ định quyết định mục đích, phương tiện xử lý dữ liệu), **Bên xử lý dữ liệu** (tổ chức/cá nhân thực hiện xử lý dữ liệu thay mặt Trường), và **Bên thứ ba** (bên ngoài được phép xử lý dữ liệu).

Chương III. Nhiệm vụ và trách nhiệm

Điều 3. Trách nhiệm của Hiệu trưởng

Là người đứng đầu cơ quan chủ quản, Hiệu trưởng chịu trách nhiệm tổ chức, chỉ đạo thực hiện quy chế. Hiệu trưởng có nhiệm vụ: bố trí cán bộ phụ trách CNTT và bảo vệ dữ liệu cá nhân; phê duyệt danh mục dữ liệu thu thập, phương án bảo mật thông tin mạng; ký kết thỏa thuận bảo mật với nhà cung cấp dịch vụ CNTT; chỉ đạo xử lý kịp thời khi có sự cố an toàn thông tin xảy ra.

Điều 4. Trách nhiệm của các bộ phận, cá nhân khác

Cán bộ CNTT/Quản trị hệ thống có trách nhiệm vận hành, bảo trì các hệ thống CNTT của nhà trường; áp dụng các biện pháp an toàn (cài đặt tường lửa, phần mềm diệt virus, mã hóa, sao lưu dữ liệu định kỳ); kiểm tra an ninh hệ thống thường xuyên.

Giáo viên, nhân viên sử dụng hệ thống thông tin phải bảo mật thông tin khi đăng nhập (không chia sẻ tài khoản, sử dụng mật khẩu phức tạp, tối thiểu 8 ký tự bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt; thay đổi mật khẩu định kỳ tối đa 3 tháng/lần). Mọi tài liệu điện tử chứa thông tin cá nhân (hồ sơ học bạ, điểm số, hồ sơ nhân sự) phải được lưu trữ an toàn, chỉ chia sẻ theo quy định của quy chế.

Học sinh, phụ huynh chấp hành các quy định về bảo vệ thông tin cá nhân; không tiết lộ thông tin cá nhân của mình hoặc người khác trên mạng xã hội, hệ thống điện tử khi chưa được cho phép; chịu trách nhiệm về tính chính xác của dữ liệu do mình cung cấp.

Nhà cung cấp dịch vụ CNTT phải ký hợp đồng bảo mật với nhà trường; toàn bộ thông tin, dữ liệu hình thành trong quá trình cung cấp dịch vụ thuộc quyền sở hữu của nhà trường; bên cung cấp dịch vụ phải đảm bảo an toàn thông tin, bảo mật dữ liệu và chuyển giao đầy đủ cho nhà trường khi kết thúc hợp đồng. Nhà cung cấp chỉ được xử lý dữ liệu sau khi có thỏa thuận với nhà trường và phải thực hiện các biện pháp bảo vệ dữ liệu theo quy định.

Chương IV. Quản lý và xử lý dữ liệu cá nhân

Điều 5. Thu thập và phân loại dữ liệu

Nhà trường chỉ được thu thập dữ liệu cá nhân cần thiết cho hoạt động quản lý, giáo dục và thi đua khen thưởng. Danh mục dữ liệu bao gồm: thông tin định danh (họ tên, ngày sinh, giới tính, số CMND/CCCD/hộ chiếu), thông tin liên hệ (địa chỉ, số điện thoại, email), thông tin học tập (lớp học, kết quả học tập, khen thưởng, vi phạm), thông tin sức khỏe (tình trạng sức khỏe, khám bệnh, khuyết tật nếu có).

Khi thu thập dữ liệu cá nhân của học sinh hoặc phụ huynh, nhà trường phải được sự đồng ý của phụ huynh học sinh (trừ trường hợp pháp luật có quy định khác). Dữ liệu cá nhân phải được xếp loại bảo mật và được đánh giá mức độ nhạy cảm, từ đó áp dụng biện pháp bảo mật tương ứng. Việc thu thập dữ liệu chỉ được thực hiện khi có văn bản đề nghị, bảo vệ quyền lợi của học sinh và phục vụ quy trình quản lý, giảng dạy, khảo thí.

Điều 6. Lưu trữ và cập nhật dữ liệu

Tất cả dữ liệu cá nhân phải được lưu trữ ở nơi an toàn. Dữ liệu điện tử phải mã hóa hoặc lưu trữ trên hệ thống có bảo mật và sao lưu định kỳ. Cơ chế truy cập dữ liệu phải hạn chế theo vai trò: chỉ những người có nhiệm vụ xử lý mới có quyền truy cập dữ liệu cần thiết.

Dữ liệu cá nhân của học sinh được cập nhật khi thay đổi; cán bộ, giáo viên, nhân viên được cập nhật khi thay đổi chức vụ hoặc nghỉ việc. Các bản cứng của dữ liệu không còn giá trị sử dụng cần được tiêu hủy theo quy trình, không vứt bỏ tự do. Dữ liệu cá nhân chỉ được lưu trữ trong thời gian phù hợp với mục đích thu thập, trừ trường hợp pháp luật yêu cầu lưu giữ lâu hơn.

Điều 7. Chia sẻ và chuyển giao dữ liệu

Việc chuyển giao dữ liệu cá nhân giữa nhà trường và bên thứ ba chỉ được thực hiện khi có sự đồng ý của người có dữ liệu hoặc theo quy định của pháp luật. Nhà trường đảm bảo mọi hợp đồng chia sẻ hoặc chuyển giao dữ liệu đều có điều khoản bảo mật dữ liệu và trách nhiệm bảo đảm ATTT.

Dữ liệu cá nhân chỉ được chia sẻ trong phạm vi cần thiết và phù hợp với mục đích đã tuyên bố. Mọi yêu cầu cung cấp dữ liệu từ bên thứ ba phải được Hiệu trưởng phê duyệt sau khi xác minh tính hợp pháp. Dữ liệu nhạy cảm phải được bảo vệ cao hơn và không được chia sẻ công khai.

Chương V. Các biện pháp đảm bảo an toàn thông tin

Điều 8. Biện pháp kỹ thuật

Nhà trường thực hiện các biện pháp kỹ thuật cơ bản để bảo đảm an toàn mạng và hệ thống thông tin: cài đặt phần mềm diệt virus, cập nhật bản vá hệ điều hành, tường lửa, phân quyền truy cập, mã hóa dữ liệu quan trọng.

Hệ thống CNTT (edoc, SMAS, CSDL ngành, website trường) phải được kiểm thử bảo mật trước khi đưa vào sử dụng. Các phương tiện lưu trữ di động (USB, ổ cứng di động) khi mang ra khỏi phạm vi nhà trường phải tuân thủ quy định mã hóa dữ liệu. Thông tin cá nhân và dữ liệu quan trọng trong hệ thống phải được sao lưu định kỳ và lưu trữ an toàn.

Định kỳ tổ chức kiểm tra, đánh giá an ninh hệ thống: thử nghiệm xâm nhập, rà soát lỗ hổng, kiểm tra nhật ký hệ thống để phát hiện sớm dấu hiệu bất thường. Các lỗ hổng kỹ thuật được vá kịp thời để tránh rủi ro mất an toàn thông tin.

Điều 9. Biện pháp hành chính và truyền thông

Ban hành nội quy, quy trình bảo mật thông tin nội bộ: quy định về sử dụng thiết bị công nghệ (máy tính, điện thoại), quy tắc gửi/nhận email công vụ, lưu trữ hồ sơ điện tử. Các tài khoản truy cập chỉ được cấp cho cá nhân có nhiệm vụ rõ ràng, khuyến khích sử dụng xác thực hai yếu tố khi có thể. Mật khẩu phải được bảo mật, không chia sẻ và phải thay đổi định kỳ.

Tuyên truyền nâng cao nhận thức về bảo vệ dữ liệu cá nhân và ATTT cho CBGVNV và học sinh theo hướng dẫn của Bộ GDĐT. Đặc biệt, giáo dục học sinh về nguyên tắc không chia sẻ thông tin cá nhân trên môi trường mạng.

Đối với các hệ thống phần mềm quản lý (như hệ thống "Học bạ số"), phải ưu tiên sử dụng giải pháp được đánh giá an toàn, bảo mật, phù hợp tiêu chí ngành (đảm bảo khả năng tích hợp, bảo mật dữ liệu học bạ). Trang bị, cấp phát

chữ ký số cho cán bộ quản lý, giáo viên theo quy định để đảm bảo tính pháp lý của văn bản điện tử.

Chương VI. Xử lý vi phạm và phối hợp khắc phục sự cố

Điều 10. Xử lý vi phạm

Mọi hành vi vi phạm quy định bảo vệ dữ liệu cá nhân hoặc an toàn thông tin mạng (như tiết lộ, mua bán trái phép thông tin cá nhân, tấn công mạng phá hoại hệ thống) sẽ bị xử lý nghiêm theo quy định. Nếu vi phạm gây thiệt hại phải bồi thường theo quy định của pháp luật.

Khi phát hiện sự cố rò rỉ dữ liệu hoặc mất an toàn thông tin (ví dụ: hệ thống bị tấn công, lộ mật khẩu, phần mềm độc hại, rò rỉ thông tin cá nhân), phải báo cáo ngay cho Ban giám hiệu và tổ CNTT; phối hợp khẩn trương khắc phục để hạn chế thiệt hại.

Điều 11. Phối hợp với cơ quan chuyên môn

Nhà trường phối hợp với cơ quan an ninh mạng khi cần thiết để xử lý vi phạm hoặc xây dựng phương án nâng cao an toàn thông tin. Định kỳ báo cáo lãnh đạo cấp trên và cơ quan chức năng về tình hình thực hiện bảo vệ dữ liệu và ATTT của nhà trường.

Chương VII. Điều khoản thi hành

Điều 12. Hiệu lực và tổ chức thực hiện

Quy chế này có hiệu lực sau khi được ký ban hành; áp dụng cho toàn trường. Các tổ chức, cá nhân trong trường chịu trách nhiệm thi hành Quy chế. BGH chỉ đạo, giám sát việc thực hiện và định kỳ rà soát, cập nhật quy chế cho phù hợp với quy định pháp luật mới.

Trường hợp các quy định khác của pháp luật có liên quan có bổ sung hoặc sửa đổi, thì được áp dụng song song để bảo đảm tính đầy đủ, hiệu quả trong bảo vệ dữ liệu và ATTT mạng.

Điều 13. Tổ chức kiểm tra

Nhà trường thực hiện kiểm tra nội bộ định kỳ việc tuân thủ quy chế này; xử lý nghiêm các vi phạm (nếu có).

Phụ lục

1. Biểu mẫu báo cáo vi phạm: Mẫu Thông báo vi phạm quy định bảo vệ dữ liệu cá nhân (Mẫu số 03 Nghị định 13/2023/NĐ-CP).

2. Danh mục dữ liệu cá nhân của nhà trường: Họ tên, giới tính, ngày sinh, Nơi sinh, mã số định danh (CCCD/CMND), địa chỉ liên hệ, số điện thoại, email, tình trạng sức khỏe, kết quả học tập, khen thưởng – kỷ luật, thông tin gia đình (cha, mẹ), hồ sơ lao động (với CBGVNV), hồ sơ nhân sự nội bộ, chữ ký số (nếu có)…

3. Danh sách hệ thống CNTT đang sử dụng: Hệ thống văn bản điện tử (eDoc), phần mềm quản lý trường học (SMAS), Cơ sở dữ liệu ngành Giáo dục và Đào tạo (theo TT 42/2021), trang thông tin điện tử của trường và các dịch vụ điện tử liên quan. Các hệ thống này đều thuộc quản lý của Trường; mọi kết nối, trao đổi dữ liệu giữa chúng phải tuân thủ quy trình bảo mật thông tin của nhà trường.