SỞ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG THPT
NGUYỄN CÔNG PHƯƠNG
Số: 515/QĐ-NCP

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Quảng Ngãi, ngày 26 tháng 11 năm 2024

QUYẾT ĐỊNH
Ban hành Quy chế đảm bảo an toàn ứng dụng công nghệ thông tin và chuyển đổi số của Trường THPT Nguyễn Công Phương

HIỆU TRƯỞNG TRƯỜNG THPT NGUYỄN CÔNG PHƯƠNG

Căn cứ Quyết định số 131/QĐ-TTg ngày 25/01/2022 của Thủ tướng Chính phủ về phê duyệt Đề án "Tăng cường ứng dụng công nghệ thông tin và chuyển đổi số trong giáo dục và đào tạo giai đoạn 2022-2025, định hướng đến năm 2030";

Căn cứ Kế hoạch số 166/KH-UBND ngày 14/10/2022 của Chủ tịch UBND tỉnh Quảng Ngãi về Tăng cường đảm bảo an toàn, an ninh thông tin trong hoạt động các cơ quan nhà nước tỉnh Quảng Ngãi đến năm 2025 và định hướng đến năm 2030; Công văn số 5609/UBND-KGVX ngày 03/11/2022 của Chủ tịch UBND tỉnh Quảng Ngãi về việc triển khai thực hiện Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ; Quyết định số 906/QĐ-UBND ngày 11/7/2022 của UBND tỉnh Quảng Ngãi về việc ban hành Kế hoạch thực hiện Chiến lược quốc gia phát triển kinh tế số và xã hội số giai đoạn 2022 - 2025 trên địa bàn tỉnh Quảng Ngãi; Kế hoạch số 73/KH-UBND ngày 29/4/2022 về thực hiện Đề án "Nâng cao nhận thức, phổ cập kỹ năng và phát triển nguồn nhân lực chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030" trên địa bàn tỉnh Quảng Ngãi;

Căn cứ Thông tư 32/2020/TT- BGDĐT ngày 15/9/2020 của Bộ Giáo dục và Đào tạo về việc ban hành Điều lệ trường trung học cơ sở, trường trung học phổ thông và trường phổ thông có nhiều cấp học;

Xét đề nghị của Ban công nghệ thông tin nhà trường,

QUYẾT ĐỊNH:

Điều 1. Ban hành Quy chế đảm bảo an toàn ứng dụng công nghệ thông tin và chuyển đổi số của Trường THPT Nguyễn Công Phương.

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

Điều 3. Ban giám hiệu, các tổ chuyên môn, các thành viên của trường THPT Nguyễn Công Phương căn cứ quyết định thực hiện./.

Nơi nhận:
- SGD&ĐT (b/c);
- BGH;
- TCM;
- Website;
- Lưu: VT, kqv.

HIỆU TRƯỞNG

TRƯỜNG THPT NGUYỄN CÔNG PHƯƠNG

Nguyễn Xuân Vinh

QUY CHẾ
ĐẢM BẢO AN TOÀN ỨNG DỤNG CÔNG NGHỆ THÔNG TIN VÀ CHUYỂN ĐỔI SỐ CỦA TRƯỜNG THPT NGUYỄN CÔNG PHƯƠNG

(Kèm theo Quyết định số: 515 /QĐ-NCP ngày 26 /11/2024 của Trường THPT Nguyễn Công Phương)

CHƯƠNG I
NHỮNG QUY ĐỊNH CHUNG

Điều 1: Phạm vi điều chỉnh

Quy chế này quy định việc đảm bảo an toàn ứng dụng công nghệ thông tin (CNTT) và chuyển đổi số của Trường THPT Nguyễn Công Phương.

Điều 2: Đối tượng áp dụng

Quy chế này được áp dụng đối với viên chức và người lao động thuộc Trường THPT Nguyễn Công Phương trong việc quản lý, khai thác, sử dụng và đảm bảo an toàn, an ninh thông tin, phục vụ công tác chuyên môn.

Điều 3: Giải thích từ ngữ

1. An toàn thông tin là bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. An toàn thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

2. Hệ thống thông tin là một hệ thống bao gồm con người, dữ liệu, các quy trình và công nghệ thông tin tương tác với nhau để thu thập, xử lý, lưu trữ và cung cấp thông tin cần thiết nhằm hỗ trợ cho một hệ thống, phục vụ cho hoạt động lưu trữ, xử lý, truyền đưa, chia sẻ, trao đổi, cung cấp và sử dụng thông tin.

3. An ninh thông tin là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

4. Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng. Sự cố có thể là sự kiện đã, đang hoặc có khả năng xảy ra gây mất an toàn thông tin trên môi trường mạng *(LAN, WAN, Internet,...)*, được phát hiện thông qua việc giám sát, đánh giá, phân tích của các cơ quan, tổ chức, cá nhân có liên quan hoặc được cảnh báo từ các chuyên gia, tổ chức về lĩnh vực an toàn thông tin trong nước và trên thế giới.

5. Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

6. Tính toàn vẹn là bảo vệ tính chính xác và tính đầy đủ của thông tin và các phương pháp xử lý thông tin.

7. Tính tin cậy là đảm bảo thông tin chỉ có thể được truy cập bởi những người được cấp quyền sử dụng.

8. Tính sẵn sàng là đảm bảo những người được cấp quyền có thể truy cập thông tin và các tài nguyên *(mạng, máy chủ, tên miền, tài khoản thư điện tử...)* ngay khi có nhu cầu.

9. Người dùng là cán bộ, công chức và người lao động các phòng, ban, đơn vị trực thuộc Sở sử dụng máy tính, các thiết bị điện tử để xử lý công việc.

10. Tham số mạng là các tham số kỹ thuật được cài đặt trong các thiết bị mạng và thiết bị máy tính để tạo ra các địa chỉ kết nối trong mạng. Các máy tính gửi và nhận thông tin thông qua các địa chỉ kết nối này.

CHƯƠNG II
TRÁCH NHIỆM QUẢN LÝ, SỬ DỤNG ĐẢM BẢO AN TOÀN, AN NINH THÔNG TIN

Điều 4. Quản lý thiết bị công nghệ thông tin

1. Thiết bị CNTT được trang bị tại Trường THPT Nguyễn Công Phương là tài sản của Nhà nước, được quản lý, sử dụng theo quy định của Trường THPT Nguyễn Công Phương, của Nhà nước. Viên chức và người lao động có trách nhiệm quản lý trang thiết bị được giao.

2. Giao cho Nhân viên CNTT làm công tác quản trị mạng, trực tiếp quản lý kỹ thuật và duy trì hoạt động của hệ thống thông tin của Trường; là đầu mối kết nối mạng LAN, mạng Internet, mạng dữ liệu chuyên dùng cho các phòng; kiểm tra hiện trạng, đề xuất sửa chữa hoặc mua mới các chủng loại thiết bị CNTT phù hợp, an toàn, bảo mật theo quy định về quản lý, sử dụng tài sản cơ quan.

Điều 5. Quản lý, khai thác, sử dụng cơ sở dữ liệu và phần mềm

1. Nhân viên CNTT có trách nhiệm cài đặt, quản lý các phần mềm hệ thống và phần mềm ứng dụng trong hệ thống mạng máy tính tại trường; Nghiên cứu, đề xuất, nâng cấp công nghệ, phần mềm theo định hướng quản lý nhà nước của ngành và tuân theo quy định của Nhà nước.

2. Lãnh đạo nhà trường và toàn thể viên chức và người lao động có trách nhiệm phối hợp với Nhân viên CNTT trong quá trình triển khai, khai thác và sử dụng phần mềm. Không tự ý cài đặt hoặc gỡ bỏ các phần mềm liên quan đến bảo mật, an toàn thông tin.

Điều 6. Phòng chống virus máy tính, bảo mật cơ sở dữ liệu và an ninh mạng

1. Bảo mật số liệu: Cán bộ quản lý, viên chức và người lao động phải có trách nhiệm bảo mật số liệu nghiệp vụ trên máy tính. Việc chia sẻ dữ liệu trên mạng do bộ phận quản trị mạng thực hiện theo quyết định của Hiệu trưởng và theo phân cấp sử dụng tài nguyên mạng.

2. Bảo mật truy cập: Các chương trình ứng dụng, phân chia sử dụng trên máy tính phải được đặt mật khẩu, mã khoá bảo mật.

3. Bảo mật hệ thống mạng và truyền tin: Mạng và đường truyền được áp dụng các chế độ bảo mật cần thiết, chống xâm nhập bất hợp pháp. Bộ phận quản trị mạng có trách nhiệm thường xuyên theo dõi, kiểm tra phát hiện kịp thời các hoạt động xâm nhập và có biện pháp xử lý kịp thời.

4. An toàn trong sử dụng: Khi không làm việc với máy vi tính trong thời gian dài, cán bộ, công chức và người lao động thuộc trường phải tắt máy tính hoặc đặt chế độ bảo vệ để đảm bảo an toàn cho dữ liệu của cá nhân.

5. Phòng, chống virus: Cán bộ quản lý, viên chức và người lao động thuộc Trường có trách nhiệm tuân thủ các biện pháp phòng và chống virus cho máy tính, đảm bảo an toàn dữ liệu thuộc cá nhân quản lý. Mọi dữ liệu từ các thiết bị lưu trữ bên ngoài đều phải được quét, diệt virus mỗi khi đưa vào máy. Những máy tính phát hiện có virus phải được tách khỏi mạng về mặt vật lý để tránh tình trạng lây nhiễm sang các máy tính khác. Không truy cập vào các đường link liên kết không rõ ràng; không mở các link, tải về các tập tin tài liệu từ các địa chỉ thư không nắm rõ thông tin, địa chỉ người gửi.

Điều 7. Đảm bảo an toàn máy chủ, máy trạm, các thiết bị di động và cơ chế sao lưu, phục hồi

1. Kiểm soát chặt chẽ việc cài đặt các phần mềm mới lên máy trạm và các thiết bị di động. Các phần mềm được cài đặt trên máy trạm và các thiết bị di động *(bao gồm hệ điều hành, các phần mềm ứng dụng văn phòng, phần mềm phục vụ công việc, tiện ích khác,...)* phải được thường xuyên theo dõi, cập nhật bản vá lỗi bảo mật của nhà phát triển, lựa chọn cài đặt các phần mềm chống, diệt virus, mã độc và thường xuyên cập nhật phiên bản mới, đặt lịch quét virus theo định kỳ.

2. Cơ chế sao lưu, phục hồi máy chủ, máy trạm: Cán bộ quản lý, viên chức và người lao động phải sao lưu định kỳ cơ sở dữ liệu và các dữ liệu quan trọng khác *(bao gồm dữ liệu phát sinh trong quá trình vận hành các phần mềm ứng dụng như: các tập tin văn bản, hình ảnh,...)*. Sau khi sao lưu, lưu trữ bản sao lưu bằng thiết bị lưu trữ ngoài theo quy định lưu trữ hiện hành nhằm phục vụ cho việc phục hồi, khắc phục hệ thống kịp thời khi có sự cố xảy ra.

Điều 8. Đảm bảo an toàn hệ thống mạng máy tính, kết nối Internet

1. Quản lý hệ thống mạng nội bộ: Mạng nội bộ khi kết nối với mạng Internet phải thông qua thiết bị tường lửa kiểm soát, có phân chia hệ thống mạng nội bộ thành các vùng mạng theo phạm vi truy cập, vô hiệu hóa tất cả các dịch vụ không sử dụng tại từng vùng mạng, thực hiện nguyên tắc chỉ mở các dịch vụ cần thiết khi có yêu cầu.

2. Quản lý hệ thống mạng không dây: Khi thiết lập mạng không dây có kết nối vào mạng nội bộ phải thiết lập các thông số cần thiết như định danh, mật mã, mã hóa dữ liệu, có thay đổi mật mã định kỳ.

3. Quản lý truy cập từ xa vào mạng nội bộ: Đối với việc truy cập từ xa vào mạng nội bộ phải được theo dõi, quản lý chặt chẽ, nhất là truy cập có sử dụng chức năng quản trị, phải thiết lập mật mã độ an toàn cao, thường xuyên thay đổi mật mã, hạn chế truy cập từ xa vào mạng nội bộ từ các điểm truy cập Internet công cộng.

Điều 9. Đảm bảo an toàn truy cập, đăng nhập hệ thống thông tin

1. Trách nhiệm, quyền hạn người dùng khi truy cập, đăng nhập các hệ thống thông tin, đảm bảo mỗi người dùng khi sử dụng hệ thống thông tin phải được cấp và sử dụng tài khoản truy cập với định danh duy nhất gắn với người dùng đó. Trường hợp sử dụng tài khoản dùng chung cho một nhóm người hay một đơn vị, bộ phận phải có cơ chế xác định các cá nhân có trách nhiệm quản lý tài khoản. Người dùng chỉ được truy cập các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình và có trách nhiệm bảo mật tài khoản truy cập được cấp.

2. Mật mã đăng nhập, truy cập hệ thống thông tin phải có độ phức tạp cao *(có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số hoặc ký tự đặc biệt như !, @, #, $, %,...)*.

Điều 10. Đảm bảo an toàn thông tin, dữ liệu

1. Thông tin, dữ liệu khi được lưu trữ, khai thác, trao đổi phải được đảm bảo tính toàn vẹn, tính tin cậy, tính sẵn sàng. Thông tin, dữ liệu quan trọng khi được lưu trữ, trao đổi phải áp dụng kỹ thuật mã hóa, thiết lập mật mã, ứng dụng chữ ký số và phải có cơ chế lưu trữ dự phòng.

2. Trong trao đổi thông tin, dữ liệu phục vụ công việc, cơ quan, cán bộ quản lý và văn thư phải sử dụng hệ thống thông tin do tỉnh Quảng Ngãi và Sở Giáo dục Quảng Ngãi cấp, phần mềm quản lý văn bản và hồ sơ công việc. Hạn chế việc sử dụng các phương tiện trao đổi thông tin dữ liệu, hệ thống thư điện tử công cộng, mạng xã hội trên Internet trong hoạt động của Trường.

Điều 11. Những điều không được làm

1. Không được lợi dụng việc sử dụng Internet nhằm mục đích: Chống lại nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; kích động bạo lực, đồi trụy, tệ nạn xã hội, mê tín dị đoan; phá hoại thuần phong mỹ tục của dân tộc.

2. Không được tiết lộ bí mật nhà nước và các bí mật khác đã được pháp luật quy định.

3. Không được chơi các trò chơi trực tuyến *(game online)* hoặc các trò chơi khác trên Internet trong giờ làm việc.

4. Không được truy cập hoặc tải thông tin từ các trang website có nội dung đồi trụy, phản động, các chương trình không rõ nguồn gốc, các thông tin quảng cáo hấp dẫn.

CHƯƠNG III
PHƯƠNG ÁN CƠ BẢN ĐẢM BẢO AN TOÀN THÔNG TIN

Điều 12. Chính sách an toàn thông tin

Xây dựng chính sách, quy trình quản lý, vận hành hoạt động bình thường của hệ thống nhằm bảo đảm tính sẵn sàng của hệ thống trong quá trình vận hành, khai thác.

1. Đảm bảo an toàn mức vật lý:

Có hệ thống điện UPS dự phòng. Hệ thống chống sét cho toàn nhà, thiết bị chống sét nguồn điện.

2. Quản lý an toàn mạng:

Hệ thống mạng được thiết kế thống nhất, được quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn và bảo mật.

Hệ thống mạng nội bộ (LAN) được bảo vệ bằng tường lửa *(tích hợp tường lửa trên Router board nếu có)* và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng.

Mạng không dây, được đặt mật khẩu và theo định kỳ 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Có cơ chế xác thực và mã hóa khi sử dụng mạng không dây.

3. Quản lý an toàn máy chủ và ứng dụng: Thuê dịch vụ công nghệ thông tin để hosting Cổng thông tin điện tử; chạy các phần mềm ứng dụng phục vụ cho công tác chuyên môn của Trường.

4. Quản lý an toàn dữ liệu:

Có cơ chế thông báo để các bộ phận trong nhà trường sao lưu dữ liệu dự phòng, lưu trữ dữ liệu cá nhân ra thiết bị ngoại vi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra.

Chỉ có Quản trị hệ thống mới có quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

5. Quản lý an toàn người sử dụng đầu cuối:

Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải thường xuyên quét virus trước khi đọc hoặc sao chép dữ liệu.

Không sử dụng các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, PDA) hoặc những thiết bị lưu trữ di động cá nhân vào mục đích không phải nhiệm vụ. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.

Các thiết bị đầu cuối khi kết nối phải được quản lý và cập nhật thông tin *(tên, chủng loại, địa chỉ MAC, địa chỉ IP)*. Sử dụng cơ chế xác thực và sử dụng giao thức mạng an toàn.

Thường xuyên theo dõi, kiểm tra các lỗ hổng bảo mật và quản lý kết nối, truy cập khi sử dụng thiết bị đầu cuối từ xa.

Viên chức chuyên trách về an toàn thông tin thường xuyên theo dõi cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống đối với các cán bộ quản lý, viên chức và người lao động đã nghỉ hưu, chuyển công tác, nghỉ việc.

Theo dõi cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

Điều 13. Phối hợp với những cơ quan/tổ chức có thẩm quyền

1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:

Trường THPT Nguyễn Công Phương giao Nhân viên CNTT là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin. Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trong nhà trường.

Nhân viên CNTT chủ trì tham mưu lãnh đạo nhà trường thực hiện nhiệm vụ phối hợp với Sở Giáo dục và Đào tạo và các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của cấp có thẩm quyền.

2. Công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin, tùy theo mức độ sự cố, phối hợp Sở Giáo dục và Đào tạo, Sở Thông tin và Truyền thông, Đội ứng cứu sự cố mạng tỉnh Quảng Ngãi, Cục An toàn thông tin Bộ GDĐT hoặc Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

Điều 14. Quy định đối với việc thử nghiệm và nghiệm thu hệ thống

1. Các phần mềm, ứng dụng khi vận hành trong hệ thống mạng máy tính của Trường THPT Nguyễn Công Phương tối thiểu phải đáp ứng những yêu cầu sau:

Phải được kiểm tra, thử nghiệm đáp ứng tiêu chuẩn an toàn thông tin trước khi đưa vào sử dụng.

Đảm bảo tính toàn vẹn của dữ liệu khi lưu chuyển trong hệ thống mạng Trường THPT Nguyễn Công Phương.

2. Nhân viên CNTT phối hợp với các bộ phân có liên quan trong nhà trường, chịu trách nhiệm theo dõi hoạt động, thử nghiệm, trực tiếp cài đặt, quản lý và vận hành phần mềm hệ thống, phần mềm tiện ích và ứng dụng công nghệ thông tin trong hệ thống mạng máy tính; nghiên cứu, đề xuất, nâng cấp phần mềm đáp ứng yêu cầu công việc của nhà trường.

3. Thực hiện kiểm tra thường xuyên nhằm phát hiện và khắc phục lỗ hổng bảo mật của phần mềm, ứng dụng; cập nhật các bản nâng cấp mới và các bản vá lỗi cho phần mềm hệ thống.

Điều 15. Quy định về quản lý an toàn dữ liệu

Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.

Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra.

Tiến hành cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ được thực hiện theo yêu cầu của đơn vị vận hành hệ thống. Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ.

Quản lý chặt chẽ các thiết bị lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của người có thẩm quyền.

Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của cán bộ quản lý, viên chức, người lao động và phải được phê duyệt từ cấp trên.

CHƯƠNG IV
TỔ CHỨC THỰC HIỆN

Điều 16. Điều khoản thi hành

1. Các cán bộ quản lý, viên chức và người lao động tại trường THPT Nguyễn Công Phương có trách nhiệm thực hiện nghiêm túc Quy chế này.

2. Mọi hành vi vi phạm các điều khoản trong Quy chế, tùy theo tính chất, mức độ sẽ bị xử lý kỷ luật, xử phạt vi phạm hành chính, bồi thường vật chất, khắc phục hậu quả hoặc truy cứu trách nhiệm hình sự theo quy định của pháp luật hiện hành.

3. Trong quá trình thực hiện, nếu có vấn đề phát sinh hoặc khó khăn, vướng mắc cần phản ánh kịp thời về Nhân viên CNTT để tổng hợp báo cáo Hiệu trưởng xem xét quyết định điều chỉnh, bổ sung cho phù hợp./.