UBND TỈNH BẮC NINH
SỞ GIÁO DỤC VÀ ĐÀO TẠO

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

Số: 528 /SGDĐT-TCHC
V/v tăng cường công tác đảm bảo an toàn trong việc dạy và học qua mạng internet

Bắc Ninh, ngày 17 tháng 4 năm 2020

Kính gửi:
- Phòng Giáo dục và Đào tạo các huyện, thị xã, thành phố;
- Các đơn vị trực thuộc Sở Giáo dục và Đào tạo;
- Các Trung tâm GDNN-GDTX cấp huyện.

Thực hiện công văn số 1247/BGDĐT-GDCTHSSV ngày 13/4/2020 của Bộ Giáo dục và Đào tạo về việc tăng cường công tác đảm bảo an toàn cho trẻ mầm non, học sinh, sinh viên trong quá trình học tập qua Internet.

Căn cứ công văn số 250/CATTT-VNCERT/CC ngày 14/4/2020 của Cục an toàn thông tin, Bộ Thông tin và Truyền thông về việc cảnh báo nguy cơ mất an toàn thông tin từ phần mềm họp trực tuyến Zoom; Công văn số 244/STTTT-CNTT ngày 16/4/2020 của Sở Thông tin và Truyền thông tỉnh Bắc Ninh về việc triển khai ứng dụng công nghệ thông tin phục vụ các buổi họp trực tuyến để đảm bảo an toàn thông tin.

Trong thời gian qua, việc dạy và học qua internet, trên truyền hình được các cơ sở giáo dục trong toàn tỉnh tích cực triển khai và đã đạt được nhiều kết quả tốt, được đông đảo học sinh và phụ huynh học sinh hưởng ứng, tuy nhiên theo khuyến cáo của Bộ GDĐT và Bộ Thông tin và Tuyền thông trong quá trình tổ chức dạy học qua Internet của một số phần mềm dạy học trực tuyến miễn phí không có bản quyền đã xảy ra hiện tượng bị kẻ xấu xâm nhập vào địa chỉ lớp học/phòng học trực tuyến, đăng tải nội dung xấu, độc, phản cảm, phản giáo dục... có dấu hiệu lạm dụng, quấy rối và bắt nạt trẻ em, học sinh, sinh viên trên mạng, không đảm bảo an toàn cho người học, người dạy; ảnh hưởng đến chất lượng dạy học qua Internet.

Để khắc phục tình trạng trên, Sở Giáo dục và Đào tạo (GDĐT) hướng dẫn các đơn vị thực hiện các nội dung sau đây:

1. Tiếp tục thực hiện có hiệu quả việc tổ chức dạy học qua Internet, trên truyền hình theo các văn bản chỉ đạo, hướng dẫn của Sở GDĐT.

2. Tăng cường các biện pháp bảo đảm an toàn thông tin đối với các hệ thống công nghệ thông tin đang quản lý và sử dụng; quán triệt tới cán bộ, giáo viên, học sinh, sinh viên thực hiện tốt một số biện pháp cơ bản đảm bảo an toàn thông tin (theo hướng dẫn tại phụ lục kèm theo).

3. Các cơ quan, tổ chức, hành chính nhà nước không nên sử dụng phần mềm Zoom để phục vụ các buổi họp trực tuyến tại đơn vị mình; trong dạy học, phổ biến

cho giáo viên những giải pháp, phần mềm quản lý, tổ chức dạy học qua Internet tin cậy, có uy tín; ưu tiên sử dụng phần mềm có bản quyền, những phần mềm do Bộ GDĐT và Bộ Thông tin và Truyền thông giới thiệu sử dụng miễn phí trong mùa dịch Covid-19, cụ thể như: Cổng học liệu và thi trực tuyến của VNPT tại địa chỉ: https://sgdbnh.lms.vnedu.vn; chương trình học tập trực tuyến và ôn luyện miễn phí tại nhà Viettelstudy.vn và hệ thống ViText của nhà mạng Viettel; phần mềm họp trực tuyến eMeting của Trung tâm Chính phủ điện tử - Cục tin học hóa – Bộ Thông tin và Truyền thông (tại địa chỉ https://emeeting.mic.gov.vn). Sở GDĐT giới thiệu hệ thống học trực tuyến qua tài khoản Email của Sở cung cấp được google hỗ trợ (có tài liệu hướng dẫn gửi kèm); Hệ thống quản lý giao bài tập về nhà cho học sinh trên phần mềm quản lý giáo dục của ngành tại địa chỉ http://qlgd.bacninh.edu.vn/.

4. Các nhà trường cần xây dựng và thực hiện quy chế quản lý, tổ chức dạy học qua Internet, trong đó hướng dẫn rõ quy trình quản lý, tổ chức một lớp học trực tuyến; các kỹ năng quản lý điều hành lớp học trực tuyến đối với giáo viên; trách nhiệm của người học khi tham gia lớp học trực tuyến, nhất là các hành vi không được làm đối với người học.

5. Tăng cường các biện pháp phối hợp giữa nhà trường và gia đình trong quản lý, tổ chức hoạt động dạy học qua Internet. Đề nghị phụ huynh nâng cao trách nhiệm, dành nhiều thời gian quan tâm, hỗ trợ học sinh kết nối, sử dụng phòng học trực tuyến an toàn và có biện pháp quản lý trong thời gian học sinh tham gia học trực tuyến và sử dụng Internet.

Tùy theo điều kiện và tình hình thực tế tại các địa phương, đơn vị có thể lựa chọn hình thức dạy học qua mạng internet cho phù hợp, đảm bảo an ninh, an toàn cho người dạy và học.

Sở Giáo dục và Đào tạo yêu cầu các đơn vị thực hiện nghiêm túc các nội dung tại công văn này, trong quá trình thực hiện nếu phát hiện sự cố cần báo cáo kịp thời về Sở GDĐT (ông Nguyễn Văn Đang, phó trưởng phòng Tổ chức – Hành chính, điện thoại: 0941.006999 và bà Nguyễn Thị Ngọc, trưởng phòng Công tác học sinh, sinh viên, điện thoại: 0912.275988./.

Nơi nhận:
- Như trên;
- UBND tỉnh (b/c);
- Lãnh đạo Sở;
- UBND huyện, tx,tp (p/h chỉ đạo);
- Các phòng thuộc Sở GDĐT (t/h);
- Lưu: VT, TCHC.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH BẮC NINH

Nguyễn Thế Sơn

Phụ lục

MỘT SỐ BIỆN PHÁP CƠ BẢN BẢO ĐẢM AN TOÀN THÔNG TIN

(Kèm theo Công văn số 528 /SGDĐT-TCHC ngày 17/4/2020 của Sở Giáo dục và Đào tạo tỉnh Bắc Ninh)

1. Khi đặt mật khẩu đăng nhập vào các hệ thống công nghệ thông tin, các phần mềm ứng dụng cần phải sử dụng mật khẩu mạnh với ít nhất 8 ký tự, có ký tự đặc biệt, có cả chữ thường, chữ HOA và số; định kỳ cần thay đổi mật khẩu, không để chế độ mật khẩu mặc định; hạn chế việc sử dụng thông tin cá nhân để đặt mật khẩu. Một mật khẩu mạnh sẽ khó bị tấn công, bị dò quét hơn. Ví dụ về mật khẩu mạnh: *1G@3df8*aH*.

2. Cần thực hiện gỡ bỏ các phần mềm không cần thiết, chỉ cài đặt trên máy tính các phần mềm thật cần thiết và cập nhật thường xuyên vì càng nhiều phần mềm được cài đặt thì càng dễ có nhiều lỗ hổng bảo mật.

3. Cần sao lưu định kỳ đối với dữ liệu quan trọng, đề phòng trường hợp bị tấn công, xóa hết dữ liệu hoặc bị mã hóa dữ liệu.

4. Cần cài đặt phần mềm diệt virus có bản quyền, cập nhật phần mềm và thường xuyên quét virus; quét virus đối với các tập tin nhận được từ thư điện tử, tải từ mạng internet, sao chép từ bên ngoài,…Kích hoạt và sử dụng chức năng tường lửa cá nhân để ngăn chặn các kết nối trái phép.

5. Không sử dụng các phiên bản Windows không còn được hỗ trợ, nâng cấp và cập nhật bản vá lỗi Windows và các phần mềm ứng dụng để giảm thiểu nguy cơ bị tấn công qua việc khai thác các lỗ hổng bảo mật.

6. Không nên truy cập các Website không tin cậy vì có thể bị cài đặt phần mềm độc hại một cách bí mật lên máy tính.

7. Không nên sử dụng phần mềm không bản quyền, không nên tải về, cài đặt phần mềm trên mạng không rõ nguồn gốc vì thường chứa mã độc.

8. Không mở thư có tiêu đề nhạy cảm, tập tin đính kèm, liên kết (link) gửi kèm thư điện tử; không cung cấp thông tin cá nhân nếu không rõ nguồn gốc thư điện tử. *Lưu ý: Tên người gửi hoặc địa chỉ thư điện tử của người gửi cũng có thể bị giả mạo.*

9. Không nên sử dụng mạng internet công cộng để đăng nhập vào các hệ thống CNTT, các phần mềm ứng dụng để tránh bị đánh cắp mật khẩu, dữ liệu.

10. Không chia sẻ thông tin về phòng họp, phòng học (ID, mật khẩu) để tránh các trường hợp bị kẻ sấu theo dõi, phá hoại.
