MEMORANDUM

TO: School Leaders
FROM: Derek Phillips
DATE: April 3, 2020
RE: Internet Safety

On March 30, 2020, the FBI released an article, warning users of teleconferencing sessions being hijacked (also being referred to as "Zoom-bombing") all over the nation. The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language. In the wake of reports of this activity being reported to the FBI's Internet Crime Complaints Center (IC3 -ic3.gov), they have published the following recommendations:

- Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests;
- Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people;
- Manage screensharing options. In Zoom, change screensharing to "Host Only";
- Ensure users are using the updated version of remote access/meeting applications. In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join;
- Lastly, ensure that your organization's telework policy or guide addresses requirements for physical and information security.

Additionally, the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) released a notice today about regarding this activity and added the following recommendations as this issue is not specific to Zoom, but rather applies to all video teleconferencing (VTC) software:

- Consider security requirements when selecting vendors. For example, if end-to-end encryption is necessary, does the vendor offer it?
- Ensure VTC software is up to date.

If you have any questions, please reach out to myself at communications@erskinecharters.org or Allen Ray at techdirector@erskinecharters.org.