CARLTON FIELDS

Compliance Tips for Distance Learning at Independent and Public Schools

EDUCATION | CORONAVIRUS | CYBERSECURITY AND PRIVACY | MARCH 30, 2020


Michael L. Yaeger


Christina M. Gagnier


James M. Sconzo


Stacey K. Sutton

In order to continue their educational mission during the COVID-19 pandemic, schools across the country, both independent and public, have responded by exploring online education or "distance learning." We consider some of the issues and offer a few practical tips below.

Software Considerations

Any new software employed in distance learning, including videoconferencing software, should be vetted, and privacy and security should be top of mind.

- *Access controls*.
    - Links to meetings should not be shared on public channels (e.g., publicly available pages on school websites) and should require a password or meeting ID so as to prevent unauthorized access to or disruption of a class by outsiders — a practice that has come to be called "Zoombombing." Become familiar with, and train your teachers on, the specific security features of the software.[1]
    - Consider changing default settings so that class participants cannot automatically share their screens or files without approval by the teacher. Allowing files to be transferred could potentially allow malware to be shared.
    - IT administrators need to control permissions and privileges for staff accounts; if someone leaves the school, that individual's access privileges need to be revoked. Also, the school should consider disabling features that are unnecessary. There are different companies that provide provisioning tools that can be integrated with a school's chosen distance learning tool.
    - Consider advising teachers and students to clear their desktops when screen sharing to avoid sharing information that should not be public.
    - *"General interest" tech*. Schools using or contemplating using tools not developed for the education space should consider whether they are compliant with existing student privacy laws and regulations, such as the federal Children's Online Privacy Protection Act. Some companies that produce tools that are widely available also have specific policies and designations for schools. For example, Zoom has a separate policy for K-12 schools if the district or school is a "school subscriber."
- *The cost of free software*. Be aware that free software may have key differences in data retention and use than paid software. Be sure to review the terms and conditions and privacy policies to understand how long the software company stores data.

  For example, the Electronic Frontier Foundation has reported that "[b]y default, Slack retains all the messages in a workspace or channel (including direct messages) for as long as the workspace exists." Users cannot automatically delete them.
- *Training*. Provide training to teachers and staff, and provide information to students on privacy settings. Consider, too, creating FAQ — one for teachers and staff, one for parents and students — that are updated as necessary and, in particular, when and if software is changed.

Americans with Disabilities Act (ADA) Considerations

- School districts that set up online learning must also provide services to students with disabilities under the federal Individuals with Disabilities Education Act and Section 504.
- The U.S. Department of Education's Office for Civil Rights has produced a webinar regarding what must be done to ensure that students with disabilities can access and use online learning.

Complying With Copyright Rules

- When teachers or students transmit a performance or display a work protected by copyright, such as a book or article published in the last 70 years, there is a potential copyright issue. But if certain rules are followed, schools can avoid having to obtain advance permission from the copyright owner.
- In general, teachers or students at a nonprofit educational institution do not infringe when they "transmit" a performance or display a copyright work as part of or in relation to a course when they follow certain guidelines:
    - Limit the use of works to an amount and time comparable to what would be displayed or performed in a live, physical classroom;
    - Limit access to the copyright works to students enrolled in the course, and take reasonable measures to prevent downstream copying, or retention of the works by students for longer than a class session;
    - Notify students that the works may be protected by copyright;
    - Avoid using works sold or licensed for distance learning (without paying for those materials); and
    - Avoid using pirated or illegally copied works.

Distance learning not only has significant value in the current crisis but also great promise for the future. In order to realize that promise, schools will need to be attentive to their legal obligations and security risks as they experiment with new products and approaches.

[1] For example, Zoom provides security tips on its blog. *See* https://blog.zoom.us/wordpress/2020/03/20/keep-the-party-crashers-from-crashing-your-zoom-event/. The University of Southern California has also provided some tips to prevent Zoombombing. *See* https://keepteaching.usc.edu/tools/zoombombing-resources/.