# PROTECTING STUDENT PRIVACY

# LEARNING FROM COVID-19

Seemingly overnight, COVID-19 stay-at-home orders shuttered K-12 schools and institutions of higher education (HE), and educators were expected to rapidly employ educational "triage" to move a generation of kindergarten to graduate-level students into remote education. Educational institutions in technologically advanced regions quickly adopted a wide variety of online tools including video conferencing, collaboration apps, project planning software, and cloud storage to piece together curriculum, resources, and communication. Within weeks, education worldwide had instituted Emergency Remote Teaching (ERT).

ERT is not like the planned, pedagogically sound, online learning already in existence,[1] which uses course management or learning-management systems (CMS/LMS). Traditional CMS/LMS are developed with student security and privacy in mind.[2] They provide a clearly written privacy policy and terms of agreement and meet regulatory compliance. Traditional systems support a planned curriculum, pedagogically sound learning, and secure storage and grading.

In contrast, Emergency Remote Teaching during COVID-19 has often brought together poorly vetted online applications that utilize undefined levels of encryption and include terms of agreement that do not meet privacy regulations. Student (and teacher) security and privacy were further at risk due to their connecting via home or public networks—often using their own personal devices.

Many of the online tools cobbled together during the COVID-19 emergency are user-friendly,[3] which means that

BY ANNETTE MELGOSA and ERNEST STAATS

teachers and students quickly embraced them to share lessons, engage collaboratively, and to post assignments.[4] This makes the task of deciding whether or not to permanently adopt these technologies after COVID-19 more difficult. Institutions choosing to do so will need to enact privacy policies and procedures for teachers and students.

### What Is Personal Data, and Why Should We Care About Guarding It?

Online data privacy refers to how entities collect, host, store, use, share, and secure a user's personal data. Protecting users' rights to manage and determine how others handle their personal data is the purpose of privacy,[5] and the Universal Declaration of Human Rights declares that entities should not intrude upon this right of an individual.[6] In line with this, in 2013, the U.N. adopted The Right to Privacy in the Digital Age.[7]

The right to personal-data privacy has been legislatively codified around the world to prevent individuals or organizations from obtaining other people's information and unethically or illegally using it to exploit them and cause harm. In today's digital world, where tracking a user's activity is ubiquitous to the online experience, even one piece of digital information can reveal additional personal data and put that person in harm's way. For example, a predator who possesses a child's age, username, or e-mail address can easily target that child. With a device ID, a hacker can spoof a person's mobile device and receive copies of incoming text messages which can then be used for blackmail or identity theft. Unfortunately, criminals in possession of student personal data have been known to threaten students and their families with physical harm.

As Christian educators, it is up to us to follow all data privacy laws within our own countries to protect the personal data of those in our care from unscrupulous and unauthorized use. We should do this not only for regulatory compliance but also because God asks us to do justice and protect the vulnerable (Isaiah 1:17).

Given that educators and educational administrators must work within a legislative environment that seeks to protect children's data privacy, it is helpful to understand the different types of personal data. Personal data is traditionally categorized as *linked* or *linkable* data. In today's digital world, electronic identifiers may also be included. Table 1 provides some examples.[8]

Personal Data may pertain to a specific area of one's life. In an educational setting, for example, a student's Personal Data includes grades, educational records, and personal information exchanged within his or her educational experience. Data privacy principles hold an organization responsible to protect all personal data in its possession. Entities that collect, store, or distribute Personal Data are accountable for enacting policy and procedures to protect it.[9]

**Table 1. Examples of Personal Data**

| Data Type | Examples of Data Type |
|---|---|
| **Linked Data—**Data that when linked to an individual can identify him or her | Data traditionally linked to a person such as name, address, phone number, date of birth, driver's license number or other ID, biometric data |
| **Linkable Data—**Data that alone cannot identify a person but if combined with other data can be used to identify the individual | Place of birth, Zip/postal code, gender, age range, ethnicity, e-mail address, religion |
| **Other Electronic Identifiers—**Persistent Identifiers (long-lasting references to a resource such as a dataset or a person) may be considered as personal data if they can be used to identify an individual; other digital identifiers may also link to individuals under certain circumstances. | Persistent Identifiers are often used to personalize a user's digital experience or to advertise to him or her. These include things like Device ID, Cookies, or an Internet Protocol (IP) address. Geolocation is another digital identifier that can often reliably track an individual. |

### Privacy Guidelines and Regulations Affecting Education

Data and child privacy regulations around the world cover similar principles while navigating a complex series of cultures and legislative traditions.[10] Table 2 provides three examples of regulations that have had an impact on worldwide regulatory efforts. Included are the U.S. Family Educational Rights and Privacy Act (FERPA), the U.S. Children's Online Privacy Protection Act (COPPA), and the EU General Data Protection Regulation (GDPR). Each reader should become familiar with privacy regulations in his or her own region of the world and consult educational authorities and legal counsel as he or she applies these regulations.

- The Global Education Privacy Standard (GEPS) incorporates common standards upon which all privacy regulations are based. Use this adapted list[11] to identify what your institution needs to understand and document:
- Understand what is or is not allowed with data, based on your jurisdiction's regulatory laws;
- Be clear about why you are going to use data in a specific manner;
- Understand what the law requires of you concerning data privacy;
- Understand the basic technical standards that relate to data privacy;
- Understand data retention and purging regulations;
- Identify who will handle the data, have access to it, or be notified if concerns arise; and
- Consider compliance across borders (Which countries may be impacted?).

### Why Now?

Why should educators concern themselves about data privacy during this time of crisis? Many of the online applications that educational institutions embraced during COVID-19 did not typically cater to school or student data privacy, as they were made for public use. To their credit, they recognized the educational sector need and temporarily offered their products to schools for free or nearly free. At their core, however, they remain focused on profit.

Several applications that rolled out to schools quickly succumbed to security or privacy issues.[12] Code fixes and patches were applied. But according to VPNoverview.com,[13] people now worry about video conferencing that allows strangers to enter sessions and wreak havoc. They wonder whether children's private data is being monetized and express concern over poor or nonexistent data encryption. They ask about the information being shared, with whom, and for what purpose.

### Understanding Privacy Vulnerabilities

It is up to administrators and teachers to understand the vulnerabilities that online Web applications bring to the educational setting. We summarize below a list of vulnerabilities which we compiled based in our own experience and the works of Aljawarneh[14] and Dennen[15]:

1. Web-based applications servers typically reside in a variety of locations around the globe, raising privacy issues.
2. "Free" online services may monetize Personal Data, causing conflict of interest.
3. Commercially oriented online applications such as video conferencing, cloud storage, or media-sharing apps pose privacy risks. Cobbling them together increases that risk.

**Table 2. Examples of Data Privacy Regulations[16]**

| | FERPA (U.S.) | COPPA (U.S.) | GDPR (EU) |
|---|---|---|---|
| **To whom does it apply?** | Schools and HE institutions that accept Federal funding | Technology solutions that are used by children under the age of 13 | Organizations that collect Personal Data from Europeans |
| **Who or what does it protect?** | Student educational Personal Data, including records | Personal Data from children 12 years or younger (e.g., name, address, date of birth, Social Security number, location, IP address, et cetera) | The rights of the user to manage his or her Personal Data |
| **What is regulated?** | Data-use limitations; parental or adult student permission to share; length of retention | Requires published privacy policy stating how data is collected, used, or shared, including length of retention; requires parental permissions at various levels | Requires policies, plans, and procedures for collection and management (including length of retention) of user data along with evidence of compliance |
| **How to ensure that technological solutions comply** | Encrypt data and utilize enhanced identity authentication. Confirm that the product has written policies that indicate compliance. | Check that the site has a clearly published privacy policy that meets COPPA compliance. | Ensure fair and lawful data handling; state the purpose and limits for data collection, use, and transfer; minimize amounts collected; ensure data accuracy; specify storage limitations; ensure data integrity and confidentiality; be accountable. |
| **Noncompliance risks from online services** | Online services with student data may not follow FERPA compliance; the school has no control over user behavior. | Online services that aren't specifically catering to children may not be COPPA compliant. | Use of online services requires due diligence to ensure that services are compliant in collecting, storing, sharing, and protecting Personal Data. |

If yours is a small school with limited legal or technical resources, reach out to your educational authority, professional associations, or colleagues in other school systems for guidance. Raise data privacy concerns with your school board, which may engage the assistance of professionals in the community or provide guidance for a school data-security and privacy plan.

4. Online services frequently change features and/or terms of service, which may create regulatory nightmares.

### What Can Educational Administration Do?

Educational institutions can emerge safely from the COVID-19 crisis and protect the school and its students and teachers by building a systematic security and data privacy plan. This is not only a regulatory imperative but also a spiritual consideration, as we know that God is not a god of confusion (1 Corinthians 14:33). Based on several authors,[17] we provide a list of actions that educational administrators can take to improve student and teacher online data privacy:

- Establish a network of legal and information-security professionals who can advise about and securely implement new technologies. If yours is a small school with limited legal or technical resources, reach out to your educational authority, professional associations, or colleagues in other school systems for guidance. Raise data privacy concerns with your school board, which may engage the assistance of professionals in the community or provide guidance for a school data-security and privacy plan.

• Adopt a data-privacy vetting procedure for new software or applications. Question how the online service collects, shares, retains, and protects private information. Consider what rights and responsibilities belong to the educational institution and/or the user. While the sidebar, *Simple Steps to Begin Vetting an App,* is useful to any educator, it provides a clear roadmap for the small school that wants to vet new educational apps.

• Appoint someone to lead in the creation and adoption of privacy policy and user training. Policies should include data collection, management, and planned deletion, any class session recording or participant monitoring, storage of student work and grades, and appropriate behavior in collaborative online settings.

• Include parents along with students (if the students are less than 18 years of age) and adult students in discussions about student privacy and what it means for them (e.g., their right to control data about themselves: biometrics, behavior, and action such as religious practices, communication such as e-mail or voice, personal data or images, personal feelings or thoughts, movement through public space, associations with others).

• Share with parents of minors and adult students the steps the educational institution is taking to protect students. Inform them about technologies or sites used as well as instances where the institution has signed consent agreements on behalf of students. Solicit parental or adult student support for the school privacy policy to mitigate risks such as cyberbullying or unauthorized dissemination of students' and teachers' personal information.

• Develop and provide parents or adult students with an institutional privacy pledge like this sample pledge: https://studentprivacypledge.org/privacy-pledge/.

• Explain how the context (private use versus educational use) determines the ways in which an application should be used and the behaviors that students (and teachers) should follow in the educational setting.

• Share with adult students and parents of minors the steps to maintain privacy in the home educational environment (for example, disable voice assistance devices such as Alexa®, Google Assistant®, or Siri® that may be active in the environment; and ensure that the student's screen is free from open tabs or visible files before video conferencing or screen sharing occurs).

### What Can Teachers or Professors Do?

The following list gleaned from four authors[18] provides examples of steps that teachers and professors should take to protect student privacy when utilizing online applications.

• Share your institution's privacy pledge and your online classroom privacy guidelines with parents and adult students.

• Recording of classes should be done only if school policy allows. If so, seek parental or participant (if over 17) permission. Announce any recording before every session, including how a student can participate silently. Remove voice-activated devices from the vicinity of your computer/tablet, and ask students or parents to do the same.

• Use only technologies that have been vetted and approved by your institution. Be aware that by requiring a student to use a social-media platform that he or she already uses privately, the student may need to change his or her privacy settings to be compliant for educational purposes.

• Learn how to use the security and privacy features of your chosen technologies. In the COVID-19 crisis, Zoombombers (unwelcome strangers) invaded online classes and dissertation defenses because the waiting room and password features that control permission to enter were not used, and screen sharing was not turned off.

• Discuss online privacy with students to ensure that they not only exercise proper privacy protocols while working within online classes but that they also understand its importance.

### Teaching Students About Privacy

When teaching adolescents and young adults about online privacy, recognize that their views are different from those

#### Simple Steps to Begin Vetting an App

Follow these guidelines to vet any online service or app before you use it in the classroom:

1. Look for a privacy statement and read it to make sure it makes sense to you. If it seems too vague, consider another app. A privacy policy should cover how the app handles children's personal information and will explain what it collects and why.

2. Check how the app or Website seeks parental permission before it collects the personal information of minors.

3. Do a quick Web search to make sure the app is legitimate and reputable.

4. Don't use an app it if requires permission to access data or takes other actions you find intrusive or unnecessary. Very few apps need access to your contacts list or your physical location. Be very careful with these apps.

5. Communicate with parents about what apps or online services you plan to use and how you plan to use them. This allows any parent who has general privacy concerns or specific concerns with the app to voice them.

6. Remember, free apps and services have to make money. They often do this by selling users' personal information.

Finally, "Privacy Guidelines for Apps for Children" (https://www.termsfeed.com/blog/privacy-guidelines-apps-children) provides examples of app privacy policies as well as examples of privacy laws from several countries.

## Additional Resources

### COVID-19 and Privacy

Consortium for School Networking (CoSN), "COVID-19 Response: Preparing to Take School Online": https://covid19edtechguidance.com/covid-19-response-preparing-to-take-school-online/

Consortium for School Networking (CoSN), "Cyber Security Considerations in a COVID-19 World": https://covid19edtechguidance.com/cybersecurity-considerations-in-a-covid-19-world/

Janssen, David, "Secure Video Conferencing Software: How to Ensure Your Privacy": *VPNOverview.com* (April 14, 2020): https://vpnoverview.com/internet-safety/business/video-conferencing-software/

Staats, Ernest, "Remote Working: Data Privacy and Security Tips + Usage Considerations" (March 31, 2020): https://www.linkedin.com/pulse/remote-working-data-privacy-security-tips-usage-ernest-staats/

### Data Privacy in K-12 and Higher Education

Consortium for School Networking (CoSN). "Protecting Privacy in Connected Learning Toolkit: Moving From Compliance to Trust" (June 2017): https://www.cosn.org/protecting-privacy-connected-learning-toolkit (requires you to enter your information)

Durand, Michael, "To Better Protect Student Data, Know the Difference Between Security and Privacy," *EdTech: Focus on Higher Education* (February 20, 2020): https://edtechmagazine.com/higher/article/2020/02/better-protect-student-data-know-difference-between-security-and-privacy

Knorr, Caroline, "Keep Your Kids Safe Online: Essential Student Privacy Questions to Ask Your Kid's School," *Thrive Global* (December 22, 2017): https://thriveglobal.com/stories/ask-your-kid-s-school-these-essential-student-privacy-and-safety-questions/

Smith, Larry. "Student Data Privacy: What Are Your Obligations?" Student Data Privacy Consortium (February 2020): https://cdn.ymaws.com/www.a4l.org/resource/resmgr/files/sdpc-publicdocs/sdpcpresentations/2020_02_12_oetc_obligations.pdf (first half of slide show defines regulations)

of older adults. Three studies, taken as a whole, paint a picture of how students perceive online privacy and what teachers might do to engage them in discussion on the subject. Based in the findings of these studies,[19] adolescents tend to:

- View privacy in transactional terms (e.g., it is OK to give up a certain amount of privacy for the convenience of a service viewed as trustworthy and providing value);
- View privacy not as a regulatory issue but as one's own personal responsibility;
- Feel confident in their ability to manage their own online privacy;
- Have little concern about privacy when using online applications for educational purposes unless they have been negatively affected.

From the same sources,[20] we gleaned ideas that teachers or professors may consider using to engage students in discussions about data privacy. Teachers might use experiential learning to explore with students:

- How information retrieval algorithms can be politicized (e.g., searching one position on an argument leads to fewer sources with alternate views);
- How their personal information can lead to profiling for monetization purposes (different pricing for different users based on data profiling);
- Examples of how they have inadvertently shared e-mails, location, or other personal information when using a single device for school and private life; and
- What personal information is being shared in popular apps, with whom, and whether it is being indexed and archived and for how long.

### Embrace New Technologies While Promoting a Sustainable Culture of Data Privacy

Education has changed! Due to the pandemic, K-12 and higher education institutions "temporarily" enacted emergency measures that put into motion a level of online engagement never before experienced across such a broad cross-section of students and teachers. Some pieces of the experiment in Emergency Remote Teaching have failed and will likely not be repeated. But the overall experience has exposed teachers and students to a wide range of popular, easy-to-use online applications in an educational setting.

Educational institutions must now choose whether or not to embrace this new opportunity more permanently as they emerge from COVID-19. For ethical and regulatory reasons, they must carefully consider how to do so securely in ways that protect users' privacy. Teachers and administrators in faith-based educational institutions understand this responsibility in terms of the immeasurable worth of a student in God's eyes (Matthew 18:2-6, 10). Any efforts they make to protect students' personal data and thereby protect the students themselves can be considered as if they were doing it for Jesus (Matthew 25:40). It will take an entire educational village (administrators, teachers, technology and legal experts, parents and students) to create a sustainable student privacy culture. If public or business-oriented online services are invited to stay within this educational village, they must be required to demonstrate that they meet ethical and regulatory standards of security and privacy. ✐

***This article has been peer reviewed.***

**Annette Melgosa, EdD,** *is the Strategic Planning and Research Analyst for Information Technology Services of the General Conference of Seventh-day Adventists in Silver Spring, Maryland, U.S.A.*

**Ernest Staats, MSIA,** *is Technical Data Protection Officer for the General Conference of Seventh-day Adventists, and Director of Information Technology Security for Global Clients at Network Paladin, LLC in Atlanta, Georgia, U.S.A.*

**Recommended citation:**
**Annette Melgosa and Ernest Staats**, "Protecting Student Privacy: Learning From COVID-19," *The Journal of Adventist Education* 82:2 (April-June 2020): 9-15.

**NOTES AND REFERENCES**

1. Charles Hodges, et al., "The Difference Between Emergency Remote Teaching and Online Learning," *Educause Review* (March 27, 2020): https://er.educause.edu/articles/2020/3/the-difference-between-emergency-remote-teaching-and-online-learning.

2. Shadi A. Aljawarneh, "Reviewing and Exploring Innovative Ubiquitous Learning Tools in Higher Education," *Journal of Computing in Higher Education* 32 (2020): 61: https://doi.org/10.1007/s12528-019-09207-0.

3. Jessica Ruf, "'Spirit-Murdering' Comes to Zoom: Racist Attacks Plague Online Learning," *Diverse: Issues in Higher Education* 37:4 (April 16, 2020): https://diverseeducation.com/article/171746/.

4. Gerrit De Vynck and Mark Bergen, "Google Classroom Users Doubled as Quarantines Spread," *Bloomberg/Quint* (Updated April 10, 2020): https://www.bloombergquint.com/business/google-widens-lead-in-education-market-as-students-rush-online.

5. UNESCO, *Keystones to Foster Inclusive Knowledge Societies: Access to Information and Knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet* (Paris: UNESCO, 2015), 60: https://unesdoc.unesco.org/ark:/48223/pf0000232563?posInSet=3&queryId=281fd075-9301-40eb-8bce-75ce81ab21e6.

6. Ibid., 56.

7. Ibid., 57.

8. Examples used in Table 1 come from the personal experiences of the authors of this article and from the following two works: Bridge Corp, "PII vs. non-PII Data: What the Heck Is the Difference?": https://www.thebridgecorp.com/pii-vs-non-pii-data/; Michael Sweeney and Karolina Lubowicka, "What Is PII, Non-PII, and Personal Data?" (Last updated April 2, 2020): https://piwik.pro/blog/what-is-pii-personal-data/.

9. Michael Durand, "To Better Protect Student Data, Know the Difference Between Security and Privacy," *EdTech: Focus on Higher Education* (February 20, 2020): https://edtechmagazine.com/higher/article/2020/02/better-protect-student-data-know-difference-between-security-and-privacy.

10. UNESCO, *Keystones,* 56.

11. Access 4 Learning Community, "Global Education Privacy Standard (GEPS)": https://privacy.a4l.org/geps.

12. These articles provide examples of some of the online applications that schools turned to during COVID-19 as well as examples of how some of these products ran into privacy issues: De Vynck and Bergen, "Google Classroom Users Doubled as Quarantines Spread"; Ruf, 'Spirit-murdering' Comes to Zoom; Alex Konrad, "All Eyes on Zoom: How the At-Home Era's Breakout Tool Is Coping With Surging Demand—And Scrutiny," *Forbes* (May 30, 2020): https://www.forbes.com/sites/alexkonrad/2020/04/03/all-eyes-on-zoom-how-the-at-home-eras-breakout-tool-is-coping-with-surging-demand-and-scrutiny/#48e3f28e57f3.

13. PR Newswire, "VPNoverview.com: People Working From Home Often Concerned With Privacy Aspects of Video Conferencing Software" (April 2, 2020): https://www.prnewswire.com/news-releases/vpnoverviewcom-people-working-from-home-often-concerned-with-privacy-aspects-of-video-conferencing-software-301033982.html.

14. Aljawarneh, "Reviewing and Exploring Innovative Ubiquitous Learning Tools in Higher Education," 58.

15. Vanessa P. Dennen, "Technology Transience and Learner Data: Shifting Notions of Privacy in Online Learning." *The Quarterly Review of Distance Education* 16:2 (2015): 45, 49, 51.

16. In Table 2, we synthesize key points related to FERPA, COPPA, and GDPR. While the actual regulations may easily be found online, these sources provide good summaries of each: Alexander R. Schrameyer et al., "Online Student Collaboration and FERPA Considerations," *TechTrends* 60 (2020): 543-544. https://doi.org/10.1007/s11528-016-0117-5; "Understanding Child Data Privacy for Distance Learning," *IEEE Innovation at Work:* https://innovationatwork.ieee.org/understanding-child-data-privacy-for-distance-learning/; Renata Mekovec and Dijana Peras, "Implementation of the General Data Protection Regulation: Case of Higher Education Institution," *International Journal of e-Education, e-Business, e-Management and e-Learning* 10:1 (2020): 104, 105: http://www.ijeeee.org/vol10/524-CN010.pdf; Lisa W. Schifferle, "COPPA Guidance for ED Tech Companies and Schools During the Coronavirus" (April 9, 2020): https://www.ftc.gov/news-events/blogs/business-blog/2020/04/coppa-guidance-ed-tech-companies-schools-during-coronavirus; "Understand What Is Personal Information Under COPPA," Amelia Vance (November 10, 2017), YouTube. https://youtu.be/JbU0bNzqi-4.

17. The ideas presented in the bulleted list were gleaned from these articles, which present a good overview of how educational institutions can protect teachers' and students' privacy: Matthew J. Bietz et al., "Privacy Perceptions and Norms in Youth and Adults," *Clinical Practice in Pediatric Psychology* 7:1 (2019): 9; Dennen, "Technology Transience and Learner Data," 56; Megan Mann, "Coronavirus (COVID-19) Guidance for Schools," *National Association of Independent Schools* (May 1, 2020): https://www.nais.org/articles/pages/additional-covid-19-guidance-for-schools/#remote; Schifferle, "COPPA Guidance for ED Tech Companies and Schools"; Rachel L. Finn, David Wright, and Michael Friedewald, "Seven Types of Privacy," in *European Data Protection: Coming of Age,* Serge Gutwirth, Ronald Leenes, Paul de Hert, and Yves Poullet, eds. (Netherlands: Springer, 2013), 3-32.

18. The ideas presented in the bulleted list were gleaned from these articles, which together contain a number of helpful tips on how teachers and professors can protect their own and students' privacy: Patrick L. Austin, "'We Learned a Lesson.' Zoom's CEO Wants You to Trust the Company Again," *Time* (April 8, 2020): https://time.com/5816075/zoom-privacy; Dennen, "Technology Transience and Learner Data," 52-55; Mann, "Coronavirus (COVID-19) Guidance;" Ruf, "'Spirit-murdering' Comes to Zoom."

19. Together, these three studies present a cohesive view of student attitudes toward online privacy. They also provide insights into how teachers might engage them in discussions about privacy: Bietz et al., "Privacy Perceptions and Norms in Youth and Adults," 93, 99, 100: doi.org/10.1037/cpp0000 270; Margaret S. Crocco, et al., "'It's Not Like They're Selling Your Data to Dangerous People': Internet Privacy, Teens, and (Non-) Controversial Public Issues," *The Journal of Social Studies Research* 44 (2020): 25, 26: https://www.sciencedirect.com/science/article/pii/S0885985X1930172X; Dennen, "Technology Transience and Learner Data," 46, 54-56.

20. Ibid.