"Have You Seen My Cartoon Yet?": Objectives on Managing Student Projects in an Online STEAM Program

KRISTEN VOGT VEGGEBERG

The COVID-19 pandemic hit multiple industries hard, including those in out-of-school learning environments. This was especially true for programs within science, technology, engineering, arts, and math (STEAM) for elementary and middle school-aged youth. As programs are normally done within a group or classroom setting, the COVID-19 pandemic made it impossible for these programs to meet in person. If STEAM programs were not shut down or canceled outright, they were quickly transferred to an online platform, but only if the focused subject was able to be transferred online. The shift to an online platform included but was not limited to Zoom-based courses led by instructors, downloadable video content, or social media live streams hosted by different platforms. The change of communication mediums allowed for a loose version of a "class" that mitigated the need for youth participants to meet in person but still allowed them to participate in STEAM programming. Eventually, many of these programs, ranging from dance, science labs, and chess (Liao, 2016), moved to become more in-person again in 2021, with distance modes in place to protect individuals.

For many within STEAM education, this program change included the application of transferring many of their offerings online as well. While some programs sought out follow-along guides, others focused on using online technology-focused platforms to teach STEAM materials, such as coding using code.org and Robotify to teach robotics (Kalelioğlu, (2015). Other mediums that could incorporate STEAM pillars like design and inquiry-based learning became more popular at this time, such as animation, video making, and cybersecurity (Hsiaoet al., (2021). All of these followed a similar pattern and delivery of traditional programming, except for their readiness in case of a sudden transition to online learning.

Several programs continued this mode of delivering education in 2021 due to the uncertainty of rising pandemic numbers. Many institutions could not afford losing out on another year without providing programming. As a result, the changes implemented in the first year of the pandemic remained. Teachers needed to adjust online programs as necessary, where issues regarding privacy, safety, and security for the participants were involved. Incorporating cloud-based platforms was necessary not only to maintain education materials but also to preserve student projects. The following section will address how understanding the issues involving student privacy, safety, and security with these platforms is manifold.

The Use of Cloud-Based Platforms in STEAM Education

STEAM education can take many different forms, as its modalities cover a wide variety of subjects meant to engage with design and inquiry-based learning (Hawari & Noor, 2020). Subjects that are usually covered include but are not limited to robotics, chemistry, mobile app design, and drones. Instructional materials and guides for these subjects often focus on completing a final product at the conclusion of the lesson. Given the subject areas, many of these programs are inclined towards the use of technology, especially computers, and online work. For many STEAM educators, the transition to even more computer-based activities was an accepted part of many pedagogies during the COVID-19 pandemic, and the lessons learned during the pandemic regarding online education will perhaps stay permanent within computer science education. This shift to technology (the 'T' in STEAM) for use in multiple platforms of online environments is not a recent

 https://doi.org/10.56638/mtopb00123

development. In fact, many of the subjects covered within STEAM often trace back to the computer itself, a combination of both technology education trends, and the pathway seen to technology within education (Shatunova et al., 2019). Computers play a role in why many out-of-school activities and programs choose technology-heavy components, including cybersecurity, where students work by using passwords. Because of the consistent use of computers within programs, there has been a somewhat easy transition to online learning in informal STEAM education, as a system was already set in place to engage with this form of technology within learning.

Educational activities regarding computing within STEAM often happen through multiple platforms and mediums, such as animation, coding (using different languages, such as Python), and designing both graphics and apps for a tablet. A storage platform is necessary for students and teachers to save these works and have them accessible across multiple modalities, such as a laptop, tablet, or cell phone. If teachers and students have an internet connection and a browser compatible with their digital device, cloud-based storage fits their requirements for preservation and storage.

Additionally, many of the practical modes of saving student work must be done on a cloud-based platform in the modern online classroom. In previous years, other formats have been used in lieu of cloud-based storage, such as a USB drive. However, this form of data management can come under scrutiny, especially when used by underaged youth in either social or academic settings. Physical forms of data management can be lost or destroyed easily, presenting a challenge for presentations, grading, or other forms of assessment. As a result, many instructors find a cloud-based storage platform for student work beneficial. Cloud-based storage is not an anathema to the challenges presented with having adequate data storage, especially within the application of protecting student identity and intellectual property online.

Challenges to Privacy and Security with Physical and Cloud-Based Storage

Cloud-based computing has become a consistent form of data management across multiple disciplines, especially in an increasingly online world (Ercan, 2010). Previously, storing data was done in individual hardware, such as floppy disks and CDs, both of which are hard to find in current educational technology. Some hardware, such as computers and USB drives, are still being used in a certain amount to this day, especially when the curriculum involves using a non-digital connection, such as a 3D printer (Hamidi et al., 2017). The popularity of these physical forms of data storage has been beginning to wane, due to both the ease of cloud storage and the impact of not being able to readily access a file if a physical copy is lost or damaged.

Cloud-based storage, one of the most popular formats in terms of storage of digital material and media, is often used through an accessible online system, such as Google Drive (Kirayakova, 2017). This free program is one example, though other examples are DropBox and a school's online platform. However, as this involves out-of-school learning, many organizations, especially those affected by the changing budgets due to the COVID-19 pandemic, must use free online platforms, namely Google Drive. This is not only because of the ease of access for many students but also due to the budget of the programs as well. Google products, which, while free to use for all educators and students, still collect valuable data from individuals, therefore putting privacy at risk.

File Size and Data Protection

Different data and file formats are used within STEAM education, and as a result, the physical storage has been kept around even when other environments that use technology have abandoned them. As of 2022, this ranges from files with small amounts of data (such as GIFs, commonly used in graphic design), to ones that can take up large swathes of data

(namely .stls, commonly used in 3D printing). This presents a challenge concurrent to student privacy, in that these large files can often use up too much bandwidth, and an external format must be used for students to save larger projects.

One of the most pertinent issues regarding student online safety is the ability to keep these large files protected in all formats. This includes online files, which are especially vulnerable to cybercriminals. As files within STEAM education can also be transferable to technologies such as 3D printers, non-cloud-based storage may be used unless more online space is purchased. Since these files are large, they may have constraints that could end with the loss of student work—such as the conversion from a bitmap file to a GIF file in images, which would change the structure of the image and thus the student's work itself. This option of purchasing more cloud-based storage has generally not been reserved for many STEAM programs during the COVID-19 pandemic, due to additional budgeting that may not be available for cash-strapped programs during the pandemic. But this difference in storage does not allow the amount of guaranteed backup in the instance of the students' files becoming lost or damaged if something happens to the physical storage component.

Cloud-based storage presents an additional threat to student safety. Keeping student data online in a cloud-based format leads to potential hacking through the use of unsafe or untrustworthy passwords by outside parties. The potential is that student data–including created files from the students themselves–can potentially be downloaded, shared, or otherwise exploited. This includes the intellectual property of students themselves, which has been proven to have issues regarding protection. Minors, unlike adults, often are not allotted the same intellectual property rights while completing their education. In addition to this issue, the challenge of making sure student identities are kept safe is also a present issue, even more so than protecting student creative materials.

As private information can be stored on cloud platforms, the abilities of teachers, administrative professionals, and even the students themselves, need special care in the application of online privacy. One format of this is the application of an authenticator, which is discussed in further detail below. Another is password safety and making sure that students have been trained in both being alert and knowledgeable about safety online, including that of sharing passwords with peers and other individuals who might know the student. This is a policy issue that individual districts and institutions should be aware of and solve in the wake of potential breaches of safety with student information.

Ways to Move Forward

STEAM subjects require online storage, especially during the COVID-19 pandemic. As students are online, so are the artifacts and materials they design. The use of this cloud storage, however, leaves students at the mercy of potential online criminals (Wu et al., 2020). There are ways in which cloud platforms can still be used safely at a larger scale. The initial response is to move all of the program storage to a physical format, as stated above. While this seems to work, especially with the application of STL files and other files needed to be plugged via USB formats, it is not a solution that can be easily replicated to protect student privacy. This is due to the challenge seen within distance learning that many have been experiencing since 2020 during the COVID-19 pandemic. In lieu of physical storage, files stored in online cloud platforms can be used and safeguarded in two different formats: stronger passwords and double authenticator applications. Both of these forms of cybersecurity have been readily available and used by professionals within different business settings and can easily be applied within a school setting.

Stronger passwords are a general recommendation for protecting student materials online and have become part of training for students regarding online safety, such as Google's "Be Internet Awesome" (Seale & Schoenberger, 2018). This includes a password generated by a digital artificial intelligence (AI) connected to an educator's user account for a cloud storage unit. This can be seen as one of the safest formats in which passwords can be given to program participants. The reason for this is that youth passwords can be easily replicated or guessed by non-student parties (Kurpjuhn, 2015).

As a result, multiple authentications must be completed to protect the online presence of youth involved in any online platform.

Password safety has arguably been one of the primary challenges in not only student privacy but also for anyone engaging in online platforms for all users (Bartoli et al., 2015). Although there have been multiple attempts by such organizations as Google and Microsoft to promote and teach about cybersecurity (Corradini & Nardelli, 2020), the ability to reproduce protected passwords is a common hacking technique. Even with the prerequisites of different password authenticators, including longer (12 characters or more), more elaborate passwords, there are still large amounts of break-ins to online accounts, including those of students. There have been studies about passwords and youth, where youth may share a password with a close friend to show a sense of trust and camaraderie (Van Ouytsel, 2021).

Passwords are a crucial but challenging aspect of online platforms for underage youth participants to engage in. This allows for the storage and protection of materials and lessons made by and for students. But because of this ease of logging in and loading files to the cloud platform, it is easy for multiple parties to access student materials. These can include many of the previously mentioned file types, which can become quite large and need to be changed. Because of this, there leaves vulnerability of access from different parties, some of which may be seeking student materials for nefarious purposes.

Therefore, to protect students and the materials they create, other tools in addition to passwords should be used in the case of online platforms, even for storage. Authentications have also become more popular to use for safety in online formats. This requires a quickly sent code of a few numbers to be pressed into an authenticator platform. The authenticator then sends a personalized code to the individual, allowing them a brief window where they can access the platform using an individualized number generated through an automatic algorithm. This format is arguably more secure than alternative password resets, which can be frustrating for busy users who do not have the skills to remember complicated passwords (Woods & Siponen, 2018). The use of an authenticator, however, should always stay within the hands of the immediate program educator to watch over student materials online. This allows protective measures to be used for student materials stored on a cloud to be safe for storage. As youth are still at risk for outside influence for nefarious purposes, as seen within multiple examples of program participants being tricked by online cybercriminals, additional protection should be kept in this case (Rithika & Selvaraj, 2013). Authenticators, being free alongside other online platforms such as Google Drive, are usually easy to use, require no training and can be connected to different accounts for all participants. Signs of a good authenticator include a quick turnaround time to use the code (and discard it), an easily accessible medium for the user to gain the code (such as a text message or mobile app), and being protected by a password known only to the individual using the authenticator.

Although many formats of file sharing and interest are a part of STEAM education, student safety—whether for intellectual rights and purposes or for their own selves—comes first before enrichment. With the COVID-19 pandemic, more programs have become online, and more students have run the risk of either being the target of cybercriminals or having their work taken by third parties (Sastre-Merino et al., 2020). This risk, though not heavily explored for nonadult participants within design, is something that should be taken into consideration with the application of online STEAM programs, cementing the need for keeping such items as passwords and authenticators in hand. Thus, these formats, both stronger passwords and authentication, are current solutions for challenges present within protecting online cloud platforms that have been used by students and their educators.

Conclusion

The range of locations in which students learn online has expanded during the COVID-19 pandemic, thus an online platform is present within these educational activities. In regard to access across multiple computers in different

locations, there are still present issues in protecting student privacy. Issues regarding student safety with physical data have always been a concern, and one in which cloud computing has served throughout different places that require access. For many individuals and the organizations that they work with in STEAM education, digital learning has become a way of life. This need to use digital learning to protect students and continue education is true even as jurisdictions look to ease the population back into a pre-pandemic lifestyle. Protecting students and their digital artifacts is necessary for online learning environments. While cloud-based storage is a valuable tool in maintaining student progress and work, instructors must take precautions to protect student files, ensuring their safety and security while navigating these online spaces.

References

Bartoli, G., Fantacci, R., Gei, F., Marabissi, D., & Micciullo, L. (2015). A novel emergency management platform for smart public safety. *International Journal of Communication Systems*, 28(5), 928-943. https://doi.org/10.1002/dac.2716

Corradini, I., & Nardelli, E. (2020). Developing digital awareness at school: A fundamental step for cybersecurity education. In I. Corradini, E. Nardelli, and T. Ahram (Eds). *International Conference on Applied Human Factors and Ergonomics* (pp. 102-110). Springer. https://doi.org/10.1007/978-3-030-52581-1_14

Ercan, T. (2010). Effective use of cloud computing in educational institutions. *Procedia-Social and Behavioral Sciences*, 2(2), 938-942. https://doi.org/10.1016/j.sbspro.2010.03.130

Hamidi, F., Young, T. S., Sideris, J., Ardeshiri, R., Leung, J., Rezai, P., & Whitmer, B. (2017, May). Using robotics and 3D printing to introduce youth to computer science and electromechanical engineering. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 942-950). Association for Computing Machinery. https://doi.org/10.1145/3027063.3053346

Hawari, A. D. M., & Noor, A. I. M. (2020). Project based learning pedagogical design in STEAM art education. *Asian Journal of University Education*, 16(3), 102-111. https://doi.org/10.24191/ajue.v16i3.11072

Hsiao, P. W., & Su, C. H. (2021). A study on the impact of STEAM education for sustainable development courses and its effects on student motivation and learning. *Sustainability*, 13(7). https://doi.org/10.3390/su13073772

Liao, C. (2016). From interdisciplinary to transdisciplinary: An arts-integrated approach to STEAM education. *Art Education*, 69(6), 44-49. https://doi.org/10.1080/00043125.2016.1224873

Kalelioğlu, F. (2015). A new way of teaching programming skills to K-12 students: Code. org. *Computers in Human Behavior*, 52, 200-210. https://doi.org/10.1016/j.chb.2015.05.047

Kiryakova, G. (2017). Application of cloud services in education. *Trakia Journal of Sciences*, 15(4), 277-284. https://doi.org/10.15547/tjs.2017.04.001

Kurpjuhn, T. (2015). The SME security challenge. *Computer Fraud & Security*, 2015(3), 5-7. https://doi.org/10.1016/S1361-3723(15)30017-8

Rithika, M., & Selvaraj, S. (2013). Impact of social media on students' academic performance. *International Journal of Logistics & Supply Chain Management Perspectives*, 2(4), 636-640.

Sastre-Merino, S., Nuñez, J. L. M., Pablo-Lerchundi, I., & Nufiez-del-Rio, C. (2020, December). Training STEAM educators in the COVID-19 emergency situation: Redesigning teaching. In *2020 Sixth International Conference on e-Learning (econf)* (pp. 72-75). IEEE. https://doi.org/10.1109/econf51404.2020.9385461

Seale, J., & Schoenberger, N. (2018). Be Internet awesome: A critical analysis of Google's child-focused Internet safety program. *Emerging Library & Information Perspectives*, 1(1), 34–58. https://doi.org/10.5206/elip.v1i1.366

Shatunova, O., Anisimova, T., Sabirova, F., & Kalimullina, O. (2019). STEAM as an innovative educational technology. *Journal of Social Studies Education Research*, 10(2), 131-144.

Van Ouytsel, J. (2021). The prevalence and motivations for password sharing practices and intrusive behaviors among early adolescents' best friendships – A mixed-methods study. *Telematics and Informatics*, 63. https://doi.org/10.1016/j.tele.2021.101668

Woods, N., & Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human – Computer Studies*, 111, 36–48. https://doi.org/10.1016/j.ijhcs.2017.11.002