Guidelines for Reviewing Online Instructional Apps for Privacy Considerations

- Student information and academic content should be contained within a password-protected environment or controlled by teacher invitation, and not discoverable by search engines or publicly viewable on the internet.
- If the app requires the use of student PII such as name, e-mail address, or student identifier, parental approval may be required.
- Check the Terms of Service (TOS) and Privacy Policy for the following:
    a) Are there age restrictions on the use of the software? If the software is not intended for use by children under 13 years of age, it cannot be used in classes where there are children under 13. If the app is appropriate for use with children 13 or older, parental consent may still be needed. (For more information, see the FTC's Complying with COPPA: Frequently Asked Questions https://www.ftc.gov/tips-advice/business-center/ guidance/complying-coppa-frequently-asked-questions)
    b) Are all student data securely maintained, used only for educational purposes, and not shared with any other organizations?
    c) Do the modification provisions allow the provider to make a material change in the TOS or Privacy Policy without providing notice or requiring consent from the school/district? Avoid using apps with this kind of provision.
    d) Is it clear that the data collected cannot be used to advertise or market to students?
    e) Often the TOS will begin with defining PII or student data that will be used throughout the agreement. A broadly written definition of personally identifiable information can help ensure that more information is included and protected. For example, a TOS that defines PII as "only user information knowingly provided by the user" is too narrow. The vendor is only obligated to protect that specific information. A better definition would be "information provided by or about students, metadata, and user content."
    f) Be wary when the TOS talks about using de-identified data for other purposes. It can be difficult to completely de-identify data.
    g) Beware of any statement indicating that providers may view access to their services through a third-party site as an exception to established rules limiting data collection.
    h) A pro-privacy TOS will specify the types of data (or specific data elements) that the service may collect.
    i) Make sure the TOS agrees with all applicable federal, state, local or tribal laws.

For more information, see Protecting Student Privacy While Using Online Educational Services: Model Terms of Service.

The SIIA/FPF Student Privacy Pledge. In 2014, the Software & Information Industry Association (SIIA) and the Future of Privacy Forum (FPF) introduced a voluntary vendor pledge to safeguard student privacy. The pledge applies to all student personal information whether or not it is part of an "educational record" as defined by federal law, and whether it is collected and controlled by the school but warehoused offsite by a service provider, or collected directly through student use of a mobile app or website assigned by their teacher. It also applies whether or not there is a formal contract in place between the school service provider and the school. Companies that violate their pledge may be subject to action by the Federal Trade Commission as deceptive trade practices. By signing the pledge, school service providers promise they will

- not collect, maintain, use, or share student personal information beyond that needed for authorized educational/ school purposes, or as authorized by the parent/student;
- not sell student personal information;
- not use or disclose student information collected through an educational/school service (whether personal information or otherwise) for behavioral targeting of advertisements to students;
- not build a personal profile of a student other than for supporting authorized educational/school purposes or as authorized by the parent/student;
- not make material changes to school service provider consumer privacy policies without first providing prominent notice to the account holder(s) (i.e., the educational institution/agency, or the parent/student when the information is collected directly from the student with student/parent consent) and allowing them choices before data are used in any manner inconsistent with terms they were initially provided; and not make material changes to other policies or practices governing the use of student personal information that are inconsistent with contractual requirements;
- not knowingly retain student personal information beyond the time period required to support the authorized educational/school purposes, or as authorized by the parent/student;
- collect, use, share, and retain student personal information only for purposes authorized by the educational institution/agency, teacher or the parent/student;
- disclose clearly in contracts or privacy policies, including in a manner easy for parents to understand, what types of student personal information they collect, if any, and the purposes for which the information is used or shared with third parties;
- support access to and correction of student personally identifiable information by the student or their authorized parent, either by assisting the educational institution in meeting its requirements or directly when the information is collected directly from the student with student/parent consent;
- maintain a comprehensive security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information against risks—such as unauthorized access or use, or unintended or inappropriate disclosure—through the use of administrative, technological, and physical safeguards appropriate to the sensitivity of the information;
- require that other vendors with whom student personal information is shared in order to deliver the educational service, if any, are obligated to implement these same commitments for the given student personal information; and
- allow a successor entity to maintain the student personal information, in the case of a merger or acquisition by another entity, provided the successor entity is subject to these same commitments for the previously collected student personal information.

For more information, see https://studentprivacypledge.org/.