Reviewing Edtech Products Video Guide

Privacy Professional Development for Educators

iKeepSafe.org/PrivacyEducation

Privacy - Practices that Protect Information

Objectives

By the end of this unit, you will be able to:

1. Define “privacy policy”
2. Explain the basics of privacy compliance for tech products in education
3. Identify the key elements needed in a privacy assessment for technology in education

Before you review the privacy policy, answer these questions:

1. Have you fully reviewed the product for educational use? (Will student data only be used for educational use?)
2. Will students be using the product?
3. What educational benefits do you perceive the student receiving from this product? Risks?
4. Does the product require adult consent for students under 13 to use?
5. Do you have authority to provide consent?
6. *Under COPPA, schools are authorized to provide consent on behalf of parents and may approve a student’s use of an educational program. An LEA’s ability to consent on a parent’s behalf is strictly limited to the educational context. That is, an LEA may only consent on the parent’s behalf if the personal information collected is used strictly for educational purposes and not for any commercial purpose.*[1]
7. What types of information are being shared?
    a. Is there any information shared that could be considered sensitive?
    b. Are you sharing personally identifiable information? (see FERPA)

Review the Privacy Policy

1. Is there a posted privacy policy?
    a. Remember, privacy policies exist to protect companies, not user privacy.
    b. If there is no privacy policy, then you cannot access the information you need to know about what information they will gather and how they will use it. You should use a different product.
    c. If there is a privacy policy, then proceed to question 2.
2. Does it describe <u>all</u> personal information, non-personal information and/or materials collected or maintained from and about students?

[1] http://www.f3law.com/downloads/COMPLETE%20Privacy%20Guidebook%2009_10_15.pdf

a. Does it specify whether or not the product, website, online service, or mobile application allows or encourages students to make personal information publicly available, and how that may be done?
b. Does it provide an explanation of how the information and/or materials are used by the operator?
c. Does it specify whether or not any of the information and/or materials is disclosed to third parties or partners? Does it include what information might be disclosed, and why?
d. Does it include a statement that that a school has the right to review, have deleted and/or refuse to permit further collection or use of the student's information? If so, does it include information on how to do so, and the implications for a user refusing collection of data?
e. Does it include verification that the operator will allow for inspection, review and amendment or changes to student data via an authorized request from a school? Does it provide information on how a school may make such a request?

3. Does it include a statement explaining the operator's general practices related to data security and integrity, including any breach of data?
4. Does it give you the ability to contact the operator regarding the privacy policies and use of students' information? (Does it provide a name, address, telephone number and email?)

Review Advertising Practices

a. Is there an explanation of how ads will be served on the site?
    i. If so, be sure to review it
    ii. Is the operator engaging in targeted advertising? (When advertisements are custom-tailored based on information collected) Under SOPIPA, operators cannot engage in targeted advertising on their product, website, online service, or mobile application.

Safety – Responsible Products

Objectives

By the end of this unit, you will be able to:

1. Define digital safety
2. Explain the basics of digital safety
3. Identify the necessary digital safety elements for tech products in education

Questions to ask

- Is there a posted Terms of Service? Does it address inappropriate content and conduct?
- Does the TOS state minimum age of users? Do your students meet the requirement?
- Is the content age appropriate? Are users generating content? Is content (chat, images, profiles, etc.) moderated?
- If present, is the advertising age appropriate?
- What can students share publicly/privately (e.g., images, videos, etc.) and with whom?

- Do students have the ability to interact others within the product? Can students interact with adults? (If yes, then with whom? What oversight is provided?) Can student interact with each other? (If yes, what oversight is provided?)
- What kind of moderation exists within the product? Is there a report abuse mechanism? Is it anonymous?

Security – Technical Protection

Objectives

By the end of this unit, you will be able to:

1. Define digital security
2. Explain the basics of digital security
3. Identify some of the necessary security elements for tech products in schools

Operators must use and maintain reasonable security procedures and practices, taking into account available technologies and the sensitivity of the data, to safeguard and protect that information from unauthorized access, destruction, use, modification, or disclosure and ensure the confidentiality of personally identifiable information collected from or about students. Such data must be delivered to products in a secure manner and stored securely.

1. Is there a statement within the posted privacy policy explaining the operator's general practices related to data security and integrity including any breach of data?
2. Does the operator meet the following security criteria?
    a. Is student data stored securely? With sensitive data such as personal information stored separately from other data?
    b. Is student data maintained in a manner that would allow a school access to the data for which it is authorized?
    c. What employees at the company have access to student data?
        i. Access to students' sensitive data, including personally identifiable information, by member company employees is not allowed unless necessary for product operation and educational purposes. In cases where access is necessary, it must be limited to authorized employees, and a procedure must be in place to revoke access when an employee leaves the organization.
        ii. Does the operator conduct background checks on all employees who have access to student data?
    d. How does the company dispose of student data?
        i. A defined process must be in place for securely deleting and disposing of data when no longer needed, inactive data, or when requested by a school or as otherwise noted per the stated terms of use or contractual agreement with a school.
    e. Does the operator conduct security audits?
        i. A defined process must exist for the operator to conduct or have

conducted regular security audits. On an annual basis, operator must allow a school or its designated third party with either access to the results of the Member Company's security audits or with approval to conduct its own security audit of Member Company practices around its data. Schools must have access to the results of audits.

f. Does the operator have a data breach policy? It should include the following:
    i. Notification Policy and System: Member Company must have in place a notification policy and system containing following elements:
    ii. Email notification of designated persons of the school district or other educational agency.
    iii. Telephonic notification of designated persons of the school district or other educational agency.
    iv. Notification of each user affected by the breach, either separately by the vendor or in conjunction with the school district or other educational agency.
    v. Only use operators with such a policy

3. Contents of Breach Notification: Does the notice answer these questions?:
    a. What was the date of the breach?
    b. What types of information that were subject to the breach?
    c. Can you generally describe what occurred?
    d. What steps is the Vendor is taking to address the breach?
    e. Who is the company's contact person the data holder can contact?
    f. How many people were affected by the breach? Some states require notifying the Attorney General's office.
    g. If you cannot answer all of these questions from the notice, the notice is incomplete
4. How are third party service providers are handled?
    a. Does the operator have agreements in place with third parties detailing their data privacy and security policies and expectations?
        i. Does this include assurances that third parties are able to comply with these policies?
        ii. Has the operator assessed third party practices surrounding student data? Addressing:
            1. Confidentiality?
            2. Security?
            3. Transfer of personally identifiable information to the school upon request?
            4. Termination of an agreement and data deletion?
            5. Data breach? Does this include notification process?

Contracts – Amend, Renew or Enter a New Contract

Are you entering, renewing, or amending a written contract with the vendor? If so, does contract contain the following (check your state's specific requirements):

1. A description of how students can control content created for education-related purposes, along with a way to transfer content to a personal account later?
2. A description of how parents, legal guardians, or students can review and correct personally identifiable information contained in their records?
3. A description of the procedures for notifying affected parents, legal guardians, or eligible students in the event of unauthorized disclosure of student records?
4. A description of how schools and third parties will comply with FERPA?
5. An outline of actions of vendor to ensure security, including designation and training of responsible individuals?
6. An outline of actions that third parties will take to ensure student data is secure and confidential?
7. A statement that the LEA owns and controls student records?
8. A statement that student records will not be retained or available **to the third party once the contract** is over and **explain how that will be enforced?**
9. A statement **prohibiting** third parties from using personally identifiable information from student records to target advertising to students?
10. A statement **prohibiting** third parties from using student information for purposes outside of those named in the contract?

A contract lacking one of these statements/conditions is nullified. Contracts containing conditions that violate federal or state law are likely invalid as well.

**Language from Fagen Friedman and Fulfrost LLP, Law Firm:*

- *"A statement that student records continue to be the property of and under the control of the school district;*
- *A description of the means by which students may retain possession and control of their own student-generated content, if applicable, including options by which a student may transfer student-generated content to a personal account;*
- *A prohibition against the Member Company using any information in the student record for any purpose other than those required or specifically permitted by the contract;*
- *A description of the procedures by which a parent, legal guardian, or eligible student may review personally identifiable information in the student's records and correct erroneous information;*
- *A description of the actions the Member Company will take—including the designation and training of responsible individuals—to ensure the security and confidentiality of student records;*
- *A description of the procedures for notifying the affected parent, legal guardian, or eligible student in the event of an unauthorized disclosure of the student's records;*

- *A certification that a student's records shall not be retained or available to the Member Company upon completion of the terms of the contract and a description of how that certification will be enforced (NOTE: This requirement does not apply to student-generated content if the student chooses to establish or maintain an account with the third party for the purpose of storing that content, either by retaining possession and control of their own student-generated content, or by transferring student-generated content to a personal account.);*
- *A description of how the district and the Member Company will jointly ensure compliance with the federal Family Educational Rights and Privacy Act;*
- *A prohibition against the Member Company using personally identifiable information in student records to engage in targeted advertising."*

---

iKeepSafe conducts formal privacy assessents of technology products for compliance with student data privacy law. To receive a formal privacy and safety review from iKeepSafe™, visit iKeepSafe.org/Privacy.