CENTER FOR DEMOCRACY & TECHNOLOGY

Privacy and Equity in the New School Year - Review Quiz

Based on the material covered in the "Privacy and Equity in the New School Year" training material, select the best answer for each of the questions below and check yourself using the answer guide on the following pages.

Question 1.
Which of the following are important components of privacy?

- A. People's ability to control their own data
- B. Protecting students' safety and well-being by protecting their data
- C. Legal compliance
- D. All of the above

Question 2.
Which of the following is **not** likely a **new** reason to collect student data following a return to in-person learning?

- A. To conduct contact tracing
- B. To assess the security of the school's internal computer network
- C. To test for COVID-19
- D. To understand inequities that were exacerbated by the pandemic

Question 3.
Which of the following are the primary risks from collecting student data during a return to in-person learning? (Select all that apply.)

- A. Overcollection
- B. Breaches and disclosures
- C. Zoombombing
- D. Stigmatization
- E. Legal risk for the schools

Question 4.
Which of the following is a key step in building equity and engaging the community?

- A. Implement data collection quietly so as not to call attention to inequities that might embarrass some families
- B. Set up times to meet with parents solely during normal business hours when teachers are available
- C. Communicate with the community about the goals of the program, the data being collected, and the uses of the data
- D. Communicate solely by email since it is faster, and delivery is guaranteed

Question 5.
Which of the following is **not** a component of compliance with FERPA?

- A. FERPA mandates that student data may not be disclosed to anyone outside the school under any circumstances.
- B. FERPA's protections apply only to personally identifiable information.
- C. FERPA's requirements have some exceptions, including one for health and safety emergencies.
- D. FERPA applies to COVID-19-related data held by a school.
- E. FERPA compliance must be complemented by compliance with state student privacy law as well.

Question 6.
Which of the following are likely **not** examples of potentially personally identifiable information? (Select all that apply.)

- A. A school announcement that a certain school has experienced a COVID 19 outbreak
- B. General statements about class performance as a whole
- C. Grades or feedback for a particular student
- D. A statement that all absent class members have been diagnosed with COVID-19
- E. A screenshot of a video conference with students' faces and names

Question 7.
Which of the following are **not** true about FERPA's health and safety emergency exception? (Select all that apply.)

- A. Whether an "articulable and significant threat to the health or safety of a student or other individuals" is left to the determination of school officials.
- B. It permits releases of personal information only to "appropriate parties."
- C. It permits releases of personal information to the media to keep the public informed.
- D. It permits blanket releases of personal information once an emergency is declared.

Question 8.
True or false: FERPA usually applies to independent health clinics on school campuses.

- A. True, because they are on a school campus.
- B. True, because most independent health clinics receive funding from the U.S. Department of Education.
- C. False, because most independent health clinics do not receive funding from the Department of Education.
- D. False, because FERPA never applies to health records.

Question 9.
What is data governance?

- A. The laws and regulations governing data privacy and security
- B. The data science practice for ensuring that student data is accurate and complete
- C. A technical system to detect and prevent data breaches
- D. The school policies that give faculty and staff the tools to manage student data in a consistent and appropriate way

Question 10.
What are the benefits of collecting and using data for remote learning?

- A. To assess if certain teaching practices are effective
- B. To enable continued learning while schools are physically closed due to the coronavirus pandemic
- C. To foster higher student engagement during remote learning compared to low-tech options such as paper packets
- D. All of the above

Question 11.
Which of the following is an important step in inventorying new technology?

- A. Creating an open, not punitive, process to ensure that teachers feel comfortable being forthcoming
- B. Limiting the inventory to just new hardware that was adopted
- C. Working solely with IT staff, as teachers do not have the expertise to evaluate the privacy and security of education technology

Question 12.
Which of the following are important steps for protecting student privacy while incorporating new technology into existing systems? (Select all that apply.)

- A. Ensuring legal compliance with federal and state law
- B. Reviewing agreements with EdTech vendors for compliance with internal data governance policies
- C. Establishing interoperability with existing systems
- D. None of the above. It is not necessary to vet new technology since the vendor is the responsible party under FERPA, not the school.

Question 13.
Which of the following are important steps in decommissioning technology? (Select all that apply.)

- A. Downloading information such as student assignments, grades, or attendance for future use
- B. Allowing the vendor to delete data after one year, as required by FERPA
- C. Notifying students, families, and staff of the decommissioning
- D. Deleting the data, which may require more than simply disabling the teacher account
- E. The school does not have to worry about how to decommission products since the vendor is required by FERPA to properly close down the account.

CENTER FOR DEMOCRACY & TECHNOLOGY

Privacy and Equity in the New School Year - Answer Guide

Question 1.
Which of the following are important components of privacy?

- ☐ A. People's ability to control their own data
- ☐ B. Protecting students' safety and well-being by protecting their data
- ☐ C. Legal compliance
- ☒ **D. All of the above**

Correct answer: D
Explanation: Privacy is the idea that people should be able to control their own information and that the entities that collect and use that information must do so in ways that meet legal obligations and do not come at the expense of student safety and well-being.

Question 2.
Which of the following is **not** likely a **new** reason to collect student data following a return to in-person learning?

- ☐ A. To conduct contact tracing
- ☒ **B. To assess the security of the school's internal computer network**
- ☐ C. To test for COVID-19
- ☐ D. To understand inequities that were exacerbated by the pandemic

Correct answer: B
New purposes for in-person data collection include assisting health agencies in contact tracing and widespread testing and better understanding the inequities faced by students. The need to assess the security of the school's internal computer network existed prior to the pandemic and is not new.

Question 3.
Which of the following are the primary risks from collecting student data during a return to in-person learning? (Select all that apply.)

- ☒ **A. Overcollection**
- ☒ **B. Breaches and disclosures**
- ☐ C. Zoombombing
- ☒ **D. Stigmatization**
- ☒ **E. Legal risk for the schools**

Correct answers: A, B, D, E
While Zoombombing is a privacy and security risk, video conferencing is not the means through which schools are collecting data to return to in-person instruction.

Question 4.
Which of the following is a key step in building equity and engaging the community?

- ▢ A. Implement data collection quietly so as not to call attention to inequities that might embarrass some families
- ▢ B. Set up times to meet with parents solely during normal business hours when teachers are available
- ☒ **C. Communicate with the community about the goals of the program, the data being collected, and the uses of the data**
- ▢ D. Communicate solely by email since it is faster, and delivery is guaranteed

Correct answer: C
Community engagement means apprising the community of the goals of the program, the data being collected, the uses of the data, and the community's rights to review, amend, or delete collected information, or possibly opt out of the collection entirely.

Question 5.
Which of the following is **not** a component of compliance with FERPA?

- ☒ **A. FERPA mandates that student data may not be disclosed to anyone outside the school under any circumstances.**
- ▢ B. FERPA's protections apply only to personally identifiable information.
- ▢ C. FERPA's requirements have some exceptions, including one for health and safety emergencies.
- ▢ D. FERPA applies to COVID-19-related data held by a school.
- ▢ E. FERPA compliance must be complemented by compliance with state student privacy law as well.

Correct answer: A
FERPA may permit sharing with partners under certain circumstances, such as through the health and safety emergency exception or when only deidentified data is shared.

Question 6.
Which of the following are likely **not** examples of potentially personally identifiable information? (Select all that apply.)

- ☒ **A. A school announcement that a certain school has experienced a COVID 19 outbreak**
- ☒ **B. General statements about class performance as a whole**
- ▢ C. Grades or feedback for a particular student
- ▢ D. A statement that all absent class members have been diagnosed with COVID-19
- ▢ E. A screenshot of a video conference with students' faces and names

Correct answers: A and B
These pieces of information likely cannot be used to identify or distinguish a person, either directly or in combination with other information, and therefore likely are not PII.

Question 7.
Which of the following are **not** true about FERPA's health and safety emergency exception? (Select all that apply.)

- ▢ A. Whether an "articulable and significant threat to the health or safety of a student or other individuals" is left to the determination of school officials.
- ▢ B. It permits releases of personal information only to "appropriate parties."
- ☒ **C. It permits releases of personal information to the media to keep the public informed.**
- ☒ **D. It permits blanket releases of personal information once an emergency is declared.**

Correct answers: C and D
The health and safety exception only permits releases of PII to "appropriate parties" such as health agencies or medical professionals and generally does not allow blanket releases of information.

Question 8.
True or false: FERPA usually applies to independent health clinics on school campuses.

- ▢ A. True, because they are on a school campus.
- ▢ B. True, because most independent health clinics receive funding from the U.S. Department of Education.
- ☒ **C. False, because most independent health clinics do not receive funding from the Department of Education.**
- ▢ D. False, because FERPA never applies to health records.

Correct answer: C
FERPA applies only to education records "maintained" by or on behalf of "an educational agency or institution" that has received funds from the U.S. Department of Education, and independent health clinics usually do not receive U.S. Department of Education funding.

Question 9.
What is data governance?

- ▢ A. The laws and regulations governing data privacy and security
- ▢ B. The data science practice for ensuring that student data is accurate and complete
- ▢ C. A technical system to detect and prevent data breaches
- ☒ **D. The school policies that give faculty and staff the tools to manage student data in a consistent and appropriate way**

Correct answer: D
Data governance means the school policies that, along with the training that accompanies them, give faculty and staff tools to manage student data in a consistent and appropriate way.

Question 10.
What are the benefits of collecting and using data for remote learning?

- ▢ A. To assess if certain teaching practices are effective
- ▢ B. To enable continued learning while schools are physically closed due to the coronavirus pandemic

- ▢ C. To foster higher student engagement during remote learning compared to low-tech options such as paper packets
- ☒ **D. All of the above**

Correct answer: D
Collecting and using data for remote learning may allow for a higher level of engagement between teachers and students than other options such as paper packets, and may allow teachers to gather data to better understand effective teaching practices.

Question 11.
Which of the following is an important step in inventorying new technology?

- ☒ **A. Creating an open, not punitive, process to ensure that teachers feel comfortable being forthcoming**
- ▢ B. Limiting the inventory to just new hardware that was adopted
- ▢ C. Working solely with IT staff, as teachers do not have the expertise to evaluate the privacy and security of education technology

Correct answer: A
Inventorying technology requires working with teachers to inventory what, if any, technology they have adopted during remote learning, creating an open process, not a punitive one, and taking an expansive view of technology, including everything from streaming lessons to learning management systems.

Question 12.
Which of the following are important steps for protecting student privacy while incorporating new technology into existing systems? (Select all that apply.)

- ☒ **A. Ensuring legal compliance with federal and state law**
- ☒ **B. Reviewing agreements with EdTech vendors for compliance with internal data governance policies**
- ☒ **C. Establishing interoperability with existing systems**
- ▢ D. None of the above. It is not necessary to vet new technology since the vendor is the responsible party under FERPA, not the school.

Correct answers: A, B, C
FERPA applies to schools, not vendors. Incorporating new technology requires ensuring its compliance with federal and state law, reviewing agreements with EdTech vendors for adherence to internal data governance policies such as for obtaining consent and use, and ensuring that the new technology is compatible with existing systems.

Question 13.
Which of the following are important steps in decommissioning technology? (Select all that apply.)

- ☒ **A. Downloading information such as student assignments, grades, or attendance for future use**
- ▢ B. Allowing the vendor to delete data after one year, as required by FERPA

- ☒ **C. Notifying students, families, and staff of the decommissioning**
- ☒ **D. Deleting the data, which may require more than simply disabling the teacher account**
- ☐ E. The school does not have to worry about how to decommission products since the vendor is required by FERPA to properly close down the account.

Correct answers: A, C, D
FERPA does not explicitly require data to be deleted after a year or products to be decommissioned. When decommissioning technology, schools should download information for future use, notify students, families, and staff of the decommissioning, and delete the data, which may require reviewing the tool's terms of service.