Student Data Recovery
KC Policy # MISC 300

APPLIES TO: Administration, Information Technology (IT), Records, Safety and Emergency Preparedness

ISSUED: *October 11, 2023*

KEYWORDS: Disaster, recovery, data files, backup, SARA (State Authorization Reciprocity Agreements), NC-SARA

EFFECTIVE: *October 11, 2023*

PURPOSE: To provide a disaster recovery plan designed to adequately backup data files, particularly with respect to the protection of student records in the event of a catastrophic event.

DEFINITION OF TERMS IN THIS POLICY:

1. **Disaster** is a catastrophic event that can be caused by a variety of factors, such as hardware or software failures, natural disasters like floods or fires, cyber-attacks, human error, and others. In which a large amount of data are lost, corrupted, or destroyed, resulting in significant damage to the college.
2. The **Family Educational Rights and Privacy Act (FERPA)** is a federal law that affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student ("eligible student"). The FERPA statute is found at 20 U.S.C. § 1232g and the FERPA regulations are found at 34 CFR Part 99.

POLICY DETAILS:

Goal

By implementing this student data recovery policy, Kettering College can ensure that its third-party service providers are responsible for ensuring the protection and recoverability of student data in the event of a disaster or data loss. The policy also ensures that Kettering College is compliant with relevant laws and regulations governing student data privacy and protection.

1. Regular Backups: Kettering College will work with its third-party cloud-based service providers to ensure that all student data is regularly backed up to a secure location. Backups will be performed regularly, and the service provider will be responsible for ensuring that backups are stored in a secure off-site location. Service provider will make reasonable efforts to air gap these.

2. Data Recovery Plan: Kettering College will establish a clear plan for recovering lost or damaged student data. The IT department will work with the service providers to follow established procedures for data restoration. The plan will include steps for identifying the cause of the data loss or damage, prioritizing recovery efforts, and restoring the data to its original state.

3. Communication Plan: Kettering College will have a communication plan in place to notify students and personnel of any data loss or damage. The plan will outline the timeframe for recovery and any potential impact on academics.

or administrative operations. The college will work with the service providers to keep students and staff informed through appropriate communication channels.

4. Data Protection: Kettering College will work with its third-party service providers to implement measures to protect student data from loss, damage, or unauthorized access. These measures will include security protocols, encryption, access controls, and firewalls. The service provider will be responsible for ensuring that all student data is stored on secure servers that are regularly updated and patched to prevent vulnerabilities.
5. Testing and Monitoring: Kettering College will periodically test the data recovery plan and monitor the third-party service provider's data storage systems to ensure that student data is secure and recoverable in the event of a disaster. The IT department will work with the service provider to conduct regular audits of the backup system and perform periodic tests of the recovery process to identify any weaknesses or areas for improvement.
6. Legal Compliance: Kettering College will ensure that its third-party service provider complies with all relevant laws and regulations governing student data privacy and protection, such as the Family Educational Rights and Privacy Act (FERPA). The college will work with the service provider to ensure that all student data is stored and protected in accordance with these regulations.
7. Training and Education: Kettering College will provide regular training and education to students and staff on the importance of data protection and recovery. All new employees will be required to complete data protection training as part of their onboarding process, and refresher courses will be offered to all staff on an annual basis. Additionally, students will be provided with data protection training on a regular basis.
8. Location of Plan: The student data recovery plan should be stored in a secure location accessible to relevant staff members to include KC IT department, KH director of information security, and senior administrators. The plan will be stored in Teams, a secure cloud-based collaboration platform, where authorized staff members can access it from any location with an internet connection. Additionally, having a printed copy of the plan located in the IT department can serve as a backup in case of a technology failure or other unexpected event. It is important to ensure that the printed copy is stored in a secure location to prevent unauthorized access or theft.
9. The Kettering College Technology Committee will be responsible for approving the student data recovery plan and any subsequent changes to it.

RESOURCES/REFERENCES:
Related KHN Policy: N/A
References: Kettering College Student Data recovery plan
Maintained by: Office of Information Technology
HISTORY OF REVISION:
Original date: October 11, 2023
Revision dates: N/A