April 24, 2000

Dr. Claire Van Ummersen
President
Cleveland State University
1983 East 24th Street
Cleveland, Ohio 44115

Dear Dr. Van Ummersen:

Congressman Dennis J. Kucinich recently contacted the Secretary of Education on behalf of students at Cleveland State University (University), expressing concern that the privacy of the students' education records is being compromised. Specifically, the students have stated that because of unsecure passwords based on birth dates and zip codes, together with the practice of posting student grades according to the student's PeopleSoft code number, computer hackers are able to access the students' financial aid records and grades.

Our Office has not received any complaints from students at the University. Therefore, we are not initiating an investigation under the Family Educational Rights and Privacy Act (FERPA) at this time. However, we ask that you respond to the issues raised in the Congressman's letter so that we may assist you in complying with FERPA. Enclosed is a copy of Congressman Kucinich's letter.

FERPA is a federal law that protects the privacy interests of parents and eligible students in education records maintained by educational agencies and institutions that receive funds under any program administered by the Secretary of Education. This Office administers FERPA (20 U.S.C. § 1232g) and is responsible for investigating complaints and providing technical assistance to educational agencies and institutions to ensure compliance with FERPA and its implementing regulations found at 34 CFR Part 99.

FERPA provides that eligible students -- students who are 18 years of age or attending a postsecondary institution -- have the right to inspect and review (or obtain access to) their education records and to seek to have them amended in certain circumstances. See 34 CFR Part 99, Subparts B and C. Eligible students must also provide a signed and dated written consent in accordance with § 99.30 of the FERPA regulations before an institution discloses education records, or personally identifiable information from education records, to third parties. There are several statutory exceptions to this "prior written consent" rule where nonconsensual disclosure to third parties is permitted. See 34 CFR § 99.31.

In order for this Office to provide technical assistance to the University, we need more information about your computer based student record system. Please submit a description of the method or methods used by the University to allow students to obtain access to their own education records, including access by telephone and computer. In addition, please provide a description of the criteria for assigning passwords or personal identification numbers (PIN). In particular, please address Congressman Kucinich's statement that the University has refused to allow students to change their passwords to include case sensitive alpha-numerics. In addition, we ask that you describe in detail how the University posts grades so that we may also advise you on that issue. In order the assist your efforts, we offer the following general comments regarding the applicability of FERPA to the electronic storage, transmission, and communication of education records.

Many institutions have asked for guidance regarding policies that allow students to obtain access to their own records through the use of a PIN or other form of "electronic signature." In cases where prior written consent is required under FERPA, the consent must be *signed* and *dated* and must specify the records that may be disclosed, state the purpose of the disclosure, and identify the party or class of parties to whom the disclosure may be made. See 34 CFR § 99.30. For example, an eligible student must provide written consent in accordance with the requirements of § 99.30 before an institution issues the student's transcript to a prospective or current employer. This Office expects to issue guidance in the near future regarding the use of electronic signatures for purposes of meeting the prior written consent rule under FERPA.

The written consent requirements in § 99.30 do not apply, however, when eligible students obtain access to their own records. Indeed, when an institution is authorized to disclose information from education records without a signed and dated written consent, including disclosures to eligible students under § 99.31(a)(12), FERPA does not specify or restrict the method of disclosure. See 34 CFR § 99.31. Because FERPA restricts disclosure of education records to unauthorized parties without the eligible student's prior consent, it is incumbent upon an institution to ensure that computer databases and other systems function so that only authorized parties may obtain access to the records. In these cases, the primary considerations are *identification* of authorized recipients of information and *security of transmission* so that records are disclosed only to authorized parties.

Institutions and agencies have long been required to establish and monitor reasonable and appropriate physical, technical, and administrative safeguards to protect against the unauthorized access to or disclosure of information from education records and to maintain the integrity of information in those records. FERPA does not mandate any specific method, such as encryption technology, for achieving these standards with

electronic storage and disclosure of information from education records. However, reasonable and appropriate steps consistent with current technological developments should be used to control access to and safeguard the integrity of education records in electronic data storage and transmission, including the use of e-mail, Web sites, and other Internet protocols.

This Office has advised previously that an institution may use a PIN combined with the student identification number to authorize disclosure of information from education records directly to the eligible student, but only so long as the institution allows only the eligible student to have access to the PIN. If the institution allows anyone else, including administrative staff, to have access to a student's PIN, there can be no assurance that the disclosure will be made only to an authorized party as required under FERPA. Regardless of the methods an institution uses to allow students to obtain access to their records, the primary consideration is whether there is reasonable assurance that the information is accessible only to the student.

The integrity and security of data storage and transmission are essential to ensure that information is disclosed only to those who are authorized to receive it. In this regard, institutions are responsible for ensuring that the policies or practices they employ are in compliance with FERPA. We look forward to working with you on this matter. Please send your response to the issues disclosed above to the following address:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202-4605

In addition, our telephone number is (202) 260-3887. As always, this Office is available to respond to any questions you might have or offer any technical assistance you may require as you prepare your response.

Sincerely,

LeRoy S. Rooker
Director
Family Policy Compliance Office

cc: Congressman Dennis J. Kucinich