UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF MANAGEMENT

Privacy, Information, and Records Management Services

May 28, 2014

Khaliah Barnes
Director, EPIC Student Privacy Project
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009

RE: FOIA Request No. 14-01135-F

Dear Ms. Barnes:

This is an interim response to your fax dated April 15, 2014, to the U.S. Department of Education (Department) requesting information pursuant to the Freedom of Information Act (FOIA), 5 U.S.C. § 552. Your request was forwarded to the Family Policy Compliance Office ("FPCO") to search for documents that may be responsive to your request.

On May 14, 2014, the Department sent you a letter (copy enclosed) in regards to a telephone conversation [with Gregory A. Smith, Director of the FOIA Service Center, and Regina Miles, FOIA Coordinator within FPCO] on Friday, May 9, 2014, asking you to narrow the scope of the request, but you advised the Department that you would like the scope of the request to remain as it is written.

Enclosed is a CD containing 551 pages of documents responsive to your request, which were processed in FPCO.

However, certain information has been withheld according to the FOIA exemption specified below:

- Personal Information is withheld under (b)(6) of the FOIA, 5 U.S.C. § 552(b)(6) and Departmental Regulation 34 CFR § 5.71(a). Disclosure of this information would constitute a clearly unwarranted invasion of personal privacy.

You have the right to appeal this initial decision by writing to the address below 35 days from the date of this letter. Your appeal should be accompanied by a copy of your initial letter of request and this denial letter, and should contain any evidence or argument you wish the Department to consider in making an administrative determination on your appeal.

Appeal Address:

U.S. Department of Education
Office of Management
400 Maryland Avenue, SW, LBJ-2W311
ATTN: Appeals Office
Washington, DC 20202-4500

Or, you may complete the online FOIA appeal form, located at:
http://www.ed.gov/policy/gen/leg/foia/foia_appeal_form_1.html.

At this time, the Department is continuing to process your request and your FOIA request case file remains open. It will not close until the Department provides you with a response regarding outstanding responsive documents from FPCO.

If you have any questions, please contact the FOIA Service Center at (202) 401-8365 or EDFOIAManager@ed.gov.

Sincerely,

Maria-Teresa Cueva
FOIA Public Liaison, OM/PIRMS

Enclosures

[redacted]

APR 15 2009

Dear [redacted]:

This is in response to your September 15, 2007, and December 29, 2008, letters to this Office in which you allege that the [redacted] (District) violated your rights under the Family Educational Rights and Privacy Act (FERPA). Based on information you provided to this Office, it appears that you are a former student and that you are 18 years of age or older. You state the following with regard to your allegation:

> ...[w]e believe that the [District] taped [its July 20, 2006] closed session [school board meeting], and rather than furnish us with a copy of this tape as we requested in our [March 8, 2007] open records request, attempted to substitute a certified agenda after the local District Attorney's office began an investigation. Attached to the original complaint is a letter from the district's attorney purporting that the tape "malfunctioned."

Specifically, you appear to allege that the District failed to provide you access to audio-visual tapes and other documents that you believe the District maintained to memorialize a July 20, 2006, school board meeting which included information from your education records pertaining to a grievance you made against the District. This Office administers FERPA, which addresses issues pertaining to education records.

FERPA is a Federal law that gives parents and eligible students the right to have access to his or her education records, the right to seek to have the records amended, and the right to have some control over the disclosure of information from the records. When a student reaches the age of 18 or attends an institution of postsecondary education, that student is deemed "eligible" and all of the rights afforded by FERPA transfer from the parents to the student. The term "education records" is defined as those records that contain information directly related to a student and which are maintained by an educational agency or institution or by a party acting for the agency or institution. Enclosed for your information is a FERPA fact sheet.

Under FERPA, a school must provide a student with an opportunity to inspect and review his or her education records within 45 days of the receipt of a request. A school is required to provide a student with copies of education records or make other arrangements when a failure to do so would effectively prevent the student from obtaining access to the records. A case in point would be a situation in which the student does not live within commuting distance of the school.

Based on the information in your complaint form, it appears that you lived within commuting distance to the District at the time you made your request and the District would only be required to provide you with an opportunity to inspect and review your education records, although it could choose to provide you with copies.

Additionally, FERPA would not require a school to provide students documents such as school calendars, updates, or notices of parent/teacher conferences, employee qualifications, or student handbooks, because such documents do not generally contain information that is directly related to individual students. Likewise, a school would not be required to notify students about school plays, spelling bees, or sporting events in which they may be participating.

In accordance with FERPA, a school generally is not required to maintain particular education records or education records that contain specific information. Rather, a school is required to provide certain privacy protections relative to those records it selects to maintain. Nor does FERPA require schools to create or to re-create lost or destroyed education records. It may destroy education records without notice to the student, unless there is an outstanding request from the student to inspect and review such records.

Additionally, FERPA generally requires that an eligible student provide written consent before a school can disclose education records to a third party. However, a school is not required to provide any third party with access to education records, even when the student has provided prior written consent for such records to be disclosed to that third party. Therefore, although the District is permitted to do so, it is not required to provide your parents or other third parties with access to, or copies of, your education records in response to a request from you.

This Office investigates those timely complaints that contain specific allegations of fact giving reasonable cause to believe that a school has failed to comply with FERPA. A timely complaint is defined as one that is submitted to this Office within 180 days of the date that the complainant knew or reasonably should have known of the alleged failure to comply with FERPA. Based on information you provided this Office and statements made by the District in regard to your request for access to audio-visual tapes or other documents relating to the July 20, 2006, school board meeting, you have not provided any evidence for this Office to determine that the District maintained any audio-visual tapes or other such documents to which you have not already been provided access. Accordingly, no basis exists for this Office to investigate your allegation that the District denied you access to your education records.

I trust the above information is helpful in explaining the scope and limitations of FERPA as it relates to your concerns.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

Enclosure

Ms. Paula Schwartz
Superintendent
Region 10 School District of Connecticut
24 Lyons Road
Burlington, Connecticut 06013

APR 15 2009

Dear Ms. Schwartz:

This is to provide the Region 10 School District of Connecticut (District) with technical assistance regarding recent changes to the definition of "personally identifiable information" in the Family Educational Rights and Privacy Act (FERPA) regulations. On December 9, 2008, the Department issued new regulations which revised the term "personally identifiable information" as follows:

> The term includes, but is not limited to –
>
> (a) The student's name;
>
> (b) The name of the student's parent or other family members;
>
> (c) The address of the student or student's family;
>
> (d) A personal identifier, such as the student's social security number, student number, or biometric record;
>
> (e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
>
> (f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
>
> (g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

34 CFR § 99.3 "Personally Identifiable Information." *See* the discussion in the *Analysis of Comments and Changes* section of the final regulations, 73 FR 74829-74833.

The preamble to the December 9, 2008, FERPA regulations explains in depth the parameters of information that is personally identifiable to a student. The discussion of Personally Identifiable Information published in both the Notice of Proposed Rulemaking (NPRM) (73 FR, March 24, 2008) and the Final

Regulations are intended to provide agencies and institutions additional information to assist them in interpreting when information is personally identifiable to a student. In this regard, the discussion beginning on page 74831 under Personally Identifiable Information states:

> The simple removal of nominal or direct identifiers, such as name and SSN (or other ID number), does not necessarily avoid the release of personally identifiable information. Other information, such as address, date and place of birth, race, ethnicity, gender, physical description, disability, activities and accomplishments, disciplinary actions, and so forth, can indirectly identify someone depending on the combination of factors and level of detail released. Similarly, and as noted in the preamble to the NPRM, 73 FR 15584, the existing professional literature makes clear that public directories and previously released information, including local publicity and even information that has been de-identified, is sometimes linked or linkable to an otherwise de-identified record or data set and renders the information personally identifiable. The regulations properly require parties that release information from education records to address these situations.
>
> We removed the "easily traceable" standard from the definition of personally identifiable information because it lacked specificity and clarity. We were also concerned that the ``easily traceable" standard suggested that a fairly low standard applied in protecting education records, i.e., that information was considered personally identifiable only if it was easy to identify the student. The removal of the "easily traceable" standard and adoption of the standards in paragraphs (f) and (g) will not affect a parent's right under FERPA to inspect and review his or her child's education records. Records that teachers and other school officials maintain on students that use only initials, nicknames, or personal descriptions to identify the student are education records under FERPA because they are directly related to the student. Further, records that identify a student by initials, nicknames, or personal characteristics are personally identifiable information if, alone or combined with other information, the initials are linked or linkable to a specific student and would allow a reasonable person in the school community who does not have personal knowledge about the situation to identify the student with reasonable certainty. For example, if teachers and other individuals in the school community generally would not be able to identify a specific student based on the student's initials, nickname, or personal characteristics contained in the record, then the information is not considered personally identifiable and may be released without consent. Experience has shown, however, that initials, nicknames, and personal characteristics are often sufficiently unique in a school community that a reasonable person can identify the student from this kind of information even without access to any personal knowledge, such as a key that specifically links the initials, nickname, or personal characteristics to the student. In contrast, if a teacher uses a special code known only by the teacher and the student (or

parent) to identify a student, such as for posting grades, this code is not considered personally identifiable information under FERPA because the only reason the teacher can identify the student is because of the teacher's access to personal knowledge of the relevant circumstances, i.e., the key that links the code to the student's name.

In response to the commenter who stated that a school should not be prevented from releasing information when the subject of the record has waived any pretense of confidentiality by contacting the media and making the incident well-known in the community, we have found that in limited circumstances a parent or student may impliedly waive their privacy rights under FERPA by disclosing information to parties in a special relationship with the institution, such as a licensing or accreditation organization. However, we have not found and do not believe that parents and students generally waive their privacy rights under FERPA by sharing information with the media or other members of the general public. The fact that information is a matter of general public interest does not give an educational agency or institution permission to release the same or related information from education records without consent.

The "reasonableness" standards in paragraphs (f) and (g) of the new definition, which replace the ``easily traceable" standard, do not require the exercise of subjective judgment or inquiries into a requester's motives. Both provisions require the disclosing party to use legally recognized, objective standards by referring to identification not in the mind of the disclosing party or requester but by a reasonable person and with reasonable certainty, and by requiring the disclosing party to withhold information when it reasonably believes certain facts to be present. These are not subjective standards, and these changes will not diminish the privacy protections in FERPA.

The standard proposed in paragraph (f) regarding the knowledge of a reasonable person in the school or its community was not intended to describe the technological or scientific skill level of a person who would be capable of re-identifying statistical information or redacted records. Rather, it provided the standard an agency or institution should use to determine whether statistical information or a redacted record will identify a student, even though certain identifiers have been removed, because of a well-publicized incident or some other factor known in the community. For example, as explained in the preamble to the NPRM, 73 FR 15583, a school may not release statistics on penalties imposed on students for cheating on a test where the local media have published identifiable information about the only student (or students) who received that penalty; that statistical information or redacted record is now personally identifiable to the student or students because of the local publicity.

Paragraph (f) in the proposed definition provided that the agency or institution must make a determination about whether information is personally identifiable information not with regard to what someone with personal knowledge of the relevant circumstances would know, such as the principal who imposed the penalty, but with regard to what a

reasonable person in the school or its community would know, i.e., based on local publicity, communications, and other ordinary conditions. We agree with the comment that the "school or its community" standard was confusing because it was not clear whether just the school itself or the larger community in which the school is located is the relevant group for determining what a reasonable person would know.

We are changing this standard in paragraph (f) to the "school community" and by this change we mean that an educational agency or institution may not select a broader "community" standard when the information to be released would be personally identifiable under the narrower ``school" standard. For example, it might be well known among students, teachers, administrators, parents, coaches, volunteers, or others at the local high school that a student was caught bringing a gun to class last month but generally unknown in the town where the school is located. In these circumstances, a school district may not disclose that a high school student was suspended for bringing a gun to class last month, even though a reasonable person in the community where the school is located would not be able to identify the student, because a reasonable person in the high school would be able to identify the student. The student's privacy is further protected because a reasonable person in the school community is also presumed to have at least the knowledge of a reasonable person in the local community, the region or State, the United States, and the world in general. The ``school community" standard, therefore, provides the maximum privacy protection for students.

We also have revised paragraph (f) in the definition of personally identifiable information to change the reference "school or its community" to "school community." In paragraph (g) of the definition of personally identifiable information, we removed the requirement that the requester have "direct, personal knowledge." As revised, paragraph (g) provides that personally identifiable information means information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the record relates.

If you have any questions, please do not hesitate to contact this Ms. Ingrid Brault at 202-260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

cc: Ms. Christine L. Chinni

(b)(6)

APR 15 2009

Dear (b)(6)

This is in response to the complaint you submitted to this Office on March 16, 2009. You allege that your daughter's school district violated your rights under the Family Educational Rights and Privacy Act (FERPA). This Office administers FERPA which addresses issues pertaining to education records. Specifically, you allege that your child's school principal violated FERPA when she disclosed your daughter's education records to her step-mother and grandmother during a November 11, 2008, meeting at the school.

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 information from the records. Education records are those records that are directly related to a student and that are maintained by an educational agency or institution or a party acting for the agency or institution.

FERPA is a Federal law that gives parents, custodial and noncustodial alike, the right to inspect and review their children's education records, unless the school has evidence that there is a court order or State law which specifically provides to the contrary. A school may ask for legal certification denoting parenthood, such as a birth certificate or court order, from the parent requesting access. Therefore, if the child's father has FERPA rights and provided consent to the District to allow you daughter's stepparent and grandmother to attend the meeting and have access to your child's education records, then FERPA would permit the disclosure.

Additionally, the term "parent" is defined as including natural parents, a guardian, or an individual acting as a parent in the absence of a parent or a guardian. The Department has determined that a parent is absent if he or she is not present in the day-to-day home environment of the child. Accordingly, a stepparent has rights under FERPA where the stepparent is present on a day-to-day basis with the natural parent and child and the other parent is absent from that home. In such cases, stepparents have the same rights under FERPA as do natural parents. You do not explain, however, the custody arrangement of your daughter.

We are enclosing a complaint form and guidance document for your reference. If after a review of this material, you continue to believe that the school violated FERPA, please complete the enclosed complaint form including the name and address of the school district that your daughter

attends, the name of the school official that disclosed the education records and the specific education records that were disclosed, and submit it to this Office. We will review the information you provide and take any necessary action.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

Enclosure

(b)(6)

APR 14 2009

Dear (b)(6)

This is in response to your February 3, 2009, letter to this Office in which you allege that the (b)(6) (District) violated your rights under the Family Educational Rights and Privacy Act (FERPA) when it disclosed information from your daughter's education records to third parties without your prior written consent. This Office administers FERPA which addresses issues that pertain to education records.

Specifically you allege:

> . . . On January 30, 2009 school Principal (b)(6) held an assembly of all middle school students and read off the names of those he claimed were failing. Those names included my daughter who was absent that day. . . .
>
> On Monday, February 2, 2009 (b)(6) repeated the assembly, again including my daughter who had just returned after a five day absence.
>
> On Tuesday February 3, 2009 (b)(6) once again held the assembly but this time he not only read the names of those who he claimed are failing but also listed the classes each was reportedly failing. . . .

FERPA is a Federal law that gives 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 information from the records. The term "education records" means those records that are directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution. Enclosed for your information are a FERPA fact sheet, guidance document, and complaint form.

Under FERPA, a school may not generally disclose personally identifiable information from a minor student's education records to a third party unless the student's parent has provided written consent. However, please note that FERPA does not protect the confidentiality of information in general and, therefore, does not apply to the disclosure of information derived from a source other than education records, even if education

records exist which contain that information. Rather, FERPA protects information derived from education records from improper disclosure. As a general rule, information obtained through personal knowledge or observation, and not from an education record, is not protected from disclosure under FERPA.

This Office investigates those timely complaints that contain specific allegations of fact giving reasonable cause to believe that a violation of FERPA has occurred. If you wish this Office to further consider your allegation, please complete the enclosed complaint form and include the following information: the name of the student; the name and address of the superintendent of the District; and verification that the information disclosed by the principal is information contained in your daughter's education records. For example, could (b)(6) or another school official view information in your daughter's education records and come to the conclusion that she was failing in one or more of her classes at the time you allege (b)(6) made such announcements at the assemblies? We will review the information you submit and take any appropriate action.

I trust that the above information is helpful in explaining the scope and limitations of FERPA as it relates to your concern.

Sincerely,

Ricky C. Norment
Program Analyst
Family Policy Compliance Office

Enclosures

Mr. Alan Horwitz
President
National Technical Institute for the Deaf
52 Lomb Memorial Drive
Rochester, New York 14623

APR 14 2009

Dear Mr. Horwitz:

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements.

We are responding to a letter that this Office received on September 20, 2008, from a student who alleged that the National Technical Institute for the Deaf (Institute) violated FERPA when a laptop was stolen from the Institute on August 25, 2008. The enclosed August 29, 2008, letter to the student from you indicates that he was informed of the theft and told that the Institute was unable to determine if anyone had accessed the education records of the students that were on the laptop. Furthermore, you explained the steps that the student may want to take with regard to safety and protection of the information.

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the December 8, 2009, FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. *See* 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes of unauthorized access and disclosure. Although FERPA does not dictate requirements for safeguarding education records, the Department encourages the holders of personally identifiable information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.

- organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.
- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.
- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

cc: Student

Ms. Barbara A. Marshall
Superintendent
St. Joseph County Independent School District
62445 Shimmel Road
Centreville, Michigan 49032

APR 14 2009

Dear Ms. Marshall:

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements. We are responding to your March 16, 2009, correspondence in which you explain that a former employee at St. Joseph County Independent School District improperly disclosed (b)(6) the special education records of approximately 50 students and informed us of the steps taken since the breach occurred.

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the December 9, 2008, FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. *See* 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes of unauthorized access and disclosure. Although FERPA does not dictate requirements for

safeguarding education records, the Department encourages the holders of personally identifiable information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.
- Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.
- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.
- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at

http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and
http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

(b)(6)

APR – 9 2009

Dear (b)(6)

This is in response to your March 9, 2009, letter to this Office, in which you express concerns relating to your child's special education needs. This Office administers the Family Educational Rights and Privacy Act (FERPA), which addresses issues that pertain to education records.

FERPA is a Federal law that gives parents the right to inspect and review 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 information from the records. Records that are directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution are "education records" under FERPA. Enclosed for your information are a FERPA fact sheet and guidance document. It does not appear that your concerns are addressed by FERPA.

Some of the concerns you raised may be addressed by the Individuals with Disabilities Education Act (IDEA). Although Part B IDEA is a Federal law, it is administered by the States. For further information regarding IDEA, you may contact:

Mr. Sam C. Howarth
State Director of Special Education
New Mexico Public Education Department
300 Don Gaspar Avenue
Santa Fe, New Mexico 87501-2789
Telephone: (505) 827-6541

Also, I am returning the materials you sent to this Office because they may be useful to you when contacting the office mentioned above. I trust that the above information is helpful to you.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

Enclosures

(b)(6)

APR – 9 2009

Dear (b)(6):

This is in response to your February 20, 2009, letter to this Office, in which you express concerns relating to special education. This Office administers the Family Educational Rights and Privacy Act (FERPA), which addresses issues that pertain to education records.

FERPA is a Federal law that gives parents the right to inspect and review 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 information from the records. Records that are directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution are "education records" under FERPA. Enclosed for your information are a FERPA fact sheet and guidance document. As you can see it does not appear that your concerns are addressed by FERPA.

Some of the concerns you raised may be addressed by the Individuals with Disabilities Education Act (IDEA). Although IDEA is a Federal law, it is administered by the States. For further information regarding IDEA, you may contact:

Mr. Gene Lenz
Deputy Associate Commissioner for Special Education
Department of Special Education
Texas Education Agency
W.B. Building
1701 N. Congress Avenue, Room 6-127
Austin, Texas 78701

Also, I am returning the materials you sent to this Office because they may be useful to you when contacting the office mentioned above. I trust that the above information is helpful to you.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

Enclosures

Dr. Dean Andrews
Superintendent
Liberty Hill Independent School District
14001 HWY 29 W
Liberty Hill, Texas 78642

APR - 9 2009

Dear Dr. Andrews:

This letter is sent in regard to a report from KEYE-TV (CBS) concerning the Liberty Hill Independent School District's (District) practice of disposing of student education records in a manner that permits the improper disclosure of personally identifiable information from student education records in violation of the Family Educational Rights and Privacy Act (FERPA). The article (enclosed) and accompanying footage available at its website shows that a reporter from the TV station, Nanci Wilson, gained unauthorized access to student education records. Specifically, the TV station filmed images of personally identifiable information from records from the District that were left in a dumpster.

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements.

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the December 9, 2008, FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. *See* 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes of unauthorized access and disclosure. Although FERPA does not dictate requirements for safeguarding education records, the Department encourages the holders of personally identifiable information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.

- Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.
- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.
- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at

http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and
http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

Mr. Joseph White
President
University of Illinois at Urbana-Champagne
506 S. Wright Street
Urbana, Illinois 61801

APR – 9 2009

Dear Mr. White:

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements.

We are responding to a letter that this Office received on November 19, 2007, from a student who alleged that the University violated FERPA when it improperly disclosed education records of all undergraduates in the engineering program by inadvertently attaching their records to an e-mail addressed to the College of Engineering departments. The enclosed email indicates that the students were informed of the breach by email dated August 29, 2007, from [redacted] Interim Associate Dean for Academic Affairs, in which he assures students that "the matter is being vigorously addressed and procedures are being changed to ensure that this kind of disclosure does not occur again."

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the December 8, 2009, FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. *See* 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes of unauthorized access and disclosure. Although FERPA does not dictate requirements for safeguarding education records, the Department encourages the holders of personally identifiable information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.
- Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.

- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.
- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

cc: Student

(b)(6)

APR – 6 2009

Dear (b)(6):

The purpose of this letter is to confirm that this Office is not initiating an investigation in response to your correspondence of September 24 and November 25, 2008, regarding your concerns with the (b)(6) (District). I originally informed you of this Office's decision by telephone on December 11, 2008. This Office administers the Family Educational Rights and Privacy Act (FERPA), which addresses issues that pertain to education records. In accordance with the FERPA regulations, this Office notifies a complainant if it does not initiate an investigation under FERPA.

You requested that the District amend the Individualized Education Plan (IEP) of your son, (b)(6) (Student), by removing a portion of a statement made on June 18, 2008, by (b)(6), director of special education for the District. Specifically, you object to (b)(6) statement in connection with a June 25 due process mediation meeting that "the only description [the Student] has related to PDD is 'by history' according to his doctor." You state that since the document containing the medical diagnosis was removed from the Student's records, (b)(6) should no longer be permitted to refer to the diagnosis. In response to your concern, (b)(6) stated that he was unable to "erase the report from his memory."

FERPA is a Federal law that gives parents of minor students 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 information from the records. "Education records" are defined as records that are directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution. When a student reaches the age of 18 or attends an institution of postsecondary education, that student is deemed "eligible" and all of the rights afforded by FERPA transfer from the parents to the student.

Under FERPA, a parent (or the eligible student, when the student is 18 years of age or older) has the right to request that inaccurate information in the student's education records be amended. However, while the FERPA amendment procedure may be used to challenge facts that are inaccurately recorded, it may not be used to challenge a grade, an opinion, or a substantive decision made by a school about a student. FERPA was

intended to require only that schools conform to fair recordkeeping practices and not to override the accepted standards and procedures for making academic assessments, disciplinary rulings, or placement determinations. Thus, the FERPA right to seek to amend education records which contain inaccurate information cannot be used to challenge a grade or an individual's opinion, unless it has been inaccurately recorded. Additionally, if FERPA's amendment procedures are not applicable to a parent's request for amendment of education records, the school is not required to hold a hearing under FERPA about the matter.

Also, FERPA does not protect the confidentiality of information in general. Rather, FERPA prohibits the improper disclosure of information derived from education records. Therefore, information that is based on opinion or hearsay and not specifically contained in education records would not be protected under FERPA.

Based on the information in your letter and in our telephone conversation, you are concerned that (b)(6) continues to remember information from a medical history and diagnosis report written by the Student's previous doctor, although the original document in question has been removed from the Student's education records. It appears that you and the Student disagree with (b)(6) opinion concerning the basis of the Student's eligibility for special education services. As explained above, your disagreement with (b)(6) opinion and other substantive decisions and opinions recorded in the Student's education records is not a permitted basis for a challenge under the FERPA amendment process. Accordingly, FERPA's amendment provisions do not apply to this situation, and the District would not be required by FERPA to consider the request to amend the records or to afford you or the Student a hearing with respect to the matter.

As we discussed in our telephone conversation, some of your concerns may be addressed by the Individuals with Disabilities Education Act (IDEA). You indicated you had contacted your State education department, which administers IDEA.

I trust that the above information is helpful in explaining the scope and limitations of FERPA as it relates to your concern.

Sincerely,

Kathleen M. Wolan
Program Analyst
Family Policy Compliance Office

[redacted]

APR – 3 2009

Dear [redacted]

This is in response to your letter, received March 18, 2009, concerning the Family Educational Rights and Privacy Act (FERPA). Specifically, you state that your step-son is a 19 year old student at [redacted] University and that his biological father is refusing to pay for his educational support. You state that the biological father's position is that Connecticut law requires that he be given copies of his son's education records and, apparently, his son is not providing those records to him. You believe that the biological father's position is in "direct conflict with both the specific letter of the provisions of FERPA and the Privacy of Students Law as well as its state purpose and intent."

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 information from the records. Under FERPA, parents must also provide a signed and dated written consent before an educational agency or institution discloses personally identifiable information from a student's education records, except as authorized by law. When a student reaches the age of 18 or attends an institution of postsecondary education, that student is deemed "eligible" and all of the rights afforded by FERPA transfer from the parents to the student.

While FERPA generally prohibits the nonconsensual disclosure of information derived from education records, one exception permits the nonconsensual disclosure of information derived from education records to that student's parent if the student is a dependent student, as defined in section 152 of the Internal Revenue Code of 1986. Further, neither the age of the student nor the parent's status as custodial parent is relevant to determining whether disclosure of information from the education records of eligible students to a parent without written consent is permissible under FERPA. If a student is claimed as a dependent by either parent for tax purposes, then either parent may have access under this provision.

However, it should be noted that a postsecondary educational institution is not required by FERPA to disclose information from education records of dependent students to his or her parents. Rather, a postsecondary institution may refuse to provide parents access to the education records of their children under FERPA since all rights have transferred to the student by statute. With regard to the Privacy of Students Law, we are not familiar with such a law. Additionally, this Department does not have the authority to enforce a State law such as the one that you cited in your letter.

I trust that this adequately explains the scope and limitations of FERPA as it pertains to your inquiry. Enclosed is a guidance document on FERPA for eligible students that I trust will be helpful to you and your family.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

Enclosure

Dr. Steven L. Walts
Superintendent
Prince William County Public Schools
Kelly Leadership Center
14715 Bristow Road
Manassas, Virginia 20112

APR – 3 2009

Dear Dr. Walts:

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements. We are responding to a letter from Mary McGowan, School Board Attorney, dated August 26, 2008, in which she explained that Prince Williams County Public Schools inadvertently disclosed student education records and informed us of the steps taken since the breach occurred.

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the December 9, 2008, FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. *See* 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes

of unauthorized access and disclosure. Although FERPA does not dictate requirements for safeguarding education records, the Department encourages the holders of personally identifiable information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.
- Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.
- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.

- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

cc: Ms. Mary McGowan

Rev. Dr. Thomas R. Ahlersmeyer
President
Concordia University
4090 Geddes Road
Anne Arbor, Michigan 48105

APR 0 2 2009

Dear Reverend Ahlersmeyer:

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements. We are responding to a letter from Dr. Dennis Genig, Vice President of Academics, dated March 24, 2008, in which he explained that student education records were stolen from Concordia University and informed us of the steps taken since the breach occurred.

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the December 9, 2008, FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. *See* 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes of unauthorized access and disclosure. Although FERPA does not dictate requirements for safeguarding education records, the Department encourages the holders of personally identifiable

information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.
- Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.
- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.
- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at

http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and
http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

cc: Dr. Dennis Genig

Dr. Robert E. Witt
President
The University of Alabama
Tuscaloosa, Alabama 35487

APR 0 2 2009

Dear Dr. Witt:

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements. We are responding to two letters concerning The University of Alabama. One letter is dated April 14, 2008, from Dr. Robert W. Halli, Honors' College Dean, explaining that the University inadvertently disclosed student education records and informed us of the steps taken since the breach occurred. The other letter is dated May 30, 2008, from Dr. James E. McLean, University professor and Dean of the College of Education explaining that the course management site was hacked into and informed us of the steps taken since the breach occurred.

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the December 9, 2008, FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. *See* 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes

of unauthorized access and disclosure. Although FERPA does not dictate requirements for safeguarding education records, the Department encourages the holders of personally identifiable information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.
- Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.
- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.

- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

cc: Dr. Robert W. Halli

Dr. James E. McLean

Dr. Edward Guiliano
President
New York Institute of Technology
Northern Boulevard
P.O. Box 8000
Old Westbury, New York 11568-8000

APR 0 2 2009

Dear Dr. Guiliano:

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements. We are responding to a letter from Dr. Richard Pizer, Provost and Vice President for Academic Affairs, in which he explained that the New York Institute of Technology inadvertently disclosed student education records and informed us of the steps taken since the breach occurred.

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the new FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. See 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes of unauthorized access and disclosure. Although FERPA does not dictate requirements for

safeguarding education records, the Department encourages the holders of personally identifiable information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.
- Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.
- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.
- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at

http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and
http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

Mr. Flavius Killebrew
President
Texas A&M University-Corpus Christi
6300 Ocean Drive
Corpus Christi, Texas 78412

APR 0 2 2009

Dear Mr. Killebrew:

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements. We are responding to a letter dated October 23, 2008, from Michael L. Rendon, Registrar, in which he explained that an unidentified individual accessed a server maintained by Texas A&M University and informed us of the steps taken since the breach occurred.

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the December 8, 2009, FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. *See* 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes of unauthorized access and disclosure. Although FERPA does not dictate requirements for

safeguarding education records, the Department encourages the holders of personally identifiable information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.
- Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.
- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.
- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at

http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and
http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

cc: Michael L. Rendon

Dr. Roy A. Church
President
Lorain County Community College
1005 N. Abbe Road
Elyria, Ohio 44035

APR 0 2 2009

Dear Dr. Church:

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements. We are responding to correspondence this Office received via e-mail on January 5, 2009, from David Cummings, VP Administrative Services, in which he explained a hacker breached two servers at Lorain County Community College and informed us of the steps taken since the breach occurred.

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the December 9, 2008, FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. *See* 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes of unauthorized access and disclosure. Although FERPA does not dictate requirements for

safeguarding education records, the Department encourages the holders of personally identifiable information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.
- Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.
- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.
- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at

http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and
http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

cc: David Cummings

Dr. Carol Seavor
President
Jefferson College of Health and Sciences
920 S. Jefferson Street
P.O. Box 13186
Roanoke, Virginia 24031-3186

APR 0 2 2009

Dear Dr. Seavor:

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements. We are responding to your letter dated December 7, 2006, in which you explained that the Jefferson College of Health and Sciences inadvertently disclosed student education records and informed us of the steps taken since the breach occurred.

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the December 9, 2008, FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. *See* 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes of unauthorized access and disclosure. Although FERPA does not dictate requirements for

safeguarding education records, the Department encourages the holders of personally identifiable information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.
- Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.
- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.
- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at

http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and
http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

Dr. Bernard Lander
President
Touro University California
1310 Johnson Lane
Mare Island
Vallejo, California 94592

APR 0 2 2009

Dear Dr. Lander:

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements. We are responding to a letter from Dr. Harold Borrero, Registrar, July 27, 2007, in which he explained that Touro University inadvertently disclosed student education records and informed us of the steps taken since the breach occurred.

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the December 9, 2008, FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. *See* 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes of unauthorized access and disclosure. Although FERPA does not dictate requirements for safeguarding education records, the Department encourages the holders of personally identifiable

information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.
- Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.
- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.
- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at

http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and
http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

cc: Dr. Harold Borrero

Dr. Darrel L. Hammon
President
Laramie County Community College
1400 East College Drive
Cheyenne, Wyoming 82007-3299

APR 0 2 2009

Dear Dr. Hammon:

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements. We are responding to a letter from Jennifer G. Hargett, Director of Enrollment Services, dated January 19, 2007, in which she explained that student education records were stolen from a Laramie County Community College school official and informed us of the steps taken since the breach occurred.

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the December 9, 2008, FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. *See* 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes of unauthorized access and disclosure. Although FERPA does not dictate requirements for safeguarding education records, the Department encourages the holders of personally identifiable

information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.
- Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.
- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.
- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at

http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and
http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

cc: Jennifer G. Hargett

Mr. Stephen B. Martin
Head of School
Colorado Virtual Academy
11990 Grant Street, Suite 402
Northglenn, Colorado 80233

APR 0 2 2009

Dear Mr. Martin:

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements. We are responding to your letter dated March 7, 2007, in which you explained that Colorado Virtual Academy inadvertently disclosed student education records and informed us of the steps taken since the breach occurred.

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the December 9, 2008, FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. *See* 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes of unauthorized access and disclosure. Although FERPA does not dictate requirements for safeguarding education records, the Department encourages the holders of personally identifiable information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information

to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.
- Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.
- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.
- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen

or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

Mr. Kent John Chabotar
President
Guilford College
5800 West Friendly Avenue
Greensboro, North Carolina 27410

APR 0 2 2009

Dear Mr. Chabotar:

This Office is responsible for administration of the Family Educational Rights and Privacy Act (FERPA), which protects the privacy interests of parents and eligible students in students' education records. See 20 U.S.C. §1232g and 34 CFR part 99. Under that authority we investigate, process, and review complaints and violations and provide technical assistance to ensure compliance with all FERPA requirements. We are responding to a letter from Julie C. Theall, General Counsel, dated April 5, 2007, in which she explains that Guilford College inadvertently disclosed student education records and informed us of the steps taken since the breach occurred.

Under FERPA, a parent or eligible student must provide a signed and dated written consent before a postsecondary institution discloses personally identifiable information from the student's education records. 34 CFR §§99.5(a); 99.30. Exceptions to the consent requirement are set forth in § 99.31(a) of the regulations. "Disclosure" means "to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means." 34 CFR § 99.3.

The preamble to the December 9, 2008, FERPA regulations explains the necessity for educational agencies and institutions to ensure that adequate controls are in place so that the education records of all students are handled in accordance with FERPA's privacy protections. *See* 73 *Fed. Reg.* 74806, 74843 (Dec. 9, 2008). The "Department Recommendations for Safeguarding Education Records" (Safeguarding Recommendations) that were published in both the Notice of Proposed Rulemaking (NPRM) and the Final Regulations are intended to provide agencies and institutions additional information and resources to assist them in meeting this responsibility. (The NPRM was published at 73 *Fed. Reg.* 15574, March 24, 2008.)

The FERPA Safeguarding Recommendations recognize that no system for maintaining and transmitting education records, whether in paper or electronic form, can be guaranteed safe from every hacker and thief, technological failure, violation of administrative rules, and other causes of unauthorized access and disclosure. Although FERPA does not dictate requirements for safeguarding education records, the Department encourages the holders of personally identifiable

information to consider actions that mitigate the risk and are reasonably calculated to protect such information. Of course, an educational agency or institution may use any reasonable method, combination of methods, or technologies, taking into consideration the size, complexity, and resources available to the institution; the context of the information; the type of information to be protected (such as SSNs or directory information); and methods used by other institutions in similar circumstances. The greater the harm that would result from unauthorized access or disclosure and the greater the likelihood that unauthorized access or disclosure will be attempted, the more protections an agency or institution should consider using to ensure that its methods are reasonable.

As explained in the FERPA Safeguarding Recommendations, one resource for administrators of electronic data systems is "The National Institute of Standards and Technology (NIST) 800-100, Information Security Handbook: A Guide for Managers" (October 2006). See http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Another resource is NIST 800-53, Information Security, which catalogs information security controls. See http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf. Similarly, a May 22, 2007, memorandum to heads of Federal agencies from the Office of Management and Budget requires executive departments and agencies to ensure that proper safeguards are in place to protect personally identifiable information that they maintain, eliminate the unnecessary use of SSNs, and develop and implement a "breach notification policy." Although directed towards Federal agencies, this memorandum may also serve as a resource for educational agencies and institutions. See http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

The Department's FERPA Safeguarding Recommendations specify that an educational agency or institution that has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, should consider one or more of the following steps:

- Report the incident to law enforcement authorities.
- Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
- Take steps immediately to retrieve data and prevent any further disclosures.
- Identify all affected records and students.
- Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.
- Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.
- Determine whether the incident occurred because of a lack of monitoring and oversight.
- Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.
- Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at

http://www.ed.gov/about/offices/list/oig/misused/idtheft.html; and
http://www.ed.gov/about/offices/list/oig/misused/victim.html.

The Safeguarding Recommendations note also that FERPA does not require an educational agency or institution to notify students that information from their education records was stolen or otherwise subject to an unauthorized release, although it does require the agency or institution to maintain a record of each disclosure. 34 CFR §99.32(a)(1). However, student notification may be required in these circumstances for postsecondary institutions under the Federal Trade Commission's Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information ("Safeguards Rule") in 16 CFR part 314. In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft.

Under FERPA, no funds shall be made available to an educational agency or institution that has a policy or practice of permitting the release of personally identifiable information in education except as authorized by statute. 20 U.S.C. §1232g(b). Failure to take reasonable and appropriate steps to protect education records could result in the release or disclosure of personally identifiable information from education records and may also constitute a policy or practice of permitting the release or disclosure of education records in violation of FERPA requirements. Should this Office investigate a complaint or other indications of noncompliance, we would take into consideration what steps an educational agency or institution has taken in response to a data breach or other unauthorized access to, release, or other disclosure of education records.

If you have any questions, please contact this Office at (202) 260-3887.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

cc: Julie C. Theall

[redacted]

MAR 26 2009

Dear [redacted]

This is in response to your January 28, 2009, letter to this Office in which you allege that [redacted] (District) violated your rights under the Family Educational Rights and Privacy Act (FERPA) when it disclosed information from the education records of your son, [redacted] (Student), to a third party without your prior written consent. This Office administers FERPA which addresses issues that pertain to education records.

Specifically, you state:

> . . . Recently . . . the . . . District violated my child's rights under [FERPA] when they disclosed information from the education records of [the Student] without my prior written notice. Specifically, they released emails from myself as [the Student's] parent to the Special Education Administrator [redacted]. The emails between [redacted] and myself have a disclosure at the bottom of them which reads
>
> CONFIDENTIALITY NOTICE: this communication and any documents, files or previous e-mail messages attached to it, constitute an electronic communication within the scope of the Electronic Communication Privacy Act, 18 USC 2510. This communication may contain non-public, confidential, or legally privileged information intended for the sole use of the designated recipient(s). The unlawful interception, use, or duplication of such information is strictly prohibited under 18 USC 2511 and any applicable laws.
>
> Based on this confidentiality notice above I had requested prior to the student file being sent from [the District] to [redacted] District that [the District] and namely [redacted] remove the e-mails from [the Student's] file. She has assured me I had been contacted.

FERPA is a Federal law that gives 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 information from the records. The term "education records" means those records that are directly related to a student and maintained by an

educational agency or institution or by a party acting for the agency or institution. Enclosed for your information is a FERPA guidance document.

Under FERPA, a school may not generally disclose personally identifiable information from a minor student's education records to a third party unless the Student's parent has provided written consent. However, there are several exceptions to FERPA's general prohibition against nonconsensual disclosure of education records. One such exception permits a school to nonconsensually disclose education records to another school where a student seeks or intends to enroll. Please see page 3 (fourth paragraph) of the guidance document for additional information on this exception.

If the District includes a statement in its annual notification that it discloses education records to a school where a student seeks or intends to enroll, it may make such disclosure of the Student's education records without notice to you. If the District does not include such a statement in the annual notification, it must notify you prior to making the disclosure. In either case, the District may generally disclose any education records, including the e-mails at issue, to another school where the Student seeks or intends to enroll regardless of the confidentiality notice in the e-mails or [redacted] assurances to you.

If the District does not include the required notice in its annual notification, and it disclosed the e-mails to the other school district before notifying you of its intention to make this disclosure, you may contact this Office again with such information. Otherwise, no basis exists for this Office to further consider your allegation.

I trust that the above information is helpful in explaining the scope and limitations of FERPA as it relates to your concern.

Sincerely,

Ricky C. Norment
Program Analyst
Family Policy Compliance Office

Enclosure

(b)(6)

MAR 18 2009

Dear (b)(6)

This is in response to your March 5, 2009, e-mail to the Secretary in which it appears you are alleging that (b)(6) (University) violated your rights under the Family Educational Rights and Privacy Act (FERPA) when it did not amend your education records as requested or offer you the opportunity for a hearing on the matter. This Office administers FERPA which addresses issues that pertain to education records.

In a March 2009 telephone conversation, you informed me that you were seeking to amend your grade point average (GPA). You indicated that the University currently uses a different method for calculating a student's GPA than it used when you were a student there. It appears you believe that if the University calculated your GPA using the current method it would result in your GPA being higher. Thus, you are seeking to have the University amend your GPA by calculating it using the method currently used by the University to calculate GPAs. In your telephone conversation, you indicated that the University informed you that it was not going back to calculate the GPA's of any former students using the current method.

FERPA is a Federal law that gives eligible students the right to have access to their education records, the right to seek to have the records amended, and the right to have some control over the disclosure of information from the records. The term "education records" means those records that are directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution.

Under FERPA, an eligible student has the right to request that inaccurate or misleading information in his or her education records be amended. While a school is not required to amend records in accordance with a student's request, the school is required to consider the request. If the school decides not to amend the record in accordance with the student's request, the school must inform the student of the right to a hearing on the matter. If, as a result of the hearing, the school still decides not to amend the record, the

student has the right to insert a statement in the record setting forth his or her views. That statement must be maintained with the record for as long as the record is maintained.

This right is not unlimited, however, and a school is not required by FERPA to afford a student the right to seek to change substantive decisions made by school officials, such as grades or other evaluations of a student. This fact is indicated in the legislative history of FERPA. The primary source of legislative history regarding FERPA is contained in the "Joint Statement in Explanation of Buckley/Pell Amendment," Volume 120 of the Congressional Record, pages 39862-39866. The Joint Statement states that FERPA was "not intended to overturn established standards and procedures for the challenge of substantive decisions made by an educational institution." (Emphasis added.) FERPA was intended to require only that educational agencies and institutions conform to fair recordkeeping practices and not to override the accepted standards and procedures for making academic assessments, disciplinary rulings, or placement determinations. Thus, while FERPA affords students the right to seek to amend education records which contain inaccurate information, this right cannot be used to challenge a grade or an individual's opinion, unless the grade or the opinion has been inaccurately recorded.

As I explained to you in our March 2006 conversation, this Office investigates those timely complaints that contain specific allegations of fact giving reasonable cause to believe that a school has violated FERPA. As I further stated in our discussion and above, you may not seek to amend a grade under FERPA. Thus, if you are seeking to amend a grade under FERPA, there is no basis for this Office to further assist you.

However, you indicated that you had additional evidence regarding the University allegedly violating your rights under FERPA that you wanted to share with this Office. I explained that as a part of the complaint process, we provide a school with such evidence to support an allegation of a violation, and we request that the school evaluate the evidence and provide us with a timely response. I also explained that the stronger the FERPA evidence you provide to this office, the more likely the office would be to provide a fair and complete finding relative to FERPA. I also informed you that your case manager is Mr. Ricky Norment of my staff, and that he has already mailed you a complaint form. I suggest you use the complaint form to provide this Office with any additional evidence which you have not previously provided. I also asked for you to use Mr. Norment as your primary contact to ensure your case gets a comprehensive review, and you agreed.

I trust that the above information is helpful in explaining the scope and limitations of FERPA as it relates to your concern. We await any additional evidence that you wish to provide to this office to support your allegation.

Sincerely,

Paul Gamill
Director
Family Policy Compliance Office

(b)(6)

MAR 18 2009

Dear (b)(6)

Please be advised that we have received your letters, dated June 1, 2008, January 10, 2009, and February 16, 2009, regarding the Family Educational Rights and Privacy Act (FERPA). You state that you wish to amend your previous FERPA complaint against the (b)(6) (b)(6) (University), alleging that the University disclosed information from your education records to the media. You enclosed a copy of a *DallasNews.com* article, dated April 17, 2008, to support your allegation.

White the article states that you are in the Beaumont Federal Correctional Institution "for making threats at the (b)(6)," you did not provide evidence to support your allegation that a improper disclosure of information from your education records was made by the University to the media. Rather, you state that because a campus law enforcement unit report about your threats was disclosed to the dean of students' office, it was a violation of FERPA to also release the report to the media. This allegation does not have merit because a law enforcement unit record does not lose its status as a "law enforcement unit record" if it is disclosed to school officials. Thus, a law enforcement unit record may be shared with school officials, as well as with the media. Furthermore, the fact that you are incarcerated for making threats at the University is a matter of public record and this Office will not be investigating your allegation.

With regard to your statement in two of your letters that this Office "did not withhold all Federal funds as required by law," please note that FERPA does not require that all Federal funds be withheld. In fact, FERPA requires that this Office work with the educational agency or institution to bring them into compliance with FERPA before taking any enforcement measures.

I trust this adequately explains the scope and limitations of FERPA as it relates to your concerns.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

(b)(6)

MAR 17 2009

Dear (b)(6)

This is in response to your letter dated February 24, 2009, in which you allege that your rights under the Family Educational Rights and Privacy Act (FERPA) have been violated. You did not enclose the two letters that you referenced wherein you asked that your children's school district send you copies of their education records. Nonetheless, you allege that the district refused your request. This Office administers FERPA which pertains to education records.

FERPA is a Federal law that gives parents, custodial and noncustodial alike, the right to inspect and review their children's education records, unless the school has evidence that there is a court order or State law which specifically provides to the contrary. A school may ask for legal certification denoting parenthood, such as a birth certificate or court order, from the parent requesting access. Enclosed is a FERPA fact sheet on the rights of noncustodial parents.

FERPA requires that schools comply with a parent's request for access to his or her children's education records within 45 days of receipt of the request. A school is not required by FERPA to provide copies of education records to a parent unless a failure to do so would effectively prevent the parent from exercising the right to inspect and review the records. For example, a school could be required to provide copies, or make other arrangements, if the parent does not live within commuting distance of the school.

Because it appears that you are seeking copies of your children's education records, and you have not indicated that the district is denying you the opportunity to inspect and review the records, no basis exists on which to consider your FERPA allegation. If you require further assistance, you may contact this Office again.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

(b)(6)

Dear [redacted]

MAR 12 2009

This responds to your February 26, 2009, email you sent to Secretary Duncan in which you appear to allege that rights afforded you under the Family Educational Rights and Privacy Act (FERPA) were violated at schools where your child attends or attended. Specifically, you state that schools have failed to include your name on their emergency contact form and have failed to include your child's complete name in their registration forms. You also state that your child's school has failed to invite you to a school event. Your letter was forwarded to this Office for response because, as you know, we administer the Family Educational Rights and Privacy Act (FERPA).

FERPA is a Federal law that gives parents the right to have access to their minor children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of information from the records. The term "education records" is defined as those records that contain information directly related to a student and which are maintained by an educational agency or institution or by a party acting for the agency or institution. Enclosed is a copy of a FERPA guidance document for parents.

Under FERPA, a school must provide a parent with an opportunity to inspect and review his or her child's education records within 45 days of the receipt of a request. A school is required to either provide a parent with copies or make other arrangements of their child's education records when a failure to do so would effectively prevent the parent from obtaining access to the records. A case in point would be a situation in which the parent does not live within commuting distance of the school. It appears that you live within commuting distance to your child's schools and it they would be required to provide you the opportunity to inspect and review your daughter's education records, though they would be permitted to provide you with copies or make other arrangements.

While a school is required to comply within 45 days with each individual request for access, a school is not required by FERPA to honor standing requests, to provide immediate access to records, or to send out grades to parents at the end of marking periods. Additionally, FERPA would not require a school to provide parents documents

such as school calendars, updates, or notices of parent/teacher conferences because such documents do not generally contain information that is directly related to individual students. Also, schools are not required by FERPA to permit parents to attend parent/teacher conferences or community events and such decisions are made at the local school level.

You also state that schools where your child attends or attended do not include the child's complete name and do not include your name on the emergency contact cards. FERPA does not require schools to create or maintain education records, or to re-create lost or destroyed education records. Additionally, FERPA does not require a school to keep education records in any particular manner, so long as the records are treated consistent with FERPA. Accordingly, the issues you raise regarding a school's inclusion of your child's complete name and inclusion of your name on the school's emergency contact card are not addressed at the Federal level and may be addressed directly with your child's schools.

This Office does not address issues pertaining to allegations of discrimination or school employee conduct. Issues regarding discrimination as you raise them may be addressed by writing to the following Office at:

New York Office
Office for Civil Rights
U.S. Department of Education
32 Old Slip, 26th Floor
New York, NY 10005-2500

I trust this information is helpful in explaining the scope and limitations of FERPA as it relates to your concerns.

Sincerely,

Paul Gammill
Director
Family Policy Compliance Office

Enclosure

(b)(6)

MAR 6 2009

Dear (b)(6)

This is in response to your September 16, 2008, letter to this Office in which you appear to be seeking to have a grade on your transcript amended. You believe that this grade caused the College to disqualify you from further attendance at the College in the fall of 2005. This Office administers the Family Educational Rights and Privacy Act (FERPA) which addresses issues that pertain to education records.

FERPA is a Federal law that gives eligible students the right to have access to their education records, the right to seek to have the records amended, and the right to have some control over the disclosure of information from the records. The term "education records" means those records that are directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or institution. Enclosed for your information are a FERPA fact sheet and guidance document.

Under FERPA, a student has the right to request that inaccurate or misleading information in his or her education records be amended. While a school is not required to amend education records in accordance with a student's request, the school is required to consider the request. If the school decides not to amend the record in accordance with the student's request, the school must inform the student of the right to a hearing on the matter. If, as a result of the hearing, the school still decides not to amend the record, the student has the right to insert a statement in the record setting forth his or her views. That statement must be maintained with the record for as long as the record is maintained.

However, while the amendment procedure may be used to challenge facts that are inaccurately recorded, it may not be used to challenge a grade, an opinion, or a substantive decision made by a school about a student. The FERPA amendment procedure is intended to require only that educational agencies and institutions conform to fair recordkeeping practices and not to override the accepted standards and procedures for making academic assessments.

You may not use the FERPA amendment procedure to seek to amend your grade on the transcript; nor may you use it to overturn the substantive decision to disqualify you from further attendance at the College. As such, there is no basis for this Office to assist you regarding your concern.

I trust that the above information is helpful in explaining the scope and limitations of FERPA as it relates to your concerns.

Sincerely,

Ricky C. Norment
Program Analyst
Family Policy Compliance Office

Enclosure