National Cooperative Education Statistics System

The National Center for Education Statistics established the National Cooperative Education Statistics System (Cooperative System) to assist in producing and maintaining comparable and uniform information and data on early childhood education and elementary and secondary education. These data are intended to be useful for policy-making at the federal, state, and local levels.

The National Forum on Education Statistics, among other activities, proposes principles of good practice to assist state and local education agencies in meeting this purpose. The Cooperative System and the National Forum on Education Statistics are supported in these endeavors by resources from the National Center for Education Statistics.

Publications of the National Forum on Education Statistics do not undergo the formal review required for products of the National Center for Education Statistics. The information and opinions published here are the product of the National Forum on Education Statistics and do not necessarily represent the policy or views of the U.S. Department of Education or the National Center for Education Statistics.

July 2006

This publication and other publications of the National Forum on Education Statistics may be found at the National Center for Education Statistics website.

The NCES World Wide Web Home Page is *http://nces.ed.gov*
The NCES World Wide Web Electronic Catalog is *http://nces.ed.gov/pubsearch*
The Forum World Wide Web Home Page is *http://nces.ed.gov/forum*

Suggested citation
National Forum on Education Statistics. (2006). *Forum Guide to the Privacy of Student Information: A Resource for Schools* (NFES 2006–805). U.S. Department of Education. Washington, DC: National Center for Education Statistics.

For ordering information on this report, write:
U.S. Department of Education
ED Pubs
P.O. Box 1398
Jessup, MD 20794–1398
Or call toll free 1–877–4ED–PUBS; or order online at *http://www.edpubs.org*

Technical contact:
Ghedam Bairu
202–502–7304
ghedam.bairu@ed.gov

FERPA Toolkit Action Plan Team

This document was developed through the National Cooperative Education Statistics System and funded by the National Center for Education Statistics (NCES) of the U.S. Department of Education. A volunteer Action Plan Team of the National Forum on Education Statistics produced this document.

Chair

Levette Williams
Georgia Department of Education

Members

Eva Chunn
District of Columbia Public Schools

Bruce Dacey
Delaware Department of Education

Mary K. Hervey DeGarmo
Brooke County Schools *(West Virginia)*

Judy Fillion

Mary Gervase
Blaine County School District *(Idaho)*

Angela Hagans
Georgia Department of Education

Wanda Jones
Georgia Department of Education

Polly Sorcan

Forum Review Procedures

Development team members review all products iteratively throughout the development process. Documents prepared, reviewed, and approved by development team members are posted to the Forum website prior to publication so that other interested individuals or organizations can provide feedback. After development team members oversee the integration of public review comments and review the document a final time, all publications are subject to examination by members of the Forum standing committee sponsoring the project. Finally, the entire Forum (approximately 120 members) must review and vote to formally approve the document prior to final publication.

Publications of the National Forum on Education Statistics do not undergo the formal review required for products of the National Center for Education Statistics. The information and opinions published here are the product of the National Forum on Education Statistics and do not necessarily represent the policies or views of the U.S. Department of Education or the National Center for Education Statistics.

Acknowledgments

The members of the FERPA Toolkit Action Plan Team of the National Forum on

Table of Contents

Introduction 1
FERPA and Its Protection 2
Education Records.....2
Directory Information 3
Annual Notification and Rights of Parents 3
Disclosure of Student Information 4
Transfer of School Disciplinary Records 6
Health Records: FERPA and HIPAA.....6
Data Requests and FERPA 7
Military Recruiters.....8
Confidentiality and Privacy Concerns 8
Surveillance Cameras 9
Videotapes and Online Information 10
Conclusion 11
Appendix A. Key Terms and Definitions 13
Appendix B. References and Other Resources 14

Introduction

As an employee of a school or other education institution, you may sometimes access individual student records while performing your official duties. Under the Family Educational Rights and Privacy Act (FERPA), you are legally and ethically obliged to safeguard the confidentiality of any information they contain. This guide provides a general overview of the legal and related issues you may encounter while carrying out your duties.

The school district is responsible for ensuring that all parents and eligible students are afforded all the rights provided them by FERPA.

The *Forum Guide to the Privacy of Student Information: A Resource for Schools* was written to help school and local education agency staff better understand and apply FERPA, a federal law that protects privacy interests of parents and students in student education records. The Forum has developed full reports on student (and staff) privacy guidance, but a shorter document was needed to provide a quick overview and links to other resources when more information is needed. This guide defines terms such as "education records" and "directory information"; and offers guidance for developing appropriate privacy policies and information disclosure procedures related to military recruiting, parental rights and annual notification, videotaping, online information, media releases, surveillance cameras, and confidentiality concerns related specifically to health-related information. Additional references to related resources from both the federal government and private organizations can be found in the online document, "FERPA Facts for School Staff," which is available at *http://nces.ed.gov/forum/ferpa_links.asp.*

For a more in-depth review of privacy laws and professional practices that apply to information collected for, and maintained in, student records, see the *Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies* (NCES 2004).

FERPA-related violations may have serious repercussions. A school district found to have violated FERPA will be required to implement a plan of action to ensure compliance, and schools that refuse to comply risk losing federal education dollars. Therefore, it is essential to train school staff in FERPA requirements, especially since the Family Policy Compliance Office (FPCO) investigates entire school districts even when complaints are filed against individual school officials.

FERPA and Its Protection

The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy interests of students. It affords parents the right to access and amend their children's education records, and gives them some control over the disclosure of the information in these records. FERPA generally prevents an education agency or institution from sharing student records, or personally identifiable information in these records, without the written consent of a parent. A "parent" is defined as a natural or adoptive parent, a legal guardian, or an individual acting as a parent in the absence of the parent or guardian. When students reach the age of 18, or attend a postsecondary institution at any age, they are considered "eligible students" and all of the rights afforded by FERPA transfer from the parents to the students. (34 CFR § 99.3)

Although student files are protected under the law, FERPA does allow the disclosure of student data without parental consent under certain, specified conditions. For example, schools may reveal information from student records to school officials with a legitimate educational interest in the information.

As employees of a school and education institution, you may have access to individual student records in performing your official duties. You are legally and ethically obliged to safeguard their confidentiality. This guide provides a general overview of FERPA and related issues you may encounter while you carry out your job duties.

Education Records

FERPA applies to any education agency or institution that receives funds under a program administered by the U. S. Department of Education.

The term "education records" is defined as all records, files, documents and other materials containing information directly related to a student; and maintained by the education agency or institution, or by a person acting for such agency or institution (34 CFR § 99.3). This includes all records regardless of medium, including, but not limited to, handwriting, videotape or audiotape, electronic or computer files, film, print, microfilm, and microfiche.

In addition, for students who attend a public school district, all records pertaining to services provided under the Individuals with Disabilities Education Act (IDEA) are considered "education records" under FERPA. As such, they are subject to the confidentiality provisions of both Acts.

For PreK–12 students, health records maintained by an education agency or institution subject to FERPA, including immunization records and school nurse records, generally would be also considered "education records" and subject to FERPA because they are:

- directly related to the student;
- maintained by an education agency or institution, or a party acting for the agency or institution; and
- not excluded from the definition of education records as treatment or sole-possession records, or on some other basis. (See Health Records: FERPA and HIPAA.)

Personal notes made by teachers or other staff, on the other hand, are not considered education records if they are:

- kept in the sole possession of the maker;
- not accessible or revealed to any other person except a temporary substitute, and
- used only as a memory aid.

Records created and maintained by a law enforcement unit for law enforcement purposes are also excluded.

More on FERPA can be found at: *http://www.ed.gov/policy/gen/guid/fpco/index.html*

Directory Information

The term "directory information" is used for the portion of the education record that, if disclosed, would not generally be considered harmful or an invasion of privacy (34 CFR § 99.3). This may include the student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance.

Under FERPA, school systems have flexibility in deciding what information will be considered directory information. A list of the types of data that may be designated and disclosed as directory information is listed under the definition of "directory information" in the Code of Federal Regulations (34 CFR § 99.3). While school systems designate varying types of information as directory information, most include a student's name, family members' names, home address, and school activities. The height and weight of athletes may also be included.

School systems should give careful consideration to designating data as "directory information" because once this designation is given, school officials may distribute the information to anyone who requests it—in or outside the school.

School systems that disclose directory information must give "public notice" of this policy and explain what is included in such information. The notice must also indicate that parents may refuse to allow the school to designate any, or all, of their child's record as directory information. Several ways public notice can be given include: a notice in the registration package sent home to parents, a notice in the local newspaper, a notice in the school handbook distributed each year, or a posting on the school system's website. FERPA requires the notice to specify how much time parents have to tell the school or school system what, if any, directory information they do not wish released.

If a school system discloses directory information, it must give "public notice" of this policy and explain what is included in such information. FERPA does not define "public notice," and the means of notification is left up to the school.

Annual Notification and Rights of Parents

FERPA regulations require that local education agencies give annual notification to parents and eligible students of their rights under FERPA (34 CFR § 99.7). The law does not requires agencies to notify parents and eligible students individually, but agencies must provide notification where they are likely to see it. In addition, education institutions must make provisions to effectively inform individuals with a disability or whose primary language is not English.

The annual notification process must ensure that parents understand that they have the right to:

- inspect and review their child's record;
- seek to amend the record if they believe it to be inaccurate;
- consent (or not) to disclosures of personally identifiable information; and
- file a complaint with the U.S. Department of Education concerning the district's failures to comply with FERPA.

Either parent has the right to review an education record unless there is evidence of a court order or state law revoking or restricting these rights. Parents may access the education records of eligible students if they claim the student as a dependent for income tax purposes. However, agencies may require verification of the requester's relationship with the child before providing access to records.

The right of parents to access information is limited to their own child or children. If the education record includes information about other students, that information must be removed prior to disclosure so that parents do not have access to any other child's records. (34 CFR § 99.12)

When parents (or eligible students) request to review their records, the education institution must respond within 45 days, even if these records are kept by an outside party acting for the school. During these 45 days, the education institution cannot destroy any of the requested records.

For more in-depth information on directory information, disclosure of student information, and annual notification to parents, see the *Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies* (National Forum on Education Statistics, 2004).

Disclosure of Student Information

Generally, schools must have written parent (or eligible student) permission to release any information from a student's education records. However, in addition to properly designated "directory information," FERPA allows disclosure, without consent, to the following parties or under the following conditions (except as noted, conditions are listed in 34 CFR § 99.31):

A legitimate educational interest

School officials with a "legitimate educational interest" may access student records under FERPA. Generally, this refers to individuals in the school district who need to know information in the student's education record in order to perform their professional responsibility. Interest in students that "fit" a profile or category is not a legitimate educational interest. The school's criteria for appropriate "school officials" and valid "legitimate educational interest" must be included in the annual notification to parents of their FERPA rights. A sample notice of rights, including suggested language can be found at the Family Policy Compliance Office's website: *http://www.ed.gov/policy/gen/guid/fpco/ferpa/lea-officials.html.*

Other schools into which a student is transferring or enrolling

Schools that submit a records request or in which a student has enrolled are eligible to receive information from that student's education records. This includes postsecondary institutions to which the student are applying. A parent (or eligible student) may also request a records transfer.

Specified officials for audit or evaluation purposes

This category exception refers to federal, state, and local education agencies that must collect data or student information to audit, evaluate, or enforce educational programs. State agencies other than those responsible for education are not included. This exception is commonly used by state education agencies to justify state-level student records systems.

Appropriate parties in connection with financial aid

Information required to determine student eligibility for financial aid, the amount of aid to award, and the conditions under which aid is to be granted may be disclosed under this category; access to information needed to enforce those terms and conditions is also allowed. This exception typically applies to postsecondary institutions.

Organizations conducting certain studies for, or on behalf of, the school

The purpose of the study conducted for, or on behalf of, a school has to be to: develop, validate, or administer predictive tests; administer student aid programs; or improve instruction. Even if these conditions are met, the school may only disclose information if: the study methodology does not permit the personal identification of parents and students by anyone other than the researchers and their representatives; the information is not used for any purpose other than to complete the study; and the information is destroyed when it is no longer needed for the stated purposes of the study.

Accrediting organizations

Disclosure of personal information is permitted to an accrediting organization if it is needed to carry out the accreditation.

Judicial orders or lawfully issued subpoenas

Schools must release information requested by a judicial order or legal subpoena. However, the school must make a reasonable effort to notify the parent (or eligible student) in advance of compliance, unless the court or other issuing agency has ordered that the contents of the subpoena not be disclosed, or that the protected education records not be included. [34 CFR § 99.31 paragraph (a)(9)(1)]

Health and safety emergencies

Disclosure to appropriate officials is valid if the information contained in the education record is necessary to protect the health or safety of the student or other individuals (34 CFR § 99.36).

State and local authorities, within a juvenile justice system, pursuant to specific state law

If state law permits, schools may release information to state and local juvenile justice authorities after receiving written certification that the information will not be disclosed to any other agency, organization, or third party without the parent's permission, except as allowed in state law.

In all of the above cases, education agencies or institutions disclosing personally identifiable information from an education record must do so on the condition that the party receiving the information will use it only for the purpose for which it was disclosed, and will not disclose the information to another, third party without prior consent. An exception is allowed if the disclosure is made on behalf of the education agency or institution under the permitted disclosures in FERPA. (34 CFR § 99.33)

Transfer of School Disciplinary Records

While FERPA does not require schools to transfer education records to third parties, it does permit their transfer to another school if a student seeks or intends to enroll in that school; as part of the education records, disciplinary records would therefore be included in the transfer. However, the No Child Left Behind Act of 2001, reauthorizing the Elementary and Secondary Education Act (ESEA), requires that states provide an assurance to the Secretary of Education that the state "has a procedure in place to facilitate the transfer of disciplinary records, with respect to a suspension or expulsion, by local education agencies to any private or public elementary school or secondary school for any student who is enrolled or seeks, intends, or is instructed to enroll, on a full- or part-time basis, in the school."

Health Records: FERPA and HIPAA

In 1996, Congress enacted the Health Insurance Portability and Accountability Act (HIPAA) to ensure continued health insurance coverage to individuals who change jobs, and to establish standards regarding the electronic sharing of health information. For purposes of HIPAA, "covered entities" include health plans, health care clearinghouses, and health care providers that transmit health information in electronic form in connection with covered transactions (45 CFR 160.103).

Technically, schools and school systems that provide health care services to students may qualify as "covered entities" under HIPAA. However, the final regulations for the HIPAA Privacy Rule exclude information considered "education records" under FERPA from HIPAA privacy requirements. This includes student health records and immunization records maintained by an education agency or institution, or its representative; as "education records" subject to FERPA, these files are not subject to HIPAA privacy requirements. In addition, school nurse or other health records maintained on students receiving services under the Individuals with Disabilities Education Act (IDEA) are considered "education records" and also subject to that Act's confidentiality provisions. Consequently, these records are subject to FERPA and not the HIPAA Privacy Rule.

Nevertheless, certain activities, when performed by a school, could be subject to other provisions of HIPAA that concern electronic transactions. According to the preamble to the December 2000 final rules, "the educational institution or agency that employs a school nurse is subject to our (HIPAA) regulation if the school nurse or the school engages in a HIPAA transaction." HIPAA transactions are defined in the Code of Federal Regulations (CFR) as "the transmission of information between two parties to carry out financial or administrative activities related to health care," including

submitting claims. However, consent must still be secured under FERPA before the records are disclosed.

For more information on the intersection of HIPAA and FERPA, see *Health and Healthcare in Schools,* "The Impact of FERPA and HIPAA on Privacy Protections for Health Information at School: Questions from Readers" (2003, Volume 4, Number 4) at *http://www.healthinschools.org/ejournal/2003/privacy.htm.*

Data Requests and FERPA

Information requests from the press, researchers, and the general public are fairly common in most school systems and state education agencies. In this regard, the FERPA statute provides that an education agency or institution may not have a policy of disclosing education records or personally identifiable information from education records, without prior consent from the parent or eligible student, unless it is considered directory information or falls under one of the other consent exceptions contained in the law [20 U.S.C. §1232(g)(b)(1)]. (For exceptions to consent guidelines, see Disclosure of Student Information.) Agencies should determine whether requests for data meet these exceptions on a case-by-case basis.

Nothing in FERPA prohibits a school from disclosing information in aggregate, or in another form that is not personally identifiable. Personally identifiable information includes:

- the student's name;
- the name of the student's parent or other family member;
- the address of the student or student's family;
- a personal identifier, such as the student's social security number or student number;
- a list of personal characteristics that would make the student's identity easily traceable; or
- other information that would make the student's identity easily traceable.

In circumstances that may lead to the identification of an individual, the disclosing education agency or institution must ensure that student-level information is not personally identifiable by removing the student's name and ID number, as well as any "personal characteristics" and "other information that would make the student's identity easily traceable." This includes, but is not limited to, such factors as physical description (race, sex, appearance, etc.); date and place of birth; religion and national origin; participation in sports, clubs, and other activities; academic performance; employment; and disciplinary actions or criminal proceedings. "Other information that would make the student's identity easily traceable" may also exist in the form of small cell sizes in aggregated or statistical information from education records.

In cases where personal information cannot be removed, school officials must secure written parental consent before disclosing the data to outside organizations. The

required consent form should specify:

- the records that may be disclosed;
- the purpose of the disclosure; and
- the identity of the party or class of parties to whom the disclosure may be made.

[34 CFR § 99.30(b)]

Military Recruiters

The No Child Left Behind Act of 2001 (NCLB) and the National Defense Authorization Act for Fiscal Year 2002 both require high schools to provide military recruiters with access to directory-type information on secondary school students. Upon request, and after notifying parents, schools must release to military recruiters the name, address, and telephone numbers of high school juniors and seniors. (The disclosed information is used only for armed services recruiting and to inform high school students of scholarship opportunities.)

To minimize their administrative burden, some schools notify parents of the military recruiters' right to student data by utilizing the same notice they use to inform parents of directory information disclosure. A sample directory information notice with reference to disclosures to military recruiters can be found on the Family Policy Compliance Office's (FPCO) website: *http://www.ed.gov/policy/gen/guid/fpco/hottopics/ht-10-09-02a.html.*

Schools that normally do not disclose directory information and, therefore, may not have a directory-information disclosure policy under FERPA, must nevertheless release to military recruiters the student information listed above unless parents (or eligible students) disallow disclosure.

Confidentiality and Privacy Concerns

"Confidentiality" is a person's obligation to not disclose or transmit information to unauthorized parties.

"Privacy" is a uniquely personal right that reflects an individual's freedom from intrusion.

Until recently, the main concern regarding confidentiality and privacy of education records centered on individuals hacking into central computer systems or otherwise illegally accessing records through other security breaches. With technology increasingly used to ensure the availability of timely and accurate information, however, the scope of this issue has expanded to include portable storage devices (flash drives), handheld computers, electronic information transfers (e-mail), and other tools and devices used to store or transfer data.

Today's information portability makes performing many school-related tasks more convenient; however, it also increases the risk of unauthorized access to protected information. As school administrators, teachers, and support staff find new ways to store and access student records, they must still ensure the information's confidentiality and privacy.

For example, if an administrator misplaces a handheld computer, any personally identifiable information it contains becomes potentially accessible to anyone who finds the device. Teachers carrying grade files home on a flash drive or storing other personally identifiable student information on home computers create the risk of unauthorized access to protected education records. Likewise, education records transferred through electronic mail could potentially be intercepted by unauthorized

individuals. Since such situations occur daily in schools across the country, local education agencies must take precautions to guard against the unintentional release or unauthorized disclosure of education records.

Each education institution subject to FERPA should consider establishing policies, procedures, and best practices to address the following questions:

- What are the current legal restrictions for disclosure and nondisclosure?
- Does the potential risk to the confidentiality and security of education records outweigh the benefit of using certain electronic devices poses?
- Does the teacher or staff member have a legitimate educational interest in the information that meets the exception rule for prior consent (see Disclosure of Student Information)?
- Is prior consent required since the ability to carry education records off school premises changes the physical context in which the education records were originally used?
- What jobs or roles include responsibility for the safety and maintenance of education records?
- What is the ethical and legal responsibility of staff in terms of preventing unauthorized use or disclosure of information?
- What is appropriate and inappropriate use of data, and how can information be protected against unauthorized access?
- What type of training will individuals who access and/or use the information require?
- Do individuals with access to personally identifiable information take an oath of nondisclosure?

Establishing policies, procedures, and best practices is not a cure-all, but it sets the foundation for ensuring a deliberate effort to safeguard the confidentiality and privacy of education records.

Updated resources can be found on the FERPA page of the Forum website: *http://nces.ed.gov/forum/ferpa_links.asp*

Surveillance Cameras

According to *Indicators of School Crime and Safety: 2005* (U.S. Departments of Education and Justice, 2006), schools continue to implement a variety of tools to improve safety and monitor activities. In fact, the report notes that "in 1999–2000, 14 percent of primary schools, 20 percent of middle schools, and 39 percent of secondary schools used one or more security cameras to monitor the school."

School cameras are typically placed in areas that do not infringe on students' right to privacy, such as classrooms, hallways, common areas, and building perimeters. However, recent reports of cameras in bathrooms have sparked a debate over the appropriate balance between student privacy rights and the need for school security. While FERPA does not specifically address this issue, school systems should have a surveillance camera policy

outlining the rights and responsibilities of students, teachers, administrators, and other school staff. As a best practice, the policy should include the following:

- a clear statement of appropriate reasons for using surveillance cameras;
- the role and responsibilities of individuals with access to the cameras;
- who will have access to any footage;
- how long will any footage be kept and how will it be destroyed; and
- a consent provision.

For FERPA purposes, surveillance videotapes (or other media) with information about a specific student are considered education records if they are kept and maintained by the school system. If the school's law enforcement unit controls the cameras/videos and it is doing the surveillance for safety reasons, the ensuing videos would be considered law enforcement, rather than education, records. As soon as school officials use them for discipline purposes, however, the tapes become education records and are subject to FERPA requirements.

For more information, see "Fact sheet 29: Privacy in Education" (Privacy Rights Clearinghouse, 2005) at *http://www.privacyrights.org.*

For more in-depth information on directory information, disclosure of student information, and annual notification to parents, see the *Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies* (National Forum on Education Statistics, 2004).

Videotapes and Online Information

When created and kept by the school or education agency, videotapes or photographs directly related to a specific student are considered part of that student's education records and, therefore, subject to FERPA. For instance, if the tape captured an altercation, it would be included in the involved students' education record, and the school has to obtain consent before publishing or disclosing its contents to unauthorized individuals. However, authorization would be needed only for the students actually involved in the altercation; other students in the video would be considered "set dressing" (not relevant to the incident) and not covered.

Information on the Internet is treated in a similar way. Posting information is considered "disclosure" and must, therefore, comply with FERPA guidelines. Even without FERPA, school officials should consider safety concerns and exercise caution when displaying information (such as identifiable pictures) about students on the Internet, even if the information is designated as directory information. Including parents in any decisions about how much student information is appropriate might be a good practice, especially for younger students.

More information on this topic can be found in *The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies* (U.S. Department of Justice Office of Justice Programs 1999), which is available online at *http://www.ncjrs.gov/school/home.html.*

Conclusion

Safeguarding the confidentiality of individual student information is the responsibility of any and all organizations and individuals who collect, maintain, access, transfer, or use education records. This guide reviews federal privacy laws, defines related terms and concepts, summarizes organizational and individual responsibilities, and describes appropriate responses to privacy-related concerns that commonly arise in a school or district setting.

This document is meant to serve as a resource for schools and school districts, but is not a substitute for the detailed direction provided in local and state privacy laws, regulations, and procedures. For a more in-depth review of privacy laws and professional practices that apply to information collected for, and maintained in, student records, see the *Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies* (NCES 2004). Additional resources about FERPA and other privacy issues can be found in the online document, "FERPA Facts for School Staff," available at *http://nces.ed.gov/forum/ferpa_links.asp.* Schools and districts should also consult all local and state privacy laws, regulations, and procedures to which they are subject.

Appendix A. Key Terms and Definitions

Source: *Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies.* (National Forum on Education Statistics, 2004). Terms marked with an asterisk (*) indicate a consistent definition with FERPA.

Confidentiality: a person's obligation not to disclose or transmit information to unauthorized parties.

Directory Information*: information contained in a student's education record that would not generally be considered harmful or an invasion of privacy if disclosed.

Disclosure: access, release, or transfer of personally identifiable information about an individual.

Education Agency: a state or local education agency authorized to direct and control public elementary and secondary, or postsecondary, institutions.

Education Institution: an institution or school that provides educational services or instruction, or both, to students.

Education Record*: any information recorded in any way—including, but not limited to, handwriting, print, computer media, videotape or audiotape, electronic files, film, microfilm, and microfiche—that are maintained by education agencies or institutions, or individuals acting on their behalf. Personal notes by teachers or other staff, kept in the sole possession of the maker, used only as memory aid, and not accessible or revealed to any other person except a temporary substitute are not considered part of the education record.

Eligible Student*: a student who has reached the age of 18; or has attended a postsecondary institution, regardless of age.

Informed Consent: an individual's agreement in the context of a written account of why personal information is requested and how it will be used.

Legitimate Educational Interest: information is used within the context of official agency or school business and its use is consistent with the purpose for which it is maintained; access to the information is necessary for school officials to perform tasks related to their position.

Parent*: a natural or adoptive parent, a legal guardian, or an individual acting as a parent in the absence of a parent or guardian.

Personally Identifiable Information*: includes the student's name; the name of the student's parent or other family member; the address of the student; a personal identifier, such as the social security number or student number; a list of personal characteristics that would make the student's identity easily traceable; or any other information that would make the student's identity easily traceable.

Privacy: a uniquely personal right that reflects an individual's freedom from intrusion.

School Official: a person employed by the agency or school in an administrative, counseling, supervisory, academic, student support, or research position; or a person under contract to the agency or school to perform a specified task.

Security: the process that focuses on the confidentiality, integrity, and availability of information systems and data.

Student*: any person who is or has been in attendance, about whom an agency or institution maintains education records or personally identifiable information.

Appendix B. References and Other Resources

References

National Forum on Education Statistics

Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies (NCES 2004–330). U.S. Department of Education. Washington, DC: National Center for Education Statistics. *http://nces.ed.gov/forum/pub_2004330.asp*

Privacy Issues in Education Staff Records: Guidelines for Education Agencies (NCES 2000–363). U.S. Department of Education. Washington, DC: National Center for Education Statistics. *http://nces.ed.gov/forum/pub_2000363.asp*

Family Policy Compliance Office (FPCO)

Policy Guidance—Access to High School Students and Information by Military Recruiters. (2002). U.S. Department of Education. Washington, DC: Family Policy Compliance Office. *http://www.ed.gov/policy/gen/guid/fpco/hottopics/ht-10-09-02a.html*

Rooker, L. (2005). *Compliance Training: Family Educational Rights and Privacy Act, Protection of Pupil Rights Amendment, and Military Recruiter Provisions of NCLB.* U.S. Department of Education, Washington, DC.

Other references

DeVoe, J.F., Peter, K., Noonan, M., Snyder, T.D., and Baum, K. (2005). *Indicators of School Crime and Safety: 2005* (NCES 2006–001/NCJ 210697). U.S. Departments of Education and Justice. Washington, DC: U.S. Government Printing Office.

Ensuring Quality School Facilities and Security Technology. Northwest Regional Educational Laboratory: The Safetyzone. Retrieved February 2006 from *http://www.safetyzone.org.*

Green, Mary W. (1999). *The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies.* U.S. Department of Justice Office of Justice Programs. Sandia National Laboratories. Retrieved February 2006 from *http://www.ncjrs.gov/school/home.html.*

The Impact of FERPA and HIPAA on Privacy Protections for Health Information at School: Questions from Readers. *Health and Healthcare in Schools* (2003, Volume 4 Number 4). George Washington University School of Public Health and Health Services, Washington, DC: The Center for Health and Health Care in Schools. Retrieved December 2005 from *http://www.healthinschools.org/ejournal/2003/privacy.htm.*

Other resources

National Forum on Education Statistics
Home page: *http://nces.ed.gov/forum/index.asp*

FERPA information website: *http://nces.ed.gov/forum/ferpa_links.asp*

Family Educational Rights and Privacy Act (FERPA). *Code of Federal Regulations (Title 34, Part 99).* Code of Federal Regulations (CFR) main page: *http://www.gpoaccess.gov/cfr/index.html*

Family Policy Compliance Office (FPCO) at U.S. Department of Education
Home page: *http://www.ed.gov/policy/gen/guid/fpco/index.html*

Privacy Rights Clearinghouse (2005). "Fact Sheet 29: Privacy in Education." Retrieved December 2005 from *http://www.privacyrights.org.*

Rules and Regulations, Federal Register (Vol. 68, No. 34, 20 February 2003).
The Federal Register (FR) main page: *http://www.gpoaccess.gov/fr*