

**SOUTHERN CONNECTICUT STATE UNIVERSITY**  
***INFORMATION SECURITY GLBA COMPLIANCE***  
***STATEMENT***

**May 27<sup>th</sup>, 2003**

**Prepared by**

**Office of Information Technology**

The following document pertains to Southern Connecticut State University's compliance with the requirements of the Gramm-Leach-Bliley Act as mandated by the federal government. This document will provide information as to the requirements set forth, SCSU's compliance assessment and progress with these requirements, and the responsibilities employees and departments must follow to remain in compliance with GLBA related concerns. The "SCSU Information Security GLBA Compliance Statement" is a guideline for appropriate practices and security measures to ensure that SCSU will comply with GLB now and into the future. Please contact OIT with questions.

For comments & suggestions ( I am using a copy of Catholic University's Security Plan as the Model which is suggested by Pamela Kedderis; I am also including latest documents from John Young, Ray Kellogg, Joe Brignola & Dave Sieser.)

Reference: <http://counsel.cua.edu/fedlaw/glb.cfm>

Draft CUA Security Plan: <http://computing.cua.edu/glb/glb.doc>

# Table of Contents

<b>I. Preamble</b>	<b>P1</b>
<b>II. Gramm Leach Bliley (GLB) Requirements</b>	
<b>III. Information Security Plan Coordinator</b>	
<b>IV. Risk Assessment and Safeguards</b>	<b>P2</b>
<b>V. Employee training and education</b>	<b>P4</b>
<b>VI. Oversight of Service Providers and Contracts</b>	
<b>VII. Evaluation and Revision of the Information Security Plan</b>	
<b>VIII. Definitions</b>	
<b>IX. Gramm Leach Bliley (GLB) Requirements Check List</b>	<b>P5</b>
<b>X. Current Security Issues &amp; Documents</b>	<b>P6</b>
<b>a) Administrative Computing - Security Issues – (from John Young)</b>	
<b>b) Southern CT State University Banner Security Procedures (D. Sieser)</b>	<b>P7</b>
<b>c) Southern CT State University Banner Policies</b>	<b>P8</b>
<b>d) Network (Ray Kellogg)</b>	<b>P8</b>
<b>e) Academic Computer Center/ Student Labs (Joe Brignola)</b>	<b>P10</b>
<b>f) Southern Connecticut State University</b>	<b>P11</b>
<b>Banner Account and System Access Form</b>	<b>P12</b>
<b>g) Information Security Programs Under Gramm-Leach-Bliley</b>	<b>P13</b>
<b>h) Family Educational Rights and Privacy Act (FERPA)</b>	<b>P18</b>

# SCSU Information Security Plan

## I. Preamble

In order to protect critical information and data, and to comply with Federal Law<sup>1[1][1]</sup>, the Office of Information Technology (OIT), in alliance with the Office of Human Resources (HR) & Department of Administrative Services (DAS- Carol Wallace)) proposes certain practices in the University information environment and institutional information security procedures. While these practices mostly affect OIT, some of them will impact diverse areas of the University, including but not limited to Finance Administration, the Office of the Registrar, Institutional Advancement, Student Life, the Library, Admissions and Financial Aid, and many third party contractors, including food services and the book store. The goal of this document is to define the University's Information Security Program, to provide an outline to assure ongoing compliance with federal regulations related to the Program and to position the University for likely future privacy and security regulations.

## II. Gramm Leach Bliley (GLB) Requirements

GLB mandates that the University appoint an Information Security Plan Coordinator conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to covered data and information, oversee service providers and contracts, and evaluate and adjust the Information Security Program periodically.

## III. Information Security Plan Coordinator

In order to comply with GLB, SCSU has designated an Information Security Policy Coordinator. This individual must work closely with offices of Information of Technology, HR and Finance Administration, other positions in OIT, as well as all relevant academic and administrative Schools and Departments throughout the University. The Coordinator is presently the Help Desk Supervisor.

The Coordinator must help the relevant offices of the University identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information involved with services including, but not limited to, Banner Web, Banner's production database, Windows 2000 accounts and other servers on campus. Additionally, the Information Security Plan Coordinator will evaluate the effectiveness of the current safeguards for controlling these risks; design and implement a

---

1[1][1] The Financial Services Modernization Act of 1999 (also known as Gramm Leach Bliley (GLB) 15 U.S.C. §6801

safeguards program, and regularly monitor and test the program. OIT will provide access to continuing training for the Coordinator that will ensure this individual's preparedness for understanding current security issues and future risks to security as well as appropriate actions and precautions to safeguard our system while complying with GLB Requirements.

#### **IV. Risk Assessment and Safeguards**

The Coordinator must work with all relevant areas of the University to identify potential and actual risks to security and privacy of information. Each School or Department head, or her designee, will conduct an annual data security review, with guidance from the Coordinator. Vice Presidents will be asked to identify any employees in their respective areas that work with covered data and information. In addition, each relevant departments will conduct a quarterly review of procedures, incidents, and responses, and will publish all relevant materials except in those cases where publication may likely lead to breaches of security or privacy. Publication of these materials is for the purpose of educating the University community on network security and privacy issues. OIT will assure that procedures and responses are appropriately reflective of those widely practiced at other peer Institutions, as measured by four advisory groups: The Educause Security Institute, The Internet2 security working group, the SANS Top Twenty risks list, and the Federal NIST Computer Security Resource Center.

In order to protect the security and integrity of the University network and its data, The Network Field Service department of OIT will develop and maintain a registry of all computers attached to the University network. This registry will include, where relevant, IP address or subnet, MAC address, physical location, operating system, intended use (server, personal computer, lab machine, dorm machine, etc.), the person, persons, or department primarily responsible for the machine, and whether the machine has or has special access to any confidential data covered by relevant external laws or regulations.

The System Admin group of Administrative Computing of OIT assumes the responsibility of assuring that patches for operating systems or software environments are reasonably up to date, and will keep records of patching activity. The Directors of OIT will review its procedures for patches to operating systems and software, and will keep current on potential threats to the network and its data. Risk assessments will be updated quarterly.

The Network Field Service department of OIT bears primary responsibility for the identification of internal and external risk assessment, but all members of the University community are involved in risk assessment. OIT, working in conjunction with the relevant University offices, will conduct regular risk assessments, including but not limited to the categories listed by GLB.

HR, working in cooperation with OIT and relevant University departments, will develop and maintain a data handbook, listing those persons or offices responsible for each covered data field in relevant software systems (financial, student administration, development, etc.). HR and the relevant departments will conduct ongoing (at least biannual) audits of activity, and will report any significant questionable activities.

The Programming and Banner Support Department of OIT will work with the relevant offices (Finance Administration, Human Resources, the Registrar, Admission, Institutional Advancement, and among others) to develop and maintain a registry of those members of the University community who have access to covered data and information. OIT in cooperation with Human Resources and Finance Administration will work to keep this registry rigorously up to date.

The Data Center of OIT will assure the physical security of all servers and terminals which contain or have access to covered data and information. OIT will work with other relevant areas of the university to develop guidelines for physical security of any covered servers in locations outside the central server area. The University will conduct a survey of other physical security risks, including the storage of covered paper records in non-secure environments, and other procedures which may expose the University to risks.

While the University has discontinued usage of social security numbers as student identifiers, one of the largest security risks may be the possible non-standard practices concerning social security numbers, e.g. continued reliance by some University employees on the use of social security numbers. Social security numbers are considered protected information under both GLB and the Family Educational Rights and Privacy Act (FERPA).<sup>2[2][2]</sup> By necessity, student social security numbers still remain in the University student information system.<sup>3[3][3]</sup> The University will conduct an assessment to determine who has access to social security numbers, in what systems the numbers are still used, and in what instances students are inappropriately being asked to provide a social security number. This assessment will cover university employees as well as subcontractors such as the bookstore and food services, and consortiums such as the Washington Library Research Consortium.

OIT will develop a plan to ensure that all electronic covered information is encrypted in transit and that the central databases are strongly protected from security risks.

It is recommended that relevant offices of the University decide whether more extensive background or reference checks or other forms of confirmation are prudent in the hiring process for certain new employees, for example employees handling confidential financial information.

OIT will develop written plans and procedures to detect any actual or attempted attacks on covered systems and will develop incident response procedures for actual or attempted unauthorized access to covered data or information.

---

<sup>2[2][2]</sup> 20 U.S.C. § 1232g

<sup>3[3][3]</sup> Social Security Numbers are kept both for historical purposes and due to the requirements of 26 U.S.C. § 6050S, the tuition payment credit reporting requirements.

The Information Security Coordinator will periodically review the University's disaster recovery program and data-retention policies and present a report to the Vice Presidents.

## **V. Employee training and education**

While directors and supervisors are ultimately responsible for ensuring compliance with information security practices, OIT will work in cooperation with the Office of Human Resources to develop training and education programs for all employees who have access to covered data. These employees typically fall into three categories: professionals in information technology who have general access to all university data; custodians of data as identified in the data handbook, and those employees who use the data as part of their essential job duties.

## **VI. Oversight of Service Providers and Contracts**

GLB requires the University to take reasonable steps to select and retain service providers who maintain appropriate safeguards for covered data and information. Business Services, in cooperation with the Office of Controller, will develop and send form letters to all covered contractors requesting assurances of GLB compliance. While contracts entered into prior to June 24, 2002 are grandfathered until May 2004, the Office of Controller will take steps to ensure that all relevant future contracts include a privacy clause and that all existing contracts are in compliance with GLB.

## **VII. Evaluation and Revision of the Information Security Plan**

GLB mandates that this Information Security Plan be subject to periodic review and adjustment. The most frequent of these reviews will occur within OIT where constantly changing technology and constantly evolving risks indicate the wisdom of quarterly (??) reviews. Processes in other relevant offices of the University such as data access procedures and the training program should undergo regular review. The plan itself as well as the related data retention policy should be reevaluated annually in order to assure ongoing compliance with existing and future laws and regulations.

## **VIII. Definitions**

*Covered data and information* for the purpose of this policy includes student financial information required to be protected under the Gramm Leach Bliley Act (GLB). In addition to this coverage which is required by federal law, SCSU chooses as a matter of policy to also define *covered data and information* to include any credit card information received in the course of business by the university, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records.

*Student financial information* is that information the university has obtained from a student in the process of offering a financial product or service, or such information provided to the university by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CFR § 225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and social security numbers, in both paper and electronic format.

## **IX. Gramm Leach Bliley (GLB) Requirements Check List**

1. Designate one or more employees to coordinate safeguard measures, including implementation of appropriate safeguards.
2. Create council or network of representatives from the appropriate offices on campus to make sure that security concerns are being addressed and handled by each department involved.
3. Identify and assess the risks to customer information in each relevant area of operation, and evaluate the effectiveness of the current safeguards for controlling these risks.
4. Design and implement a safeguards program, and regularly monitor and test it.
5. Select appropriate service providers and contract with them to implement safeguards.
6. Evaluate and adjust the program in light of relevant circumstances, including changes in business arrangements or operations, or the results of testing and monitoring of safeguards.

Since we follow FERPA guidelines, privacy issues have been addressed and protective measures are generally in place on campus. So the primary issue that seems to be of significant importance to IT is the creation of a plan to monitor and secure all electronic data.

Note: Currently, most users, if not all, have logon authentication, application authentication, and server access restrictions. In addition, most users, if not all, have restricted access to server areas. In the case of Banner's production database, the main data server has building access security, room access security plus authentication requirements for accessing the server. From a network perspective there are firewalls as well as a series of authentication requirements.

We need to ensure that we have proper documentation of items for the Auditors.

## **X. Current Security Issues & Documents**

### **a) Administrative Computing - Security Issues – (from John Young)**

#### **Physical Security in Jennings 128**

- Entry into room is being changed from key based system to card key system, which will log all entries into the room by person, date, time.
- Temperature and water detection systems are installed. Remotely controlled by Pat Norton in Facilities. (no change)
- Fire suppression is Halon (no change)
- All equipment is on State of Connecticut Insurance carrier. \$25,000 deductible for major loss.
- Disaster recovery procedures and policies are documented as part of campus wide emergency plan. (no change)

#### **Backups**

- All Windows, UNIX, and VMS servers under the responsibility of Administrative Computing are backed up on a nightly basis.
- Backups are verified by computer operator or UA each morning. System administrators are the backup for computer operators in their absence.
- Copies of backups are sent to an off site location (Archives One) on a weekly basis.
- All servers are provided power through a UPS system, which provides power conditioning, battery backup, and generator backup in case of loss of power. UPS system is on a maintenance contract through the Facilities office. Currently, the batteries are past their recommended life expectancy and need to be replaced. The estimated cost is \$8,000.
- System Administrators have copies of backup documentation.

#### **Other Documentation**

- Documentation on all servers under the responsibility of Administrative Computing is maintained by the appropriate system administrators.
- A more comprehensive list of policies and procedures is planned and will be completed when time is available.
- Copies of all software license agreements and contracts under the responsibility of Administrative Computing are kept in the Administrative Computing Office.
- Access rights for email, campus portal, web posting services, and WebCT are currently granted under the Banner to Campus Pipeline integration process for all faculty, staff, and students.

- Access rights to Windows for faculty and administrators are currently being administered as part of the Windows 2000 migration project.
- A single procedure, in which access requests are initiated by Human Resources has been under discussion for several years, but has never been implemented. Time constraints in both the HR and IT departments are the major contributor to this.

**b) Southern CT State University Banner Security Procedures (Dave Sieser)**

- 1) Banner Team leader will consult with IT representative in order to develop module security matrix.**
- 2) Team leader will send request for a Banner account to be created with the request form to designated security representative.**
- 3) Team leader will communicate appropriate access to designated security representative who will then assign proper role and classes to user.**
- 4) Designated security representative will contact user in order to communicate user ID and password. In this way, only the designated security representative who created the account will know the password. The user can then go to the appropriate form to change their password (highly recommended!)**
- 5) If access for an individual needs to be changed, the team leader (or designee) will communicate such to the designated security representative of such changes.**
- 6) All staff members will be asked to read and sign a statement**
  - i) Of understanding regarding the rights and responsibilities that go along with access to Banner data-base information.**
- 7) Conrad Calandra (Banner Communication Director) is presently the designated security representative for all modules including Student, Finance, HR, Alumni and Financial Aid.**
- 8) IT has created and made available a set of reports (GWRX01, GWRX02 and GWRX03) which enables administrators to request a list of all Banner objects (forms, reports and processes) any functional Banner user has access to related to that administrator's area of responsibility.**

### **c) Southern CT State University Banner Policies**

- I. A user must have received Banner Navigation Training before he/she is to be given a Production account.**
  
- II. User must receive Data Standard documentation before he/she is to be given a production account.**
  
- III. Banner passwords should not be shared with anyone.**
  
- IV. No form or process will be assigned to a user unless that person has received training in such.**

**All staff members will be asked to read and sign a statement of understanding regarding the rights and responsibilities that go along with access to Banner database information.**

### **d) Network ( Ray Kellogg)**

Here's what we've done to secure our network:

\* Firewall is in place and provides non-routable IP addressing on our LAN.

All direct In-Bound traffic is blocked.

\* Intrusion Detection module installed in core route-switch in

Engleman....provides comprehensive attack detection, including:

Reconnaissance Activity (probing or mapping our network to identify "targets

of opportunity," such as ping sweeps and port sweeps), DoS Activity (attempts to consume bandwidth or computing resources to disrupt normal operations), Exploits Activity (attempts to gain access or compromise systems on our network, such as Back Orifice, failed login attempts, and TCP hijacking), and Misuse Activity (attempting to violate university policy; this can be detected by configuring the sensor to look for custom text strings in the network traffic; for example, Southern could easily configure the Cisco IDS to send an alarm on and eliminate any connection that transmits the phrase "Southern or SCSU Confidential" in e-mail or File Transfer Protocol (FTP).

\* L3 network upgrade provides a unique subnet for every telecom closet (provides traceability and controlled access to network resources on a closet by closet basis).

\* ACL's (Access Control Lists) set up between subnets as a secure method of controlling who may access what network resource. (works in concert with the subnets for each closet).

\* TACACTS (Terminal Access Controller Access Control System) and RADIUS (Remote Authentication in Dial-In User Service) for access and authentication to Local Area Network Equipment. Full logging capability provides accounting logs that are generated and filed for documentation

reference on an as-needed basis. All remote connections to Local Area Network switches and routers are via SSH encrypted sessions.

\* VPN's (Virtual Private Networks) provided for Faculty-Staff remote access via the web using SSL (Secure Sockets Layer) protocol for encryption.

\* Purchase order is out for a wireless gateway that will authenticate, provide access and generate accounting records for all wireless users on Southern's LAN.

\* Purchase order is out for a wireless network tool that enables us to discover rogue access points, do complete site surveys before for optimum placement of access points, ensure all users employ the right level of security, wireless Intrusion Detection.

#### **e) Academic Computer Center/ Student Computer Labs – (Joe Brignola)**

The objective of this document is to explain the current procedures used in the Academic Computer Center (ACC) student computer lab rooms as related to its security measures. This will include the major PC (Windows), Macintosh and Unix student computer lab rooms.

#### **DETAILS**

The ACC has 20 supported student computer lab rooms throughout the campus. They all follow similar procedures as follows:

1. Each room is keyed locked with only certain full time individuals with a key. When the room is not in use, the rooms are kept locked. Any part-time employee that needs to open the rooms after normal business hours, access is granted through Campus Police.
2. Students entering the room must sign in on a log sheet at the door.

3. Students must also show their current student ID card.
4. Students must use their current student ID card to print any work.
5. New login procedures, for the FALL 2003, will require all students to have a current computer account and log in and out of the computers to use them. Log files will be kept on their activity and their current status as a student will be checked periodically.
6. Student employees are available to help and supervise in these rooms at all times.

**f) Southern Connecticut State University**

**Banner Account and System Access Form**

Access to Banner system modules and networks imposes certain responsibilities and obligations and is granted subject to university policies, and local, state and federal law.

Acceptable use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, individual's rights to privacy, and to freedom from intimidation and harassment.

**GUIDELINES:**

**In making acceptable use of resources YOU MUST:**

- Use resources only for authorized purposes.
- Protect your Banner User ID and System information from unauthorized use.
- You are responsible for ALL activity attributed to your Banner User ID.
- Access only information that you have been given authorization/access to work with.

**In making acceptable use of resources you MUST NOT:**

- Use another person's User ID, password, files, or data without permission.
- Attempt to circumvent or subvert system or network security measures.

**I have read and understand the rights, privileges and responsibilities of being provided a Banner System User ID and Password, and agree to follow these to the best of my ability.**

(Please circle your choice(s). – Explain special needs on back of form. – Thank you.)

\_\_\_\_ This is a **FIRST TIME** Banner Account. I need CHAIRPERSON, FACULTY, and STAFF access.

\_\_\_\_ I currently have a Banner Account and need CHAIRPERSON, FACULTY and STAFF access.

Employee Name (Please Print)

\_\_\_\_\_ Dept/\_\_\_\_\_

Signature \_\_\_\_\_ Date \_\_\_\_\_

**Comments:**

---

---

---

---

**Office Use only:**

**Account Name:** \_\_\_\_\_

**Department:** \_\_\_\_\_

**Initial Password:** \_\_\_\_\_

**Type(s) of Access:** \_\_\_\_\_

\_\_\_\_\_

## g) Information Security Programs Under Gramm-Leach-Bliley

**(Notes following were drafted for the Educause 2003 Networking Conference)**

<http://www.educause.edu/conference/networking/2003/>

**Q.** What is the law?

**A.** The law is Financial Services Modernization Act of 1999[1][1], also known as the Gramm-Leach-Bliley Act (GLB). It regulates the disclosure of non-public personal information[2][2] by financial institutions.

Institutions of higher education (IHEs) are covered by the law's definition of "financial institutions" as they participate in financial activities, such as offering Federal Perkins Loans.

**Q.** What does the law require of IHEs?

**A.** IHEs must have a written information security program. The purposes are threefold:

To insure the security and confidentiality of customer information;

To protect against any anticipated threats or hazards to the security or integrity of such information; and

To protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

**Q.** Who is a customer ?

**A.** A customer is defined as a consumer who has a customer relationship with you.[3][3] A consumer means an individual who obtains or has obtained a financial product or service from you that is used primarily for personal,

family, or household purposes, or that individual's legal representative.[4][4] This would include a student who obtained a loan from the school or parents who sent in income tax information in connection with their child's application for a financial aid package.

However, as it does not make sense to have safeguards in place for only those students who have obtained loans from the university given practical issues as well as other laws such as FERPA, most IHEs will be considering a comprehensive security program. In the same vein, if you are protecting customer credit card information under the law, it makes sense to apply the security controls to all credit card information held by the IHE.

The law covers both paper copies of information and electronic copies. The safeguarding provision applies not only to all such information about persons with whom the university has a customer relationship, but also pertains to customers of other financial institutions that have provided such information.

**Q.** What is customer information?

**A.** In a general sense, customer information typically gathered in connection with obtaining a financial product or service to includes names, addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers.[5][5]

**Q.** What is a financial product or service?

**A.** The term financial product or service is defined in 16 CFR 313.3(l)(1) as "any product or service that a financial holding company could offer by engaging in a financial activity under section 4(k) of the Bank Holding Company Act of 1956." That, in turn, takes you to certain sections of the Federal Reserve Board's so-called "Regulation Y," specifically 12 CFR 225.26 and 225.28.

Regulation Y, which is permissive and therefore not a very apt vehicle for defining what GLB requires, includes the activities that we all agree are subject to GLB, like making student or faculty loans, as well as some oddities that may also be applicable to colleges and universities, like career counseling services to individuals who seek employment at financial institutions, and management consulting activities on any subject to a financial institution and on financial, economic, accounting, or audit matters to any company (which might apply to business school practicum programs).\*

The FTC has agreed to work with the higher education community in defining how GLB applies to colleges and universities.

**Q.** What is the time frame?

**A.** The May 2002 regulations under this law dictate that by May 23, 2003 the IHE must have implemented an information security program. There are a

number of components to the program, which will be addressed below. As long as the written plan is in place by May 23, 2003 (or a fairly comprehensive draft), it would seem the university would be exposed to minimal liability if the training is not completed by May 23, 2003, so long as implementation has begun.

**Q.** What are the general components of the program?

**A.** IHEs must develop, implement and maintain a comprehensive written information security program that contains administrative, technical and physical safeguards that are appropriate to the school's size and complexity, the nature and scope of the IHE's activities, and the sensitivity of any customer information at issue. The written program does not have to be all in one document, e.g. it can be a combination of policies, (perhaps some already in existence) that together equal a comprehensive policy. Review your existing policies and see where the gaps are.

**Q.** Didn't universities get an exemption from this law?

**A.** There are two different sets of rules under this law; the safeguarding rules at 16 CFR Part 314 and the privacy rules at 16 CFR Part 313. Institutions of higher education, while not exempt from the definition of "financial institutions," are generally excluded from the requirement to comply with the GLB privacy policy regulations as long as the institution

complies with the Family Educational Rights and Privacy Act. IHEs are not exempt from the safeguards requirements of the law. The final rules on the safeguarding program came out in May 2002.

\* This answer on financial product or service provided courtesy of Jeff Swope, Palmer and Dodge, LLP

### **h) Family Educational Rights and Privacy Act (FERPA)**

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
  - School officials with legitimate educational interest;
  - Other schools to which a student is transferring;

- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

For additional information or technical assistance, you may call (202) 260-3887 (voice). Individuals who use TDD may call the Federal Information Relay Service at 1-800-877-8339.

Or you may contact us at the following address:

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

[▲Top](#)

This page last modified—May 6, 2003 (jer).

---