E-Sign Act
The Electronic Signatures in Global and National Commerce Act (E-Sign Act) was enacted on June 30, 2000. The E-Sign Act provides, in part, that a signature, contract, or other record relating to a transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form or because an electronic signature or electronic record was used in its formation.

Disclosures via website
Subject to certain conditions, disclosure may be made through Internet or intranet sites.
CFR 34 668.41(b) & (c)

Voluntary consent required
Voluntary consent to participate in electronic transactions is required for all financial information provided or made available to student loan borrowers and for all notices and authorizations to FSA recipients required under 34 CFR 668.165—Notices and Authorizations.

See *Volume 4* for more information on notices and authorizations for disbursements.

Using electronic processes for notifications & authorizations
So long as there are no regulations specifically requiring that a notification or authorization be sent via U.S. mail, a school may provide notices or receive authorizations electronically. You may also use an electronic process to provide required notices and make disclosures by directing students to a secure website that contains the required notifications and disclosures.

For additional information on electronic transactions involving student loans, see Section 2 of *Standards for Electronic Signatures in Electronic Student Loan Transactions*, in GEN-01-06, May 2001.

The School Eligibility Channel may make further disclosures of this information to the Department's Office of Inspector General and to the U.S. Department of Justice under 34 CFR 99.33(b). Schools should check with the program review staff to find out if any redisclosure is anticipated.

THE E-SIGN ACT & INFORMATION SECURITY

The E-Sign Act permits lenders, guaranty agencies, and schools to use electronic signatures and electronic records in place of traditional signatures and records that, under the HEA and underlying regulations, otherwise must be provided or maintained in hard-copy format.

The E-Sign Act provides specifically for the creation and retention of electronic records. Therefore, unless a statute or regulation specifically requires a school to provide or maintain a record or document on paper, your school may provide and maintain that record electronically. Similarly, unless a statute or regulation specifically requires schools to obtain a pen and paper signature, you may obtain the signature electronically as long as the electronic process complies with the E-Sign Act and all other applicable laws.

Obtaining voluntary consent for electronic transactions

Before conducting electronic transactions to provide to a recipient of FSA funds, the recipient must affirmatively consent to the use of an electronic record. The recipient's consent must be voluntary and based on accurate information about the transactions to be completed.

The consent must be obtained in a manner that reasonably demonstrates that the individual is able to access the information to be provided in an electronic form. For example, if you are going to send financial information by email, you could send a request for consent to the recipient via email, require the recipient to respond in a like manner, and maintain a record of that response.

Safeguarding confidential information in electronic processes

Any time a school uses an electronic process to record or transmit confidential information or obtain a student's confirmation, acknowledgment, or approval, the school must adopt reasonable safeguards against possible fraud and abuse. Reasonable safeguards a school might take include password protection, password changes at set intervals, access revocation for unsuccessful logins, user identification and entry-point tracking, random audit surveys, and security tests of the code access.

If your school uses an electronic process to provide notices, make disclosures, and direct students to a secure website, it must provide notice of this each year to each student, whether via email, campus mail, or the traditional mail of the U.S. Postal Service.

The annual individual notice must

- identify the information required to be disclosed that year,
- provide the exact Web address for the information,
- state that persons are entitled to a paper copy upon request, and
- inform students how to request a paper copy.

Establishing & maintaining an information security program

The Federal Trade Commission (FTC) has ruled that most colleges are subject to the provisions of the Financial Services Act's Security Provisions (also known as the Financial Services Modernization Act). In the regulation, the commission created a definition of financial institutions that includes most colleges on the basis of the financial relationships they have with students, donors, and others. Consequently, colleges must draft detailed policies for handling financial data covered by the law, such as parents' annual income, and must take steps to protect the data from falling into the wrong hands.

Financial institutions, including postsecondary institutions, are required to have adopted an information security program under the FTC rule. For specific requirements, see the box on "FTC Standards for Safeguarding Customer Information" on the following pages.

Thus, while schools have maximum flexibility in choosing a system that provides for electronic requests for release of personally identifiable information, they must ensure that their systems provide adequate safeguards.

Information security requirements

➔ Federal Trade Commission regulations:
16 CFR 313.3(n) and 16 CFR 314.1–5
➔ Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act or GLB Act)
Pub. L. No. 106-102
Sections 501 and 505(b)(2)
➔ 15 USC 6801(b), 6805(b)(2)

Reporting security breaches to students and ED

Schools are strongly encouraged to inform their students and the Department of any breaches of security of student records and information. The Department considers any breach to the security of student records and information as a demonstration of a potential lack of administrative capability.

PREVENTING COPYRIGHT VIOLATIONS

A school must implement written plans to effectively combat the unauthorized distribution of copyrighted material by users of the school's network without unduly interfering with educational and research use of the network.

These plans must include the use of one or more technology-based deterrents and must include procedures for handling unauthorized distribution of copyrighted material (including disciplinary procedures). No particular technology measures are favored or required for inclusion in the school's plans, and each school retains the authority to determine its own plans, including those that prohibit content monitoring.

The school's plans must also include measures to educate its community about appropriate versus inappropriate use of copyrighted material, including the information described under the student consumer information rules in *Chapter 6*. These mechanisms may include any additional information and approaches that the school determines will contribute to the effectiveness of the plans. For instance, the school might include pertinent information in student handbooks, honor codes, and codes of conduct in addition to email and/or paper disclosures.

Copyright requirements

Program Participation Agreement
34 CFR 668.14(b)(30)
See *Chapter 6* for requirement to disseminate copyright policies.

Examples of deterrents

Technology-based deterrents include bandwidth shaping, traffic monitoring, accepting and responding to Digital Millennium Copyright Act (DMCA) notices, and commercial products designed to reduce or block illegal file sharing.
GEN-10-08

FTC Standards for Safeguarding Customer Information

Colleges participating in the FSA programs are subject to the information security requirements established by the FTC for financial institutions.

Customer information that must be safeguarded

These requirements apply to all customer information in your school's possession, regardless of whether it pertains to students, parents, or other individuals your school has a customer relationship with or pertains to the customers of other financial institutions that have provided such information to you.

Customer information means any record containing nonpublic personal information[1] about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

Establishing & maintaining an information security program

As a financial institution covered under these information security requirements, your school must develop, implement, and maintain a comprehensive information security program.[2]

The information security program must be written in one or more readily accessible parts and contain administrative, technical, and physical safeguards that are appropriate to the size and complexity of the school, the nature and scope of its activities, and the sensitivity of any customer information at issue.

The safeguards shall be reasonably designed to achieve the following objectives:

- insure the security and confidentiality of customer information,
- protect against any anticipated threats or hazards to the security or integrity of such information, and
- protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Required elements of an information security program

Designated coordinators. Your school must designate an employee or employees to coordinate its information security program.

Risk assessment. Your school must identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information and assess the sufficiency of any safeguards in place to control these risks.

At a minimum, the school's risk assessment should include consideration of risks in each relevant area of your operations, including

- employee training and management;
- information systems, including network and software design, as well as information processing, storage, transmission, and disposal, and
- detecting, preventing, and responding to attacks, intrusions, or other system failures.

Safeguards & testing/monitoring. Your school must design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

Evaluation & adjustment. Your school must evaluate and adjust its information security program in light of the results of the required testing and monitoring, as well as for any material changes to your operations or business arrangements or any other circumstances that it has reason to know may have a material impact on your school's information security program.

Overseeing service providers. A service provider is any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to your school. Your school must take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue and require your service providers by contract to implement and maintain such safeguards.

[1] Personally identifiable financial information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

[2] The administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

Sources:
FTC regulations: 16 CFR 313.3(n) and 16 CFR 314.1–5
Gramm-Leach-Bliley Act: Sections 501 and 505(b)(2)
U.S. Code: 15 USC 6801(b), 6805(b)(2)

The school must have a written plan for the periodic review of the effectiveness of these measures, using relevant assessment criteria.

The school must, in consultation with its chief technology officer (or other designated officer), periodically review the legal alternatives for downloading or otherwise acquiring copyrighted material (and disseminate the results, as described in *Chapter 6*) and offer legal alternatives for downloading or otherwise acquiring copyrighted material (to the extent practicable and as determined by the school).

The Department anticipates that individual institutions, national associations, and commercial entities will develop and maintain up-to-date lists that may be referenced for compliance with this provision.