

FERPA & Red Flags Rule *for Students*



MADISON
AREA | TECHNICAL
COLLEGE

MADISON COLLEGE

FERPA & Red Flags Rule Tutorial

Part I: FERPA



MADISON
AREA | TECHNICAL
COLLEGE

What is FERPA?

The **Family Educational Rights and Privacy Act of 1974 (FERPA)**, as amended (also referred to as the Buckley Amendment), is a Federal law designed to protect the confidentiality of a student's educational records.

FERPA governs the release of student educational records by the college and access to these records. Institutions may not disclose information from student education records without a student's written consent (with a few exceptions noted later in this tutorial).

This act is enforced by the Family Policy Compliance Office, U.S. Department of Educational, Washington, D.C.

FERPA & Red Flags Rule Tutorial

Who is covered under FERPA?

Students who are or have been in attendance at the college **are covered** under FERPA. FERPA rights begin once a student is "in attendance". For Madison College this means when the student has registered the first time.

Applicants who are denied admission or who never enrolled at the institution **are not covered** under FERPA.

Primary Rights of Students Under FERPA

- To inspect and review their education records.
- To request to amend their education records to ensure accuracy.
- To have control over the disclosure of personally identifiable information from their education records.
- To file a complaint with the U.S. Department of Education if they believe that Madison College has failed to comply with the requirements of FERPA (Family Policy Compliance Office, U.S. Department of Education, 400 Maryland Avenue, SW, Washington, DC 20202-4605).

Education Records

“Education Records” are all records that:

- Contain information directly related to the student.
- Are maintained by an educational agency or institution or by a party acting on behalf of the agency or institution.
- Can exist in any medium including: printed, handwritten, computer-generated, videotape, film, microfilm, email and any other form of electronic storage.

Exceptions to “Education Records” include:

- Sole Possession Records – Personal notes kept by faculty/staff if kept in the sole possession of one who made the record and never revealed to another individual.
- Employment Records of those whose employment record is not contingent upon being a student.
- Law Enforcement Records maintained by law enforcement unit of the college that were created by the law enforcement unit for the purpose of law enforcement only.
- Doctor-patient privilege records.
- Alumni Records or those that ONLY contain non-standard data collected about students who no longer attend. The data has been collected after last attendance or graduation.

Examples of Education Records

- Student information displayed on a computer screen
- Student Schedules
- Class Rosters
- Class Assignments
- Grade Rosters
- Grades
- Transcripts
- Degree Audits
- Any printed material with a student ID on it, or other personally identifiable information

Access to Records

Access to information should be limited to individuals who are "school officials" with a "legitimate educational interest" in the specific information being accessed.

Who is considered a "School Official"?

- A person employed by the institution in an administrative, supervisory, academic or research, or support staff position.
- A person serving on an institutional governing body.
- A person employed by or under contract to the institution to perform a special task, such as an attorney or auditor.
- A person or organization acting as an official agent of the institution and performing a common business function or service on behalf of the institution.
- A student serving on a committee.

Prior Written Consent

FERPA requires that Madison College obtain a student's written consent prior to disclosing any other personally identifiable information contained in education records except to school officials with legitimate educational interests or other authorized representatives under FERPA.

The student must provide signed and dated written consent in person with photo ID before disclosure. The consent must:

- Specify records to be disclosed
- State purpose of disclosure
- Identify party or class of parties to whom disclosure may be made

Example of Prior Consent at Madison College:

Madison College's **Authorization to Disclose Academic Information and Grades** (available on Blackboard).

Exceptions to Prior Written Consent Requirement

Non-directory information is not released to anyone other than the student, except for the following agencies which can receive this data without the student's permission as provided by the Privacy Act:

- School officials with legitimate educational interest.
- Federal, State, and local authorities involving an audit or evaluation of compliance with education programs.
- Agencies providing financial assistance to the student, such as employers, Division of Vocational Rehabilitation and the Veterans Administration.
- Properly authorized educational authorities for the purpose of research, provided that the information is not given in personally identifiable format.
- Accrediting organizations carrying out their accrediting functions.
- Courts or legal officers on the basis of a subpoena.
- In connection with a health or safety emergency if necessary to protect the student or others.
- The Wisconsin Technical College Board as part of the process of securing state funds.
- State and local officials to whom disclosure is required by the state statute adopted prior to November 19, 1974.

Public Access to Records

- The public may obtain directory information.
- The public may obtain non-directory information by obtaining a signed consent from the student.
- The College must comply with the Wisconsin Open Records Law and requests for information submitted under this law.

What is restricted or protected under FERPA?

- **Access to Student Records** – At the postsecondary level, the public has no inherent rights to access or inspect a student's education records. This right is limited solely to the student.
- **Grades, Progress Report, Exams** – Such things as progress in a course, deficiencies in a subject area, scores, and grades are all examples of personally identifiable information that make up a student's education record. This information is protected under FERPA and parents may not have access unless the student has provided prior written consent identifying what information may be released.

Directory Information

Directory Information is information which would not generally be considered harmful or an invasion of privacy if disclosed. A policy for identifying directory information, or having no directory information at all, must be determined and adhered to by institutions. Students have the right to restrict the disclosure of this information.

The following information has been identified as Directory Information, and some or all of it may be made public if the student has not requested that it be withheld:

- Name
- Major Field of Study (Program)
- Participation in Officially Recognized Activities and Sports
- Weight and Height of Members of Athletic Teams
- Dates of Attendance (Term Start/End Dates–Not specific dates)
- Enrollment Status (Full or Part-time)
- Degrees and Awards Received
- Email Address

A Student's Right to Withhold Directory Information

A student has the right to request that all directory information not be disclosed. To withhold all directory information, complete a **Request to Withhold Student Information** form and submit it with photo ID to the Enrollment Center, Madison College, 1701 Wright Street, Madison, WI 53704.

Due to the consortium between Madison College and Western Technical College, requests submitted by students of both institutions to Madison College will affect student record information at both institutions until revoked.

Upon submitting the request, all future requests must be made in-person with photo ID or accessed online by signing on the [myMadisonCollege](#) Student Center. This includes, but is not limited to:

- Class registration
- Class schedules
- Transcript requests
- Financial aid inquiries
- Account inquiries

Requests to Review Education Records

A student may submit a written request identifying the records he or she wishes to inspect.

- Requests to review education records must be made in writing to the Enrollment Center. Review may be immediate, but the Enrollment Center may take up to 45 days to honor the requests if files are not accessible.
- If photocopies of records are requested, fees for copies are the same rate charged by the college library.
- Should a student find a part of his or her education records misleading or inaccurate, they may submit a written request to the Enrollment Center clearly identifying the part of the record requesting to be changed and specifying the reason it is inaccurate or misleading. If the decision is not to amend the record as requested, the student will be notified and advised as to his or her right to a hearing as well as hearing procedures.

FERPA Resources & Links

College Resources:

- [Protection of Student Records](http://madisoncollege.edu/protection-student-records) – madisoncollege.edu/protection-student-records
- [Access to Student Records](http://madisoncollege.edu/access-student-records) – madisoncollege.edu/access-student-records
- **Questions?** Contact the Enrollment Center submit a Records Category question online through askMadisonCollege, phone (608) 246-6210 or visit us in person at the Truax Campus, Room A1000.

Federal Resources:

- [Family Policy Compliance Office](http://ed.gov/policy/gen/guid/fpco/ferpa) – ed.gov/policy/gen/guid/fpco/ferpa
- [FERPA for Students](http://ed.gov/policy/gen/guid/fpco/ferpa/students) – ed.gov/policy/gen/guid/fpco/ferpa/students
- **Questions?** Contact the Family Policy Compliance Office:
Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, DC 20202-8520

MADISON COLLEGE

FERPA & Red Flags Rule Tutorial

Part II: Red Flags Rule



MADISON
AREA | TECHNICAL
COLLEGE

What is the Red Flags Rule?

Signed into law in 2003, the Red Flags Rule (RFR) is a component of the Federal Trade Commission's (FTC) Fair and Accurate Credit Transactions (FACT) Act.

Section 114 of the act requires the College to have an Identity Theft Prevention Program designed to detect, prevent and mitigate Identity Theft in connection with opening an account or an existing account.

The Red Flags Rule allows the College to detect and respond to any Red Flags to prevent and mitigate Identity Theft:

- **Red Flags** – Patterns, practices or activities that indicate the possibility of Identity Theft.
- **Identify Theft** – Fraud committed or attempted using another person's identifying information without authority.

Which accounts require the College's compliance?

Two types of accounts require compliance – covered accounts and service provider accounts. Even though the College is not a financial institution, compliance is required.

1. **Covered Accounts** (established with College to obtain services or products for personal purposes):

- Federal and Emergency Loans and Loan Refunds
- Direct Deposit information
- 1098-T information & Wisconsin Tax Refund Intercept Program accounts
- Delinquent Accounts sent to Collection agency
- Contracted agreements, including third-party arrangements
- Active OneCard debit accounts

2. **Service Provider Accounts** (established between the College and another business to provide the College with a service):

- Online payments
- Collection recovery

What does the RFR mean for the College?

Each institution is responsible for determining and implementing their own unique RFR program. The program will be updated whenever significant changes in business processes occur, as new processes require new techniques to monitor for fraud.

Compliance is attained through a four-step process:

1. Identifying Red Flags
2. Detecting Red Flags
3. Prevention & Mitigation of Identify Theft
4. Annual Review and Updates

STEP 1: Identifying Red Flags

A. Notifications and Warnings from Credit Reporting Agencies

- Report of fraud accompanying a credit report.
- Notice of report from a credit agency of a credit freeze on an applicant.
- Notice or report from a credit agency of an active duty alert for an applicant.
- Receipt of a notice of address discrepancy in response to a credit report request.
- Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

STEP 1: Identifying Red Flags

B. Suspicious Documents

- Identification document or card that appears to be forged, altered or inauthentic.
- The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification.
- A request for service that appears to have been altered or forged.
- A request made from a non-college issued e-mail account.
- A request to mail something to an address not listed on the file.

STEP 1: Identifying Red Flags

C. Suspicious Identifying Information

- Identifying information presented that is inconsistent with other information the student provides (e.g., inconsistent birth dates).
- Identifying information presented that is inconsistent with other sources of information (e.g., address mismatch on personal documents).
- Identifying information presented that is the same information shown on other applications that were found to be fraudulent.
- Identifying information presented that is consistent with fraudulent activity (e.g., invalid phone number or fictitious billing address).
- Social security number presented that is the same as one given by another person.
- A person's identifying information is not consistent with the information that is on file for the student.

STEP 1: Identifying Red Flags

D. Suspicious Account Activity

- Account used in a way that is not consistent with prior use.
- Mail sent to the student is repeatedly returned as undeliverable.
- Notice to the College that a student is not receiving mail sent by the College.
- Notice to the College that an account has unauthorized activity.
- Breach in the College's computer security system.
- Unauthorized access to or use of student account information.

E. Alerts from Others

Notice to the College from a student, Identity Theft victim, law enforcement or other person that the College has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

STEP 2: Detecting Red Flags

A. Student Enrollment

In order to detect red flags associated with the enrollment of a student, staff should take the following steps to obtain and verify the identity of the person opening the account:

- Require certain identifying information such student ID or Social Security number, name, date of birth, academic records, home address or other identification, and
- Verify the student's identity at time of issuance of student identification card (review government-issued photo identification or other personally identifiable information).

B. Existing Accounts

In order to detect red flags for an existing covered account, staff should take the following steps to monitor transactions on an account:

- Verify the identification of students if they request information and/or services (in person with required form of photo ID,; or via telephone, facsimile or email with student ID or Social Security Number, current mailing address and phone number);
- Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes; and
- Verify changes in banking information given for billing and payment purposes.

STEP 3: Preventing & Mitigating Identity Theft

When a red flag is triggered, the College will take one or more of the following steps, depending on the degree of risk posed by the red flag:

A. Prevent & Mitigate

- Continue to monitor a covered account for evidence of identity theft.
- Contact the student or applicant.
- Change any passwords or other security devices that permit access to covered accounts.
- Not open a new covered account.
- Notify the Program Administrator for determination of the appropriate step(s) to take.
- Notify law enforcement.
- Determine that no response is warranted under the particular circumstances.
- Communicate ability to provide FERPA block on directory information.

STEP 3: Preventing & Mitigating Identity Theft

B. Protect Student Identifying Information

In order to further prevent the likelihood of identity theft, the College will take the following steps to protect student identifying information:

- Ensure that its website is secure or provide clear notice that the website is not secure.
- Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information.
- Ensure that office computers with access to covered account information are password protected, and provide automatic lock-out for computers.
- Avoid use of social security numbers.
- Ensure computer virus protection is up to date.
- Require and keep only the kinds of student information that are necessary for College purposes.

C. Should a student become aware of a potential incident of Identity Theft, the student is expected to notify the College from their Madison College student email account by sending all pertinent information to records@madisoncollege.edu.

STEP 4: Annual RFR Program Review & Update

On an annual basis, the College's program will be reviewed and potentially revised, as methods of identity theft are constantly evolving.

RFR Resources & Links

College Resources:

- [Protection of Student Accounts](http://madisoncollege.edu/protection-student-accounts) – madisoncollege.edu/protection-student-accounts
- [Student Records](http://madisoncollege.edu/student-records) – madisoncollege.edu/student-records
- **Questions?** Contact the Enrollment Center submit a Records Category question online through askMadisonCollege, phone (608) 246-6210 or visit us in person at the Truax Campus, Room A1000.

Federal Resources:

- [Fighting Fraud with the Red Flags Rule](http://ftc.gov/bcp/edu/microsites/redflagsrule) – ftc.gov/bcp/edu/microsites/redflagsrule