

Notification of Rights under FERPA for Postsecondary Institutions

The Family Educational Rights and Privacy Act (FERPA) affords students certain rights with respect to their education records. They are:

(1) The right to inspect and review the student's education records within 45 days of the day the College receives a request for access. Students should submit to the registrar, dean, head of the academic department, or other appropriate official, written requests that identify the record(s) they wish to inspect. The College official will make arrangements for access and notify the student of the time and place where the records may be inspected. If the records are not maintained by the College official to whom the request was submitted, that official shall advise the student of the correct official to whom the request should be addressed.

(2) The right to request the amendment of the student's education records that the student believes are inaccurate or misleading. Students may ask the College to amend a record that they believe is inaccurate or misleading. They should write the College official responsible for the record, clearly identify the part of the record as requested by the student, the college will notify the student of the decision and advise the student of his or her right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the student when notified of the right to a hearing.

(3) The right to consent to disclosure of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent. One exception which permits disclosure without consent is disclosure to a school official with legitimate educational interests. A school official is a person employed by the College in an administrative, supervisory, academic, or support staff position (including law enforcement unit personnel and health staff); a person or company with whom the College has contracted (such as an attorney, auditor, or collection agent); a person serving on the Board of Trustees; or person(s) assisting another school official in performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility.

Upon request, the College discloses education records without consent to officials of another school, upon request, in which a student seeks or intends to enroll. [Note; FERPA requires an institution to make a reasonable attempt to notify the student of the records requested unless the institution states in its annual notification that it intends to forward records on request.]

(4) The right to file a complaint with the U.S. Department of Education concerning alleged failures by Beville State Community College to comply with the requirements of FERPA. The name and address of the Office that administers FERPA is:

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

COMPUTER ACCESS TO RECORDS BEVILL STATE COMMUNITY COLLEGE

Information in student record files is protected by the “Family Education Rights and Privacy Act of 1974 as Amended” (FERPA), and the Bevill State Community College policy that established the general structure for which data are made accessible to data users is in compliance with FERPA. Bevill State Community College has determined that information in student record files can be changed only by personnel in the following areas: student history, Admissions/Records, financial aid, financial Aid Office; student accounts, Business Office. All other personnel, with the exception of those with administrative authority for the management of information, have “inquire” access only.

Inquiry Access

“Inquiry” access is a tool by which certain information stored on computer files may be viewed on a computer terminal/PC. “Inquiry” access allows an authorized user the opportunity to view information on specific students and courses. Information cannot be updated with “Inquiry” access.

Responsibility of Persons with Access

Persons approved for access are responsible for the security of their passwords and the protection of information. The authority to access is linked to a person’s user ID. At no time should individuals share their passwords with another person or display the password in public view. Persons approved for access are responsible for signing off when finished with access.

Persons with access will use information ONLY for the purpose approved and will not release information to any other individual or office for another purpose. Persons having access to student records should be aware that there are possible civil sanctions and College disciplinary action for violating records privacy agreements.

All persons accessing confidential or restricted student data must guarantee to maintain data about individual students in a secure fashion, such that it cannot be viewed– by screen access, file access, or in printed form– by unauthorized individuals. Although it is allowable to print a report of screen of confidential information for authorized record keeping or advising purposes, users should not release printed information to other individuals or offices. Any personally identifiable confidential data contained in print form or on computer files which are no longer needed should be destroyed in such a way that identification of a student is not possible.

All persons with access must read and sign an agreement acknowledging an understanding of their responsibilities for password security and maintaining the confidentiality of data that is accessed. This signed agreement is kept on file in the Personnel Office.

Persons with access are also responsible for terminal/PC equipment security, which included password sign-on and sign-off procedures and the proper placement of the equipment so that the screen cannot be viewed from a public location.

Termination of Employment

Supervisors of departments or units are responsible for maintaining the overall security of access and the release of information in their areas. As personnel changes occur, supervisors **MUST** notify the Director of Computer Services in order to initiate access deletion when a staff member terminates employment or transfers to another department.

Detection of Security Violation

If a security violation is detected, employees must contact their supervisors immediately. Supervisors are responsible for contacting the Director of Computer Services to request that passwords be changed.

Review and Renewal Procedures

Computer access to information in student record files will reviewed annually by the Assistant to the Dean of Student Services-Admissions.

Questions About Access

Questions regarding assistance with computer equipment and passwords should be directed to the Director of Computer Services. Questions about specific access to information or interpretations of FERPA should be directed to the Assistant to the Dean of Student Services-Admissions.

ACCEPTANCE OF RESPONSIBILITY

Computer Access to Records

I understand my acceptance of access to information in student record files signifies I assume responsibility for complying with the policy of Bevill State Community College that protects the privacy of that information and the release of that information. I have reviewed copies of and have read the policies "Computer Access to Records" and "Student Records Policies and Procedures". By my signature below, I understand and agree to preserve the security and confidentiality of information I access.

I also agree to inform my immediate supervisor (who will inform the Director of Computer Services) when my need to access information in student record files ceases to exist or change in any way.

I understand that I am responsible for the personal security of my password that there are possible civil sanctions and College disciplinary actions violating records privacy agreements.

Signature of Bevill State Community College Employee

Date