NEOSHO COUNTY COMMUNITY COLLEGE

THE FAMILY EDUCATIONAL RIGHTS & PRIVACY ACT OF 1974 (FERPA)

The Family Educational Rights and Privacy Act (FERPA) affords students certain rights with respect to the student's education records.

NCCC complies with the Family Rights and Privacy Act of 1974 by using the following policy regarding access to, and protecting the confidentiality of, student records. The Chief Academic Officer is the FERPA Compliance Officer for NCCC. For more information, call 800-729- 6222 (KS only) or 620-432-0302, office of the Vice President for Student Learning.

Upon request, any student of NCCC will be granted access to and review of any or all records pertaining directly to said student. Access to records will be granted no more than forty-five (45) days following such request. If information in these records is found to be inaccurate, misleading, or detrimental to the student, a committee composed of faculty and administrators will hear all cases challenging the content of such records. Such hearings will be scheduled within ten (10) working days of receipt of a written request for said hearing.

No personally identifiable records from NCCC will be released to parents, spouse, or others without the expressed, written consent of the student. Within the provisions of the Family Rights and Privacy Act, access will be granted to the following without the consent of the student:

a) school officials, including teachers and administrators, who have a legitimate educational interest;
b) officials of schools to which the student wishes to transfer;
c) authorized representatives of the Comptroller General of the United States, the Secretary of Education, or an administrative head of an education agency;
d) in connection with the student's application, receipt or continued eligibility/status for financial aid, or
e) a court order.

Should a student owe the College any delinquent amount, official records will not be released to the student or a third party. However, this does not preclude the student from personally reviewing his/her records and challenging any of the information. Financial aid transcripts may be sent at the request of other institutions.

The right to file a complaint with the US Department of Education concerning alleged failures by the College to comply with the requirements of FERPA. The name and address of the office that administers FERPA is:

Family Policy Compliance Office
US Department of Education
600 Independence Avenue, S.W.
Washington, D.C. 20202-4605

Gramm-Leach-Bliley Act of 1999 (GLBA)

Overview: This document summarizes Neosho County Community College's comprehensive written information security policy (the "policy") mandated by the Federal Trade Commission's Safeguards Rule and the Gramm-Leach-Bliley Act ("GLBA"). In particular, this document describes the Program elements pursuant to which the Institution intends to (i) ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers. The policy incorporates by reference, the College's existing policies and procedures and is in addition to any College policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA.

Designation of Representatives: The institution's chief information officer is designated as the program officer who shall be responsible for coordinating and overseeing the policy. The program officer may designate representatives of the Institution to oversee and coordinate particular elements of the policy. Any questions regarding the implementation of the program or the interpretation of this document should be directed to the program officer or his or her designees.

Scope of Policy: The policy applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the Institution, whether in paper, electronic or other form that is handled or maintained by or on behalf of the Institution or its affiliates. For these purposes, the term nonpublic financial information shall mean any information (i) a student or other third party provides in order to obtain a financial service from the Institution, (ii) about a student or other third party resulting from any transaction with the Institution involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.

Elements of the Policy:

Risk Identification and Assessment
The Institution intends, as part of the policy, to undertake to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the policy, the program officer will establish procedures for identifying and assessing such risks in each relevant area of the Institution's operations, including:

Employee Training and Management
The program officer will coordinate with representatives in the Institution's student/financial services and financial aid offices to evaluate the effectiveness of the Institution's procedures and practices relating to access to and use of student records, including financial aid information. This evaluation will include assessing the effectiveness of the Institution's current policies and procedures in this area.

Information Systems and Information Processing and Disposal
The program officer will assess the risks to nonpublic financial information associated with the Institution's information systems, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. This evaluation will include assessing the Institution's current polices and procedures relating to acceptable use policy, information technology security policy, and records retention policy. The program officer will also assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

Detecting, Preventing and Responding to Attacks
The program officer will evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. Designing and Implementing Safeguards.

Overseeing Service Providers
The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The program officer will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

Overseeing Service Providers
The program officer shall coordinate with those responsible for the third party service procurement activities among the department of technology services and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access.

Adjustments to Program
The program officer is responsible for evaluating and adjusting the program based on the risk identification and assessment activities undertaken pursuant to the program, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on the program.

NEOSHO COUNTY COMMUNITY COLLEGE

HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT OF 1996 (HIPAA)

This notice describes how medical information about students may be used and disclosed. Please review it carefully. If students have any questions, please contact our head athletic trainer, director of nursing, or chief student affairs officer at 800 West 14th, Chanute, Kansas 66720 or by phone at 620-431-2820.

The NCCC athletic department provides health care to our student- athletes in partnership with physicians and other professionals and organizations. The information privacy practices in this notice will be followed by all departments and all employed associates, staff or volunteer.

Medical record information and the relationship with medical staff are considered private. With proper written consent, the College will make every effort to give family medical updates as appropriate. The College creates a record of the care and services received to provide quality care and to comply with legal requirements. This notice applies to all of the records of care that we maintain, whether created by our Training staff or by the student's doctor. A personal doctor may have different policies or notices regarding the doctor's use and disclosure of medical information created in the doctor's office. The College is required by law to keep medical information about the student private, give this notice of our legal duties and privacy practices with respect to medical information about the student and follow the terms of the notice that is currently in effect.

The College may use and disclose medical information for treatment (such as sending medical information to a specialist as part as a referral); to obtain payment for treatment (such as sending billing information to an insurance company or Medicare); and to support the College's health care operations (such as comparing patient data to improve treatment methods). The College may disclose medical information and/or participation status to athletic coaches for health and safety. The College may disclose information to administrators and academic counselors to support academic progress. The College may release information to sports information staff and members of the media regarding participation status.

Regarding medical information, the student has the right to look at or get a copy of medical information that the College uses to make decisions about care. The student has the right to a personal representative to assist in reviewing medical information. If the student believes that information in the records is incorrect or incomplete, the student has the right to request that the College amend the records. The student has the right to a list of those instances where the College has disclosed medical information about the student, other than for treatment, payment, health care operations or where the student specifically authorized a disclosure.

The College reserve the right to change the terms of this notice at any time. Changes will apply to medical information the College already holds, as well as new information we receive after the change occurs. If the College changes their notice, they will post the new notice in their athletic training facilities. The student can receive a copy of the current notice at any time. The student will also be asked to acknowledge in writing the receipt of this notice on our Student- Athlete Authorization/Consent for Disclosure of Protected Health Information.