Sauk Valley Community College
Everything You've Always Wanted to Know About Privacy of Student Records But Were Afraid to Ask
August, 2003

The Gramm-Leach-Bliley (GLB) Act that took effect in May, 2003 requires colleges to take steps to ensure the security and confidentiality of student records. The goals of the college's information security program are:

- To ensure the security and confidentiality of student information;
- To protect against any anticipated threats to the security or integrity of such information; and
- To guard against the unauthorized access to or use of such information that could result in substantial harm or inconvenience to any student.

The tool we use to comply with this law is to follow the guidelines of the Family Educational Rights and Privacy Act (FERPA). All Sauk employees should possess at least a basic understanding of FERPA rules.

Table of Contents

Sauk Valley Community College
FERPA FAQs

What is FERPA?

FERPA stands for Family Educational Rights and Privacy Act (also referred to as the Buckley Amendment). Passed by Congress in 1974, the Act grants four specific rights to the adult student:

- The right to see the information that the institution is keeping on the student
- The right to seek amendment to those records and in certain cases append a statement to the record
- The right to consent to disclosure of his/her records
- The right to file a complaint with the FERPA Office in Washington

What are the basic rules?

Student educational records are considered confidential and may not be released without the written consent of the student.

As a faculty or staff member you have a responsibility to protect educational records in your possession.

Some information is considered public (sometimes called "directory information"). This information can be released without the student's written permission. However, the student may opt to consider this information confidential as well.

You have access to information only for legitimate use in completion of your responsibilities as a college employee. "Need to know" is the basic principle.

What are education records?

Information recorded in any form that is directly related to a student and maintained by the college and by those acting for the college. This includes personal information, enrollment records, grades and schedules. The storage medium in which you find the information does not matter. A student educational record may be a document in the Admissions office, a computer printout in your office, a class list on your desktop, or a computer display screen.

Education records do not include:

- Records of instructional, supervisory and administrative personnel kept in the sole possession of the maker of the record and not revealed to anyone other than the maker's substitute;
- Records of the Security department created and maintained by that department and used solely for security purposes;
- Records relating to employees, other than student workers;
- Records which include information about an individual after he/she is no longer a student.

The College must grant requests to review records within a reasonable time, no more than 45 days after the request is received.

What is directory information?

- Name
- Address
- Telephone number
- Major field of study
- Dates of attendance
- Degrees and awards received
- Most recent educational institution attended
- Photographs
- Participation in recognized activities and sports
- Weight and height of members of athletic teams

What is prior written consent?

A signed and dated document specifying the records to be disclosed, the purpose of the disclosure and the identity of the person to whom records will be disclosed.

When is consent not required?

- For legitimate educational purposes within the college.
- For officials at an institution in which the student seeks to enroll.
- To comply with a court order or subpoena.
- In connection with a health or safety emergency if necessary to protect the student or others.
- For parents of students who are dependents for income tax purposes, and who have provided IRS documentation as such.
- If it is directory information.
- For accrediting organizations.
- For appropriate parties in connection with financial aid to a student to determine eligibility, amount or conditions of financial aid, or to enforce the terms and conditions of aid.

Some special "don'ts" for faculty and staff

To avoid violations of FERPA rules, DO NOT:

- At any time, use any part of the Social Security number of a student in a public posting of grades.
- Link the name of a student with that student's Social Security number in any public manner.
- Leave graded tests in a stack for students to pick up by sorting through the papers of all students.
- Circulate a printed class list with students name and Social Security number or grades as an attendance roster.
- Discuss the progress of any student with anyone other than the student (including parents) without the consent of the student (or proper IRS documentation from parents).
- Provide anyone with lists of students enrolled in your classes for any commercial purpose.
- Provide anyone with the student schedules or assist anyone other than college employees in finding a student on campus.
- Leave the door open when your office is vacant.
- Leave grades, test scores, etc., or personal information in the classroom between classes or during breaks.
- Leave student records (class lists, grades, work or home phones, student schedules, etc.) in view on your desk or on your computer.

What can happen if we fail to follow the law?

Violations of FERPA rules can lead to lawsuits, loss of federal funding, conviction of a misdemeanor under the Public Information Act with possible imprisonment or fines, and dismissal.

Saul Valley Community College
Student Records and Confidentiality
(From College Catalog)

The College policy on student records complies with the "Family Educational Rights and Privacy Act." This Act is designed to protect the privacy of education records, to establish the rights of students to inspect and review their education records, and to provide guidelines for correction of incorrect or misleading data through formal and informal hearings. More specifically, FERPA affords students the following:

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, Director of Admissions and Records, or the Dean of Student Services 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.

2. The right to request the amendment of the student's education records that the student believes is 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 they want changed, and specify why it is inaccurate or misleading. If the College decides not to amend 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 amendments.

3. The right to consent to disclosures of 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 school officials with legitimate educational interests. A school official is defined as a person employed by the College in an administrative, supervisory, academic, or support staff position (including law enforcement unit 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 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.

4. The right to file a complaint with the U.S. 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
    U.S. Department of Education
    400 Maryland Avenue, SW
    Washington, DC 20202-4605

No one outside of the College shall have access to nor will the College disclose any information about student education records without the written consent of the student. Exceptions are:

- School officials demonstrating a legitimate educational interest
- Schools in which a student seeks or intends to enroll
- Federal, State, and local authorities involved in auditing or evaluating compliance with education programs
- In connection with financial aid
- Organizations conducting studies for or on the behalf of educational institutions
- Accrediting organizations
- Parents of a dependent student, as defined by the IRS
- Compliance with a judicial order or subpoena (the College must make a reasonable effort to notify the student in advance of compliance)
- Directory information
- Results of a disciplinary hearing to an alleged victim of a crime of violence
- Certain agencies such as the U. S. Attorney General's Office, and the state education agencies

The following information is designated by the College as a public or "Directory Information" and **may not be released** for any purpose at the discretion of the College.

- Name
- Address
- Telephone number
- Major field of study
- Dates of attendance
- Degrees and awards received
- Most recent educational institution attended
- Photographs
- Participation in recognized activities and sports
- Weight and height of members of athletic teams

Currently enrolled students may request to withhold Directory Information by submitting to the Office of Admissions and Records a "Request to Prevent Disclosure of Directory Information" form. A copy of the Act or questions concerning the Family Educational Rights and Privacy Act may be referred to the Dean of Student Services, ext. 305

Helpful Guidelines to Implement FERPA

How can you protect information? What can you do to assure confidentiality? Listed below are some strategies rules, basic in-office, and out-of-office procedures. The list is not all-inclusive but will provide a helpful start.

Only access information if it is job related

Do not "look up" information about your friends, enemies, neighbors, family, etc. unless it is job related, unless there is a "need to know". That is, you may have to file something in a friend's file-**YES, it's job related;** your sister comes in to request a copy of her academic transcript-**YES, it's job related**. You want to know what grade your daughter earned in a class- **NO, it's not job related;** you want to find out what classes your friend registered for-**NO, it's not job related.**

Protect information from others

Clear your computer screen when you leave your desk or if you are dealing with another student. Someone looking at your terminal may find out all kinds of information about the student whose record you have on your computer screen. Do not throw any "education records" in the garbage or recycle bin; instead shred anything that is to be thrown away so the students name, social security number, grades, etc. are protected.

Do not discuss students by name or situation in a public place where other students or people are present. Do not make any comments about a student at work or away from work. It is sometimes very easy to add something to a social conversation such as "he says he's so smart. Well, I know he only has a 1.25 GPA at Sauk".

Dealing with parents and spouses

Parents and spouses have no inherent rights to inspect a student's education records or to be given information about the student (unless it is directory information). **The right to inspect is limited solely to the student.** Records may be released to parents or spouses only if student has given his/her written consent.

Preventing the release of information

If a student has requested not to release information, a "Confidentiality" warning will appear on the computer screen when you access that student on the computer system. This means no information, including directory information, may be released. Nothing may be released; no telephone number, no address, nothing usually allowed under the release of directory information. Your response to the individual requesting information should be, "We have no information about this person." If the individual persists, refer him/her to the Registrar, Director of Admissions, or Dean of Student Services.

If you are ever in doubt, do not release any information until you consult with the Registrar, Director of Admissions, or Dean of Student Services.

Electronic Information Security Policy

Introduction

The ability to store College data on computers and share it across the network enhances use and expands our functionality. Commensurate with that expansion is the need for appropriate security measures. Security is not distinct from the functionality.

The Electronic Information Security Policy (Policy) recognizes that not all communities within the College are the same and that data is used differently by various units within the College. The principles of academic freedom apply to this policy, and this policy is not intended to limit or restrict those principles. These policies apply to all units within the College.

Each unit within the College should apply this policy to meet their information security needs. The Policy is written to incorporate current technological advances. The technology installed at some units may limit immediate compliance with the Policy. Instances of non-compliance must be reviewed and approved by the Dean of Information Services in conjunction with the Information Security Committee.

Throughout the document, the terms "must" and "should" are used carefully. Musts are not negotiable; should are goals for the College. The terms "data" and "information" are used interchangeably in the document.

The terms "system" and "network administrator" are used in this document. These terms are generic and pertain to any person who performs those duties, not just those with it as their primary job duty. Many students, faculty, and staff members are the system administrators for their own machines.

Purpose of This Policy

By "information security", we mean protection of the College's data; we mean protection of the College's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.
The purpose of the information security policy is:

- To establish a College-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of College data, applications, networks and computer systems.
- To define mechanisms that protect the reputation of the College and allow the College to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

Responsibility

The Dean of Information Services in cooperation with the Committee is responsible for implementing the policy.

The Committee must see to it that:

- The information security policy is updated on a regular basis and published as appropriate.
- Appropriate training is provided to data owner, data custodians, network and system administrators, and users.
- Each unit appoints a person to be responsible for security implementation, incident response, periodic user access reviews, and education of information security policies including, for example, information about virus infection risks.

Members of the Committee are each responsible for establishing procedures to implement these polices within their areas of responsibility, and for monitoring compliance.

General Policy

Required Policies

- The College will use a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the College's data, network and system resources.
- Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.

Recommended Practices

- Vulnerability and risk assessment tests of external network connections should be conducted on a regular basis. At a minimum, testing should be performed annually, but the sensitivity of the information secured may require that these tests be done more often.
- Education should be implemented to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This should be tailored to the role of the individual, network administrator, system administrator, data custodian, and/or users.
- Violation of the Information Security Policy may result in disciplinary actions as authorized by the College.

Data Classification Policy

It is essential that all of the College's data be protected. There are, however, graduations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. We have specified three classes below:

High Risk- Information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA, GLB, or the Data Protection Act, are in this class. Payroll, personnel, and financial information are also in this class because of privacy requirements.

This policy reorganizes that other data may need to be treated it would be treated as high risk because it would cause damage to the College if disclosed or modified. The data owner should make this determination. It is the data owner's responsibility to implement the necessary security requirements.

Confidential- Data that would not expose the College to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. It is the data owner's responsibility to implement the necessary security requirements.

Public- Information that may be freely disseminated.

All information resources should be categorized and protected according to the requirements set for each classification. The data classification and it's corresponding level of protection should be consistent when the data is replicated and as it flows through the College.

- Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.
- No College –owned system or network subnet can have a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
- Data custodians are responsible for creating data repositories and data transfer procedures which protect data in the manner appropriate to its classification.
- High risk data must be encrypted during transmission over insecure channels.
- Confidential data should be encrypted during transmission over insecure channels.
- All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.
- Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified, deleted, or disks destroyed consistent with industry best practices for the security level of data.

Access Control Policy

- Data must have sufficient granularity to allow the appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. This balance should be recognized.
- Where possible and financially feasible, more than one person must have full rights to any College owned server storing or transmitting high risk data. The Department of Information Services will have a standard policy that applies to user access rights. This will suffice for most instances. Data owners or custodians may enact more restrictive policies for end-user access to their data.
- Access to the network and servers and systems will be achieved by individual and unique logins, and will require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.
- As stated in the Acceptable Use Policy, users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files and documents. All users must secure their username or account, password, and system from unauthorized use.
- All users of systems that contain high risk or confidential data must have a strong password, the definition of which will be established and documented by Department of Information Services after consultation with the user community. Empowered accounts, such as administrator root, or supervisor accounts, must be changed frequently, consistent with guidelines established by Information Services.
- Passwords must not be placed in emails unless they have been encrypted.
- Default passwords on all systems must be changed after installation. All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, and reconfigured.
- Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.
- Users are responsible for safe handling and storage of all College authentication devices. Authentication tokens should not be stored with a computer that will be used to access the College's network or system resources. If an authentication device is lost or stolen, the loss must be immediately reported to the appropriate individual in the issuing unit so the device can be disabled.
- Terminated employee access must be reviewed and adjusted as found necessary. Terminated employees should have their accounts disabled upon transfer or termination. Since there could be delays in reporting changes in user responsibilities, periodic user access reviews should be conducted by the unit security person.
- Transferred employee access must be reviewed and adjusted as found necessary.
- Monitoring must be implemented on all systems including recording log on attempts and failures, successful log on and date and time of log on and log off.
- Activities performed as administrator or super user must be logged where it is feasible to do so.
- Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks. There should be a documented procedure for reviewing system logs.

Virus Prevention Policy

- The willful introduction of computer viruses or disruptive/destructive programs into the College environment is prohibited, and violators may be subject to prosecution.
- All desktop systems that connect to the network must be protected with an approved, licensed anti-virus software product that it is kept updated according to the vendor's recommendations.
- All servers and workstations that connect to the network and are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that is updated according to the vendor's recommendations.
- Headers of all incoming data including electronic mail will be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail will be scanned where such capabilities exist.
- Where feasible, system or network administrators should inform users when a virus has been detected.
- Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

Intrusion Detection Policy

- Intruder detection must be implemented on all servers and workstations containing data classified as high risk.
- Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.
- Server, firewall, and critical system logs should be reviewed frequently. Where possible, automated review should be enabled and alerts should be transmitted to the administrator when a serious intrusion is detected.
- Intrusion tools should be installed where appropriate and checked on a regular basis.

Internet Security Policy

- All connections to the Internet must go through a properly secured connection point to ensure the network is protected when the data is classified high risk.
- All connections to the Internet should go through a properly secured connection point to ensure the network is protected when the data is classified confidential.

System Security Policy

- All systems connected to the Internet should have a vendor supported version of the operating system installed.
- All systems connected to the Internet must be current with security patches.
- System integrity checks of host and server systems housing high risk College data should be performed.

Acceptable Use Policy

An acceptable use policy will be available that includes these requirements:

- College computer resources will be used in a manner that is compliant with College policies and State and Federal laws and regulations. It is against College policy to install or run software requiring a license on any College computer without a valid license.

- Use of the College's computing and networking infrastructure by College employees unrelated to their College positions must be limited in both time and resources and must not interfere in any way with College functions or the employee's duties. It is the responsibility of employees to consult their supervisors, if they have any questions in this respect.
- Uses that interfere with the proper functioning or the ability of others to make use of the College's networks, computer systems, applications, and data resources are not permitted.
- Use of College computer resources for personal profit is not permitted except as addressed under the College policies.
- Decryption of passwords is not permitted, except by authorized staff performing security interviews or investigations. Use of network sniffers shall be restricted to system administrators who must use such tools to solve network problems. Auditors or security officers in the performance of their duties may also use them. They must not be used to monitor or track any individual's network activity except under special authorization as defined by campus policy that protects the privacy of information in electronic form.

Exceptions

In certain cases, compliance with specific policy requirements may not be immediately possible. Reasons include, but are not limited to, the following:

- Required commercial or other software in use is not currently able to support the required features;
- Costs for reasonable compliance are disproportionate relative to the potential damage.

In such cases, units must develop a written explanation of the compliance issue, a plan for coming into compliance in a reasonable amount of time, and submit them to the Committee for written approval.

Sauk Valley Community College
FERPA Quiz

If a student's parents calls asking how a student is doing in a class, can you give out that information?

No. Even though the person inquiring may be the student's parent, FERPA recognizes students in secondary education as adults, regardless of age. Therefore, you cannot give out that grade, or any other non-directory information.

General Rule: You must assume that the student is an adult who is entitled to privacy, even from parents. Parents may assert their rights to the records if the student is a dependent according to the tax code.

Can a parent or spouse be given information over the phone concerning the student's tuition charges, account balance, or financial aid?

No Even though the parent or spouse may have paid the tuition, you cannot give out such information. You must assume that the student is an adult who is entitled to privacy, even from parents or his/her spouse. Parents may assert their rights to the records if the student is dependent according to the tax code (appropriate IRS tax information must be provided).

You receive a call from a recruiting firm asking for names and addresses of students with a GPA of 3.0 or better. They say they have good job information for these students. Can you help these students get jobs by giving out this information?

No. Although we all want to help students to get good jobs, that request should be sent to the appropriate office.

General Rule: Do not give out student information that pertains to grade point average to anyone without prior written consent of that student. In this case the request should be forwarded to the Admissions Office. All outside requests for any information such as Dean's List must be referred to the Admission's Office. Information about the recruiting firm could be provided to students in the appropriate major, and to campus Career Services**.**

Can faculty write a letter of recommendation without the student's or former student's authorization?

Yes. But only if the information contained in the recommendation is based on personal knowledge and does not reference information contained in the education record (e.g. grades, schedule, etc.). It is always best to obtain a written release. A good rule of thumb – do not give out student record information to anyone outside the College without prior written consent of the student.

A person goes to the Dean's office with a letter containing a signature that gives consent to release the transcript of a student. Do you give the transcript to them?

No. Transcripts and record information are available only through the Admissions Office.

General Rule: Official transcripts are available only through the Admissions Office. Do not give any records to a third party.

You receive a phone call from the local police department indicating that they are to determine whether a particular student was in attendance on a specific day. Since they are in the middle of an investigation are you allowed to give them this information?

No. The police should be directed to the Dean of Student Services.
General Rule: Information about whether or not a student was enrolled in a particular semester is directory information and can be obtained through the Admissions Office. If the police require more information, a subpoena may be required. Additionally, FERPA requires notification of the student, unless it is specifically stated on the subpoena that the student must not be notified.

You receive a frantic phone call from an individual who says he is a student's father and must get in touch with her immediately because of a family emergency. Can you tell him when and where her next class is today?

No. For the safety of the student you cannot tell another person where a student is at any time. Inform the caller they should contact the Dean of Student Services for more information.

Is it wrong for professors to leave exams, papers, etc., outside their offices for students to pick up?

Yes. That is a violation of the privacy rule because it is inappropriate for students to have access to other students' information.

General Rule: You may not leave personally identifiable materials in a public place.

An unauthorized person retrieves information from a computer screen that was left unattended. Under FERPA, is the institution responsible?

Yes. Information on a computer screen should be treated the same as printed reports.

General Rule: The medium in which the information is held is unimportant. No information should be left accessible or unattended, including computer displays.

You are the faculty advisor of the College's student affiliate of a national service club. The local chapter is required to keep on file, in your office, a current copy of the chapter's financial statements. A reporter from the student newspaper calls and asks you for a copy of the most recent statements. Does FERPA prohibit the disclosure of this information?

No. FERPA only pertains to information that is directly related to a student. The finances of a student organization do not directly relate to a student while other considerations might restrict

sharing this information with the newspaper, FERPA does not. FERPA would prohibit sharing this information if the financial statements became a document used in an investigation into suspected fiscal irregularities by the chapter treasurer.

Does FERPA prohibit the disclosure of the work address and telephone number of an alumnus by the Foundation?

No. FERPA does not protect information about a student that is gathered after the student graduates. Had the request been for the alum's GPA, FERPA would apply.

The campus suffers significant damage from vandals. As a security officer, you investigate the incident and obtain several students' confessions that they committed the acts of vandalism. You share this information with the local police and the Office of Student Services. The Office of Student Services intends to use the information to initiate disciplinary action against the students. Do the students involved have the right to inspect and review the records you have made of their confessions?

Yes. Once the information is shared with the Office of the Student Services, it becomes protected by FERPA and is subject to the right of inspection and review. Had it been shared only with the police, students would not have a right to inspect because FERPA would not apply.

You serve as chair of the nursing program's admissions committee. A first year student who was admitted under special conditions requests the opportunity to review her admissions file. She insists on reviewing these materials no later than the close of business the following day. Does FERPA require you to respond to her request by allowing her to review the records when she wants to?

No. Sauk must grant the request to review within a reasonable time, but in no case more than 45 days after the request is received. It is likely not reasonable to have to respond to a request within 24 hours.

A student's father comes to the Admissions Office and presents a piece of paper signed by the student that states: "I consent to the disclosure of my education records to my father." The paper is signed and dated. The father proves to you that he is the father of the student in question. Does this constitute sufficient written consent under FERPA?

No. This consent does not specify the records to be disclosed, or the purpose of the disclosure. Specific information concerning the records, the name of the person to whom the disclosure is made, and the purpose of the disclosure must be presented in writing.

As Dean of Student Services you learn that a Sauk student is under criminal investigation for selling drugs. The district attorney's office delivers a grand jury subpoena that requests copies of the student's disciplinary records. May you comply with the request without first obtaining the student's consent?

Yes. Prior written consent to disclosure is not required where a subpoena has been issued.

A husband and wife are in your class together. The wife comes to pick up her grade and requests you send home her husband's grade with her, explaining that he is at work. Can you give her his grade?

No. FERPA requires that the student submit written consent to release that information. The consent in this case should be signed by the husband and should specify that the grade for that class should be released to the wife because he could not attend class.

You are a faculty member at Sauk. Your nephew is a student at Sauk, and you promised his mother that you would pull up his grades once they were posted since you have access to Banner. Do you have a right to do so?

No. You have access to information only for legitimate use in completion of your responsibilities as a college employee. The mother may request her son's grades from the Admissions Office if she provides IRS documentation showing that he is her dependent, or the son may submit appropriate written consent to the Admissions Office.