Understanding the Importance of FERPA & Data Protection in Higher Education. An Application: Website at La Salle University

Robert Frank
La Salle University, frank22@hotmail.com

Lynne Wagner
La Salle, wagnerl@lasalle.edu

Follow this and additional works at: https://digitalcommons.lasalle.edu/mathcompcapstones
Part of the Education Law Commons, and the Graphics and Human Computer Interfaces Commons

Recommended Citation
https://digitalcommons.lasalle.edu/mathcompcapstones/36

This Thesis is brought to you for free and open access by the Mathematics and Computer Science, Department of at La Salle University Digital Commons. It has been accepted for inclusion in Mathematics and Computer Science Capstones by an authorized administrator of La Salle University Digital Commons. For more information, please contact careyc@lasalle.edu.
Understanding the Importance of FERPA & Data Protection in Higher Education. An Application: Website at La Salle University

Robert Frank
Lynne Wagner
May 20, 2018
# Table of Contents

**Executive Summary** .................................................................................................................. 3

**FERPA, Privacy, and Information Security in Higher education** ................................................. 4

  Reasons for FERPA ....................................................................................................................... 4

  Student Information Rights ......................................................................................................... 8

  Data Access and Parental Rights ................................................................................................. 11

  Data Responsibilities and Faculty & Staff Guidelines ............................................................ 13

  Information Security to Mitigate Risk ......................................................................................... 15

  FERPA Requirements for Universities ...................................................................................... 17

  New Regulations in Data Protection and Privacy, GDPR ...................................................... 18

  Final Thoughts on FERPA and Privacy .................................................................................... 20

**Application: Website at La Salle University, Philadelphia, PA** .................................................. 22

  FERPA and Data Protection at La Salle University ................................................................. 22

  Current La Salle University Office of the Registrar Website with Students Records Policy ........ 23

  Proposed Changes and Prototype ............................................................................................ 25

    Agile and User Stories .............................................................................................................. 25

    Prototype Creation .................................................................................................................. 27

  Challenges Faced in Development ........................................................................................... 27

  Walkthrough of Website .......................................................................................................... 30

  Home Page ............................................................................................................................... 30
Executive Summary

Personal data protection is a paramount conversation globally. The higher education industry is abundant in varying types of highly sensitive information; the security of this data is critical, requiring all stakeholders be educated and aware of the standards and best practice securing it. This project’s main outcome is to conduct in-depth research on personal data protection regulations within higher education and the development of an example educational webpage for the La Salle University community relating to policy, practice, and procedures of the Family Educational Rights and Privacy Act (FERPA).

The Mission of La Salle University affirms a community commitment to education, stating that “all knowledge is practical and empowering,” (La Salle University Mission and Heritage, n.d.) and thus, our goal is to leverage by this research and develop an educational resource for all of its stakeholders: Students, Parents/Guardians, as well as Faculty & Staff.
FERPA, Privacy, and Information Security in Higher education

Reasons for FERPA

The separation of the United States from the British Empire in 1776 through the Declaration of Independence and Revolutionary War marked a new beginning in the experiment of democracy. The founders of the country realized the difficulties in attempting to legislate a country in a manner that reflects the ideals and freedoms they fought to obtain and at times struggled to adjust its laws to appease all states. In fact, the Constitution of the United States is not the original governing document of the United States. Amidst the Revolutionary War, the majority of states ratified the Articles of Confederation to provide legal direction for a small, albeit centralized, government and these articles were the main governing document tying the states as a single country for nearly a decade. Delegates from the states convened in the 1780s in an attempt to amend the document to better fit the evolving nation, however the representatives deemed it best to start anew. The current Articles of Confederation had become obsolete for the current and future federation of states. Alexander Hamilton’s certainty that the new Constitution fit with the future of the United States was adamant. Hamilton and other founding fathers argued amongst themselves via publications. The resulting Federalist and Anti-Federalist papers acted as the public forum in which the writers argued the pros and cons of the new Constitution. Under the pseudonym Publis, Hamilton published a portion of The Federalist Papers and in the first argues for constitution as upholding the principles of liberty. (Kammen, 1986). His thoughts coupled with those of many other founding members of the United States built the base of a country founded on the concept that privacy and liberty of an individual should be held above all else.
Furthermore, the founders conceived the Constitution to be a living document, fluid to the changes of the times and the will of its citizens. In *Federalist* 44, Hamilton states:

Had the convention attempted a positive enumeration of the powers necessary and proper for carrying their other powers into effect, the attempt would have involved a complete digest of laws on every subject to which the Constitution relates; accommodated too, not only to the existing state of things, but to all the possible changes which futurity may produce… (Madison, n.d.)

In this passage, Madison is arguing that the attempt to categorize and define every law before ratification would be fruitless. He recognizes the inability of the founders to predict a requirement for every law and subsequently defers to the document’s flexibility and ability for amending as a safeguard for permanent ambiguity. Despite the foresight for fluidity, the authors of the Constitution could not have predicted the extraordinary evolution of technology. In a short two hundred years the people of the world saw the change of horse and carriage as a primary means of transportation to cars and planes, correspondence from quill and paper to ball point pens and Xerox copies, and entertainment and communication from news print to radio and television. While each invention brings about new improvements in humans’ daily lives, it is not without some mild disorder. At times newer technologies might be seen as fads, burning out within a few years. The result is trepidation to legislate the new technologies, at times until it is too late. Within the last thirty years, the capabilities of computers have grown near exponentially with the microprocessors in cellular phones evolving to perform some of the same computations and tasks as processors in computers. The increased portability and ease of electronic use resulted in a mass influx of data to electronic storage and with the advent of the internet much of that data became easily accessible from near anywhere in the world. The
The ultimate challenge became making sure that the liberty and privacy of an individual remains sacrosanct as increasing amounts of information accumulated.

The concept that an individual has the innate right to privacy is not a direct result of the dawning of the digital age. An article coauthored by attorneys Samuel Warren and Louis Brandeis titled “The Right to Privacy” is one of the first publication addressing the privacy of an individual. Published in an 1890 issue of the Harvard Law Review, the article takes inspiration from an 1834 ruling by the United States Supreme Court regarding copyrights, Wheaton v. Peters. Subsequent arguments arose stating that privacy was ultimately the catalyst that drove immigrants from Europe to America in the time before the American Revolution. Many historians view the early European legal system as one that was attempting to reduce the rights of the individual. Religious persecution resulted in many Europeans traversing the Atlantic to obtain religious freedom. With only a century or two having passed since their ancestors’ intentional exile; privacy was on the minds of many. Europe began to address concerns with Germany and Sweden passing security laws in 1970 and 1973, respectively. The further rise of technology only exacerbated issues surrounding individual privacy. The United States also began to address the issue but rather than immediately passing legislation, the House of Representatives held a Special Inquiry, or investigation, on privacy. Major legislation governing individual privacy would not appear the Privacy Act of 1974.

The Family Educational Rights and Privacy Act, FERPA, governed by the U.S. Department of Education, came into effect on November 19, 1974 and is known by the moniker The Buckley Amendment. James Buckley, a United States senator from New York, saw growing public concern over the secretive manor in which schools were controlling student information and became a primary sponsor of FERPA. In addressing Congress, he stated:
Many absurd and sometimes tragic examples of similar abuses exist…The parents of a junior high student are told their daughter won’t be able to attend graduation ceremonies because she’s a “bad citizen.” What has she done that’s bad, the parents ask? Well, the principal says, the school had a whole file on her “poor citizenship,” but the parents can’t know what’s in that file. In this Catch-22 case, one of the few to get a legal hearing, the New York State Commissioner of Education, Ewald B. Nyquist, stated flatly that the school’s argument that it was acting in the best interest of the student in refusing to reveal the information to the parents - had no merit. (Stone, 2002)

The senator would later argue that no individual or institution had greater rights to student information than parents. The act is codified within United States Code at 20 USC §1232g and the Code of Federal Regulation at 34 CFR §99. Since its inception in 1974, FERPA required amending to address issues regarding campus safety, campus sex crimes, and student personal well-being. The last FERPA amendment passed in 2001, making it the tenth amendment since its original passing. The enforcement of the act originally rest with the Department of Health, Education, and Welfare (HEW). In 1980, restructuring of HEW resulted in educational duties splitting to its own branch, the Department of Education (DOE). Within DOE, the Family Policy Compliance Office (FPCO) ultimately holds responsibility for FERPA. Initially, FERPA applied to educational institutions who received federal funds, subsequent expansion included federal programs such as Pell Grants and the Guaranteed Student Loan Program. No department of an educational institution is exempt from compliance, including non-educational areas such as Human Resources or Purchasing. Punishment for noncompliance is the loss of eligibility to receive federal funds. The loss however, is not immediate. Following a FPCO investigation, the
agency will work with the institution to reestablish their compliance in the event that a lapse surfaces. In fact, since FERPA’s inception no institution has lost federal funding, largely due to FPCO’s willingness to work in correcting issues rather than punishing for violations.

**Student Information Rights**

As a regulatory act, FERPA’s main charge is to protect student data. The term student, as defined by FERPA, is any individual, minor or adult, who attends an educational institution via any form of correspondence, be it through a satellite, internet connection, videoconference, paper correspondence, or in person. The date of an individual’s classification as a student has the potential to be a few different dates in the individual’s academic tenure but it cannot be any later than the first day of courses. Although the definition of student is clear, there are instances where an individual may find their data at multiple institutions. Individuals younger than eighteen, still attending high school, and enrolled in post-secondary courses have an educational record at both schools. Despite the fact the aforementioned definition of student denotes that any individual enrolled in post-secondary education, such an individual may have no more protections afforded to them than their peers do. A student upon enrollment in a post-secondary educational institution technically owns his/her own educational data, but parents or guardians still have the ability to contact the student’s high school for access to the post-secondary data through an agreed upon data sharing agreement between the secondary and post-secondary institution. A legal aged student enrolled full time in a post-secondary school has more rights to their data and parents or guardians must follow guidelines to access any data the school maintains regarding the student.

Educational institutions collect vast amounts of data on students. Retention policies and regulations require the institutions to maintain their records and make them easily producible.
This results in increased scalability of databases and other forms of digital storage requiring proper security and while these institutions strive to maintain the security of their entire technological infrastructure, there are two types of data an institution may store. There are two types of data an institution may keep on students, educational records and non-educational records, of which the educational record receives more legal protections than its counterpart. Ensuring this data is protected is paramount to maintaining the current and future privacy for individuals. Educational records contain a multitude of data that if compromised, could lead to identity theft and other personal security risks. FERPA views an educational record to be data directly relating to the student’s course work with the university and includes the following: enrollment records, transcripts, personally identifiable information (PII), declarations, petitions, and any information regarding student matriculation within the institution or obtained from other institutions via transfer or other applications. The institution is responsible for protecting this data in any capacity it is stored, whether on premise or in the cloud. Hosting data in the cloud requires an institution to properly vet and audit the vendor offering services. Data sharing contracts and indemnification clauses are often major parts of any cloud agreement. Without the institution’s ability to audit and manage the hardware and infrastructure, the onus falls to the vendor to implement all feasible measures to secure the data. There are times when an educational institution will collect data not considered an education record. Sole possession records, law enforcement records, employment records, medical records, alumni records, and peer-reviewed grades prior to formal instructor submission to the institution are all exceptions to educational records and are not subject to the same scrutiny.

The methods in which regulatory laws handle medical information at an educational institution exist in a slightly ambiguous plane. An educational institution may provide medical
assistance through a variety of means. The institution’s free health clinics and student counseling centers maintain data on prior student visits should he/she require future visits. These records, classified as treatment records under FERPA instead of HIPAA (Health Insurance Portability and Accountability Act) and are only available to the professionals treating the student and the institution can elect not to share said records with the student. (34 CFR §99.10(f)) Specifically outlined in 20 U.S.C. § 1232g(a)(4)(B)(iv):

The term "education records" does not include...records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice. (20 U.S.C. §1232g(a)(4)(B)(iv))

Further implications arise if the student petitions the institution to view these records. If an institution allows the student to view his/her records, the classification of the record changes to an educational record and the same rights and provisions of FERPA govern its protection. While considered a treatment record, not an educational record, data protection standards are still applicable; however the sharing is limited. An institution can choose to share information obtained or not and the ability to share that information is limited. Similar to educational records, the institution has the ability to share the data with a parent or guardian, provided the
institution can verify any required prerequisite information. It also has the power to disclose information to medical or law enforcement personnel if there is a reasonably credible health or safety threat. Regardless of the ultimate classification of the data, the institution maintains the obligation to ensure the security and maintain the integrity of the data. Securing data subsequently protects the privacy of the student.

**Data Access and Parental Rights**

When it comes to data access, there are guidelines an institution must follow for accommodating a request. Any requests to view educational records require a response within 45 days of submission. Furthermore, any reasonable explanation or interpretation of the records by the education institution also require a response. Should circumstances arise where an appropriately submitted request is not receivable, the school will make provisions or arrangements for secure data sharing to the individuals who initiated the request. Additionally, an educational institution cannot levy a charge that would result in the inability to view any record in question but may impose a reasonable fee for any copy made. Although institutions have the ability to destroy records, the law prohibits them from doing so until fulfilling all active relevant requests. There is data pertaining to a student record in a post-secondary institution that the institution can chose not to allow a student to access. FERPA considers financial records containing information about a parent or guardian’s financial status or standing as well as letters of recommendation regarding admission, employment, or scholarship to be inconsequential to a student’s individual educational record. Similarly, if a record about a student contains information on another student, he/she can only view applicable information to himself or herself. Considering the high chance for parental data to exist within a student record and the
potential for student data to interact with other student data, FERPA strives to secure the data and ultimate privacy of all parties associated with an educational record.

The requirement for parental rights pertaining to a post-secondary student’s educational record became apparent shortly before the time of the regulation’s creation. Historically, within the United States, colleges and universities acted *in loco parentis*, or in place of the parents. In the 1960s and 1970s amidst the Civil Rights Movement, university Deans and administrators became less involved and overbearing concerning students. School administrators in prior decades had more of a nurturing, guardian mentality. (Johnsen, 2007) Subsequently, their status of temporary guardian dissolved and returned to the parent. Parental access in a post-secondary environment is possible but has guidelines parents must adhere to following transfer of data rights to the student. There is more than one way a parent or guardian can view a student’s data; primarily, the student can complete and sign a waiver form, designating a person to whom an educational institution may disclose educational records. A parent or guardian will be granted access to their student’s data provided he/she can produce recent and valid tax documentation that claims the student is a dependent. Evidence of court orders, statutes, or other legal documents pertaining to revocation of custody rights will prevent said parent or guardian from access to student educational records. Without a court order or subpoena, the only individuals with permission to view student records, aside from parents or students, are institution officials or officials of a student’s prospective educational institution. While a parent can maintain rights to post-secondary educational records pertaining to their student, there is data an institution is not obligated to disclose. Without consent, an institution has no requirement to inform a parent of disciplinary and health records. Furthermore, regardless of the dependent status of the student, once he/she turns 21 years of age there is no requirement to report violations of federal, state,
local, or institutional laws pertaining to alcohol or controlled substances. Instead, FERPA defers to state or local laws for legal action. FERPA also makes no mention of notification of student academic standing and provides no accommodation.

**Data Responsibilities and Faculty & Staff Guidelines**

The responsibility of securing, managing, and storing the data within the institution is not central to one department but the responsibility of the whole institution. Each department should have a designated primary data owner whose responsibilities include approving access and ensuring the data adheres to any applicable laws or policies. Data owners usually hold a management position within a department, such as a vice president, dean, or department chair but can also include individuals performing statistical analysis such as business intelligence or institutional advancement and effective analytics. Personnel that qualify as data administrators are users from any department with the ability to access or update data. In many instances, a data administrator is an end user or user and while this is usually a faculty or staff member, it can also include students employed by departments. Lastly, there are system administrators whose role is to manage the systems on which the data exists. These individuals are not limited to a purely information technology role and include individuals who can configure applications, databases, networks, or other systems used in accessing data. Setting guidelines for collecting, accessing, and handling data through confidential data and acceptable use policies is crucial in setting an institutional baseline for employees to follow for proper data management. These documents allow an institution to define potentially nebulous terms and specify differences between types of data. Furthermore, the policies empower the institution, giving it options for recourse if employees are found to be in violation, potentially up to dismissal from employment.
During the course of an academic career, students primarily interact with faculty members/professors. The faculty, as adjudicators of student performance, generate large portions of data governed by FERPA. Items such as grades and advising notes require specific conditions for submission, storage, and access. Faculty members should be cognizant as to whom they are sending data as well as what the data is. It is important to be able to de-identify any data that is sent over an unencrypted or non-password protected format. Consider a professor publishing a list of exam grades outside an office or classroom. The list of grades on a spreadsheet corresponds with student ID numbers followed by the student’s grade; students will not know their peer’s ID numbers and may allow them to view grades without any violations. This concept, however, predicates the fact that the institution is keeping the ID numbers private and maintaining the records securely. An educational institution, at the very least, has a single identifying number used to associate students across any necessary table in their primary database. Provided other forms of PII, such as a Social Security number, do not generate the number, it has the potential to allow the association of individuals with their corresponding data anonymously. It does not mean, however that the data can be transferred in an unsecure manner. It also must be understood that the identifiers used in anonymous data association be kept anonymous. In cases where faculty or staff members must share any educational records via electronic transmission or external storage, such as an email or USB driver, respectively, the data or device should be password protected and encrypted or anonymized. Faculty and staff members need constant awareness of their surroundings and should consider peripherals to help secure data such as polarized screen filters.
Information Security to Mitigate Risk

In addition to advocating for the education of its attendants, the faculty and staff at an educational institution are also responsible for helping mitigate risk for any data the institution maintains. Total risk elimination is unfeasible, however, adhering to the regulations and policies set forth by administrative staff will greatly reduce risk. It is important to consider the manner of securing data when its transmission or sharing occurs. Packets transmitted over a network in plain text has the potential for interception by a packet sniffing program as well as reconstruction of those packets, rendering any data transmitted vulnerable. (Cole, W., & R., 2009) It is paramount that data, transmitted in any manner, maintain proper protections. Professors submitting final grades should file them in person with the appropriate institution entity or through an institutional intranet. Professors can utilize an institutional intranet, with a proper and secure configuration, to transmit data on the correct protocol and ports as well as be behind an authenticated log in. Moreover, the module access an employee has needs regular auditing to ensure it reflects his/her job responsibilities. Staff and faculty may transition from one job or department to another and granted new authorizations to systems required for their duties as an employee. The lack of authorization auditing as transfers occur results in permission creep where users accumulate access moving from job to job within the institution. The compromising of a user’s account through phishing or a disgruntled employee might damage a system or database. With proper protocols in place, users should see their permissions adjusted to reflect only their current role.

The first step in any restriction of unauthorized access is identity management, the first step of which is a user’s password. IT personnel can set requirements for credentials to meet in order to meet the proper security standards. The requirements for credentials usually follow a
format consisting of letter case, minimum character counts, symbols, and numbers. Password policy can also govern the use and storage of passwords. The growing number of systems requiring passwords may lead individuals to write passwords on notes under a keyboard or unlocked or secured locations such as a desk drawer. It is important these instances do not occur and users understand proper password security. There are instances where employees required a shared password for a service account or encrypting files that need transmission to other parties. These passwords have guidelines for sharing as well; browser driven password vaults and unprotected spreadsheets are inappropriate methods of distributing passwords. The proper security individuals should discourage the sharing of passwords through email. Additionally, the institution should discourage transmission of an encryption password through the same means of the transmission of its respective encrypted file. The passwords for encrypting these files need to be unique. With the growing amount of digital systems at any institution, there is the desire to use a single password to authenticate for all systems. While a properly managed and secured single sign on authentication system is adequate for protecting an institution from unauthorized access, users must not use their SSO passwords as a means of encrypting documents. Many times, end users will experience technological difficulties, which they are not able to resolve on their own. Institution technology staff may assist an end user to diagnose and resolve or escalate issues to the proper group. These individuals should never ask for a password and end users should immediately be suspect if that occurs. In addition to a strong password policy, dual factor authentication can enable an additional level of security beyond the conventional requirements for passwords. Dual factor authentication requires the use of dongles or apps to provide a code in which a user authenticates with after entering a password.
To ensure proper data protection, institutions also require education and training for faculty and staff. Understandably, individuals interacting with sensitive data should receive information on proper handling and security of the data. However, this cannot be the only information communicated between the institution and its staff. Too often, individuals fall victim to phishing attacks and see login credentials compromised. Phishing, the act of sending fraudulent emails disguised as legitimate communication, has the potential to allow an attacker access to an institution’s systems or obtain other information that would allow social engineering or identity theft. Similarly, faculty and staff must be aware of any web page they visit and items they may download. Some websites display banner ads and not all have innocent intent. A file downloaded by a user could contain malicious code such as a key logger, spyware, crypto-locker, or Trojan. These malicious programs have the potential to steal or hijack data and anti-virus software will not always catch these programs. To help combat and prevent any unfortunate occurrence of phishing, virus, or spyware employees should receive training as part of their institutional onboarding process. Furthermore, individuals who interact with secure data regularly require training in methods of identification and avoidance during regular intervals. The sad reality of technology is that it has use for good and bad. Many times individuals who maliciously exploit programs or other end users are technologically ahead of digital protections in place to combat these threats. Therefore, training for individuals to be able to properly identify and avoid these threats is paramount to maintain security and compliance.

FERPA Requirements for Universities

Institutional staff govern the protection of FERPA data, following its guidelines for data protection and proper release. The staff is also responsible for the notification of and individual’s rights to the community at large. Communication of these rights from the institution
must come at regular annual intervals. The notification needs to include information pertaining
to a student or parent’s right for inspecting and reviewing applicable educational records as well
as the right to amend or petition an amendment to a record. Other rights include consent to
disclose PII and the ability to file complaints or report violations. A request to amend an
educational record does not require the institution to proceed with any change. In an instance
where a ruling results in the rejection of the request, the institution must notify the student or
parent requesting the change and notify him or her about their right to a hearing. FERPA can
grant hearings on an educational record and outlines the following conditions for judging the
hearing: the information contained within the record is inaccurate, misleading, or violates a
student’s privacy rights. Should a record require amending, the institution shall make any
required changes and subsequently inform the applicable party in writing after the change occurs.
The judge for any hearings originates from the institution and must not have any conflict of
interest in the ultimate ruling.

**New Regulations in Data Protection and Privacy, GDPR**

Additional regulations pertaining to data protection have a larger reach than just
education. The European Union passed legislation effective 25 May, 2018 that sets strict
guidelines for any entity collecting data on its citizens. The General Data Protection Regulation
is the newest in a stream of data protection laws originating from the EU and the scope for this
particular regulation goes far beyond the boundaries of Europe. The territorial scope of the
GDPR extends to any company containing data of a citizen of a country belonging to the EU,
even if that company has no European offices. (Conference & Zoladz, 2017) Much of the text
lends itself to protecting the rights of the individual, most notably, the right to be forgotten.
There are obvious guidelines for other access to individual personal data including updating and
portability. The right to be forgotten, however, is a fairly new concept and makes one of its first appearances in legislation in this regulation. The right first gained traction in the mid 2000’s and partially stems from an idea found in the British Rehabilitation of Offenders Act of 1974. This act outlines certain crimes and applies a period of time in which after a conviction the record is not viable nor appears on a background check for the defendant. In the GDPR, an individual can submit a request to any entity to remove any trace of their data from entity servers. Data removal under the desire of being forgotten is becoming more and more popular. The idea of an individual’s right to be forgotten while originating with the absolution of criminal activity, has led to the idea that any individual can have their data removed in totality from internet servers. In a four year span beginning in 2014, Google received over 650,000 requests to remove data pertaining to individuals; that totaled more than two million URLs. (Doubek, 2018)

The regulations in GDPR move far beyond just personal data management. There are regulations surrounding the entire digital experience for companies having operations in European territories. Any end user on a computer has seen the end user license agreement. Further updates to a program with an end user agreement can incur further requirements for acceptance before use of the applicable software. At times, software installations can prepopulate settings such as agreement check boxes, but the GDPR has a provision for ensuring boxes are not pre-checked or agreements are not pre-populated. (Foulsham & Hitchen, 2017) There are also regulations pertaining to notification requirements for data breach or loss. Any incident must be communicated to individuals within 72 hours. Responses to breaches also need to follow a plan approved by an entity’s information security department. This plan must be tested periodically to ensure it is compliant with the regulation.
Final thoughts on FERPA and Privacy

Higher educational institutions provide education for students who ultimately will become the leaders of the next generation. The protection a student’s personal information means he/she can pursue his/her education with confidence and comfort. An institution’s communication to students and parents/guardians regarding the rights to the security of their respective educational record provides an assurance their data will not fall into malicious hands and allows students to concentrate on their studies rather than worry about having their education or identity compromised. The Federal Education Rights Protection Act outlines the guarantees afforded to students and their families throughout their educational careers. Proper communication and education of individual rights and the responsibility of faculty and staff goes beyond the norm of conventional education and every member of an educational institution has the responsibility to protect the individual, the institution, and themselves. Adhering to the guidelines in FERPA, an institution can ensure the continued success of its mission and provide education for current and future students. By following FERPA regulations, providing all afforded protections, and properly educating faculty and staff, educational institutions throughout the United States help to provide a future for students through a combination of protection and education.

The ultimate goal of these regulations is to ensure the privacy of every individual who has data contained within any institution’s bounds. The advancement of an individual’s presence in digital media due to a larger online footprint requires a better plan for prevention and in the event of breaches, action. The growth of student data in the form of electronic education records is staggering. Privacy laws are a paramount to the security of a student. In terms of education, individuals who pledge themselves to an institution require a reasonable level of security and
privacy. Some legislative entities, believe that regulating privacy is the best course of action.

Regardless of an entity’s intent or ultimate action the protection of individuals is most important, especially when considering the security of their data. In conclusion, the privacy and security of individuals, especially in an educational realm, requires proper prevention and response.

Ensuring proper protection of an individual’s information guarantees the respective privacy of each person.

Our team decided to apply these fundamental concepts and security standards to the place that we are associated with as both students and employees; La Salle University. The goal was to create an interactive website that improves on what currently exists at the University. The audience is aimed at three groups: Students, Parents, and Faculty and Staff. The next section of our report details the development of this site.
FERPA and Data Protection at La Salle University

La Salle University is a private, Catholic Liberal Arts College founded in 1863. The college became a coeducational institution in 1970 and achieved its university status in 1984. As of the spring of 2018, the University serves just over 4000 undergraduate students, 1700 graduate students, and 150 Doctoral students. The institution uses Title IV funds under the U.S. Department of Education and is therefore a FERPA mandated organization and has been operating and evolving with the laws of FERPA since its inception in 1974.

The policy and its necessary communications are facilitated by the Office of the University Registrar. In addition to a statement about FERPA listed in both the Undergraduate and Graduate catalogs, information about FERPA and Student’s Right to Privacy can be located on the Office of the University Registrar’s website at www.lasalle.edu/registrar. La Salle University ensures that it is meeting the requirements of FERPA and other related Student Data Privacy laws. University Registrar Jean Landis has access to a multitude of resources on FERPA. “I reference the Family Educational Rights and Privacy Act Regulations found on the Department of Education’s website. As a member of the American Association of Collegiate Registrars and Admissions Officers (AACRAO) I am able to have access to the foremost authority on FERPA—Leroy Rooker. La Salle’s General Counsel also serves as a resource in regards to FERPA.” She informed us that AACROA sends updates and weekly newsletters alerting its members to new information and regulations. She states, “I am also a member of a regional Registrar’s listserv that discusses topics such as FERPA…when at any conference, large or small, I always attend the FERPA session(s). There is always something to brush up on or some new insight on compliance that one can learn.”
The website that exists and the communication plan they have meets the requirements on providing data and access to students about their rights. The research team feels that the site can be expanded upon, however; including more educational information to students and staff members about data privacy and a more automated way of submitting documents and notices to the Office of the Registrar. To do this, the research team has partnered with the Office of the Registrar and the Information Technology department at La Salle University to gain access to developing a site focused on obtaining these goals.

Current La Salle University Office of the Registrar Website with Student Records Policy:
Information about FERPA and the Student Records Policies is embedded into the Registrar’s Website in two pages.

1. **STUDENT RECORDS POLICIES** – This page defines how students will be notified of their annual rights under FERPA. It describes the timelines on how to request inspection of the student record and how to withhold disclosure of their directory information. It also states how to file a complaint to the U.S. Department of Education.

2. **PARENTAL DISCLOSURE** – This page clarifies what the rights are for parents’ access to their child’s confidential information. The way this can occur is when either:
   a. The student completes the University’s “Student Consent to Release Educational Records” form at the Office of the Registrar or have it notarized, or
   b. The parent can prove that the child is claimed on their federal taxes as a dependent.
Proposed changes and Prototype

Agile and User Stories

The goal of the team is to create a more detailed, interactive site that aims to engage three groups: students, parents, and faculty/staff. All of these groups are affected by FERPA. Students and parents need to understand their rights and faculty and staff need to know how to handle student information. There is the need for an educational component for faculty and staff, and that was decided to be a quiz. There is also the need to create a workflow situation for the authorizing of student consent. Lastly, there is a need to expand on data privacy outside of
FERPA for all three parties. The team decided to follow the Agile structure to create the base of the site. This methodology utilizes the concepts of Epic, Features, and User Stories. These details were stored in the professional Project Management Site rallydev.com.

The Epic is the site itself, while the Features are the Content Pages: Data Protection and Privacy, Faculty & Staff, Parent, and Student. The User Stories for each group are below:

<table>
<thead>
<tr>
<th>As a...</th>
<th>I want to...</th>
<th>So that...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student</td>
<td>Access the University Policy</td>
<td>I can understand what my rights are</td>
</tr>
<tr>
<td>Student</td>
<td>Sign in to the portal</td>
<td>I can authenticate that I am a student</td>
</tr>
<tr>
<td>Student</td>
<td>Fill out Student Consent web form</td>
<td>I can submit my consent electronically to the Registrar’s Office</td>
</tr>
<tr>
<td>Student</td>
<td>Fill out Directory web form</td>
<td>I can opt out of being included in Directory Information</td>
</tr>
<tr>
<td>Student</td>
<td>Install Spider Software</td>
<td>I can identify sensitive data on my computer</td>
</tr>
<tr>
<td>Parent</td>
<td>Access parent site</td>
<td>I can view my rights as a parent</td>
</tr>
<tr>
<td>Parent</td>
<td>Download pdf</td>
<td>I can see the student consent form and its requirements</td>
</tr>
<tr>
<td>Parent</td>
<td>Install Spider Software</td>
<td>I can identify sensitive data on my computer</td>
</tr>
<tr>
<td>Faculty/Staff Member</td>
<td>View FERPA definitions</td>
<td>I can understand what is directory versus sensitive data</td>
</tr>
<tr>
<td>Faculty/Staff Member</td>
<td>Install Spider Software</td>
<td>I can identify sensitive data on my computer</td>
</tr>
<tr>
<td>Faculty/Staff Member</td>
<td>View Encryption video</td>
<td>I know how to secure my student information</td>
</tr>
<tr>
<td>Faculty/Staff Member</td>
<td>Take Quiz</td>
<td>I can increase my knowledge</td>
</tr>
</tbody>
</table>
Prototype Creation

A prototype was designed in Microsoft PowerPoint to demonstrate how the separation of student, parent, and faculty/staff page would work.

Challenges Faced in Development

Requirements: WordPress, La Salle University Hosted Site

The initial direction of this project was to design an interactive site for La Salle University that would go live for its users. The Web Design team granted access to the research team in the form of a test administrative panel to develop in WordPress. The site URL can be found here: [http://tst.lasalle.edu/ferpa/](http://tst.lasalle.edu/ferpa/)
WordPress is a software program that offers user-friendly, dynamic themes that allow for people of many technical backgrounds to learn how to develop a site. The back-end coding is PHP and the design can be expanded on using custom HTML and CSS. Without having used WordPress before, we were unaware of the exact nature of the programming and its capabilities. It would eventually be discovered that at baseline, WordPress is very limited in its features and that the software relies on a massive library of open-sourced plugins in order to enhance the design of the user’s site. Although the La Salle Web Design team was very gracious in lending us the use of a test site, they were unable to designate us full rights within the administrative panel to select and install these plug-ins. At first, the Web team was able to offer us a suggestion on a plug-in that supported one facet of our design and they granted us with access to it; but as time in development continued, we realized that we would need access to more of these plug-ins, and the team was unfortunately inundated with their own actual work.

Our team needed to make a decision: do we continue to work in the environment that we have although it is supremely limited in its capabilities, or do we develop on our own? By developing on our own, we had another set of challenges: we could develop limitless on a local environment, or we could use a host. Developing locally would restrict us from sharing our site to anyone and it also would disable the ability to utilize any web form submission for practical use. On the other hand, hosting our site would mean that we could face legal issues using La Salle branding on a site that wasn’t owned by the University. Other realizations about legal consequences began to surface as we became more educated on web design and the WordPress software. For instance, at a WordPress seminar hosted by Philadelphia Girl Develop It in February, Lynne learned that there are website accessibility requirements under the Americans with Disabilities Act for FERPA institutions. The breadth of understanding all of the legal
ramifications and how many sets of approval that this would require from the administration at La Salle University was starting to become apparent. We would need to gain approval from the following, but not limited to: Web team, Registrar, Marketing, IT Security and Compliance, and the University’ s General Counsel. The time constraints we were facing coupled with the goal of the project which was to learn a new technical skill and implement our ideas on FERPA and Data Privacy without limits, helped us ultimately make our decision: develop locally.
Walkthrough of locally hosted La Salle University FERPA and Data Protection Website:

I. **Home Page** – features a header with each main subpage. It contains the marketing video “Explorers are Never Lost” as well as the “Inside Higher Ed” RSS News Feed.

![Header with feature pages](image)

---

**FIND US**

1900 West Olney Avenue
Philadelphia, PA 19141
215.551.1000

![Links to Social Media](image)

Proudly powered by WordPress
II. **Student Page**—describes what FERPA is and how it applies to students. There are links to the Student Records Policy and Student Consent to Release Records as well as the Internet Protection Portal.

La Salle University adheres to the rules of FERPA. A student should understand their rights to privacy under FERPA and can find valuable resources here regarding the law and also on how to protect yourself online.

**FERPA for Students**

FERPA is a Federal law that is administered by the Family Policy Compliance Office (Office) in the U.S. Department of Education (Department). 20 U.S.C. § 1232g; 34 CFR Part 99. FERPA applies to all educational agencies and institutions (e.g., schools) that receive funding under any program administered by the Department.

Once a student reaches 18 years of age or attends a postsecondary institution, he or she becomes an "eligible student" and all rights formerly given to parents under FERPA transfer to the student. Please refer to the La Salle University Student Records Policy for a full description of how the University protects your information.

There is a very in-depth guidance from the Department of Education that provides eligible students with general information about the Family Educational Rights and Privacy Act (FERPA).

a. **Toolips** – this was a custom feature we added to define some of our common terms throughout the website.
b. **Student Records Policy** – a verbatim delivery of the current La Salle University Records Policy

**STUDENT RECORDS POLICY**

**Edit**

La Salle Student Records Policy

La Salle University, in accordance with the Family Educational Rights and Privacy Act (FERPA) of 1974, has adopted the following Student Records Policy. All Students will be notified of their rights under FERPA annually via e-mail. These rights are also included in the University catalog. Revisions and clarifications will be published as warranted. This is our policy:

**RIGHT TO INSPECTION AND REVIEW OF RECORDS**

Any current or previously enrolled student has the right to inspect and review his or her education records within 45 days of the Office of the University Registrar receiving a written request for access. This right does not extend to applicants, those denied admission, or those admitted who do not enroll. The University Registrar’s Office will make arrangements for access and notify the student of the time and place where the records may be inspected. If the requested records are not maintained by the University Registrar’s Office, they will advise the student of the correct official to whom the request should be addressed.

**RIGHT TO AMEND RECORDS**

Students may ask La Salle University to amend a record that they believe is inaccurate. He or she should write the University official responsible for that particular record, clearly identify the part of the record they feel should be changed, and specify why it is inaccurate. If the decision is not to amend the record as requested by the student, the student will be notified and advised 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.

**RIGHT TO CONSENT TO THE DISCLOSURE OF PERSONALLY IDENTIFIABLE**

Student. One exception, which permits disclosure without consent, is disclosure to school officials with legitimate educational interests. A school official is a person employed by La Salle University in an administrative, supervisory, or academic or research, or support staff position (including law enforcement unit personnel and health staff). 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.

A student’s education records shall also be released if properly subpoenaed pursuant to a judicial, legislative, or administrative proceeding. The Office of the University Registrar will make a reasonable attempt to notify the student and allow ten working days, from the date the subpoena was received, for the student to respond.

**DIRECTORY INFORMATION**

Directory information is not considered confidential and includes: name, local, home, and e-mail addresses; local and home telephone number; major field of study; enrollment status (e.g., undergraduate or graduate; full-time, part-time, non-degree); grade level; class; anticipated degree and expected date of degree; degrees, honors, and awards received; participation in officially recognized activities; student ID number; user ID, or other unique personal identifier used by the student for purposes of accessing or communicating in electronic systems; most recent educational agency or institution attended; and photograph.

Under the provisions of the Family Educational Rights and Privacy Act, currently enrolled students may withhold disclosure of directory information.

Complete the **Opt out of Directory Information Form**.

**RIGHT TO FILE A COMPLAINT**

Students who feel that La Salle University is not in compliance with the requirements of the Family Educational Rights and Privacy Act may file complaints with:

Family Policy Compliance Office
U.S. Department of Education
443 Laramie Avenue, SW
Washington, D.C. 20202
c. Student Opt out of Directory Information

OPT OUT OF DIRECTORY INFORMATION

To prevent disclosure, written notification must be received by the Office of the University Registrar by October 15th in the fall semester and February 15th in the spring semester. The University will honor each request to withhold any of the categories of information listed above but cannot assume responsibility to contact a student for subsequent permission to release them. Decisions about withholding any information should be made very carefully. Should a student decide to inform the institution not to release certain information, any future requests for such information from non-institutional persons or organizations will be refused. La Salle University assumes that failure to request the withholding of directory information indicates approval for disclosure.

Please select one or more of the pieces of directory options below to sign opt out of:

- Name
- University ID Number
- Local and Home Address
- Local and Home Telephone Number
- Major/Minor field of Study
- Enrollment Status
- Degrees Awarded
- Participation in University Activities

Other, please explain:

Student First Name:
Lynne

Student Last Name:
Wagner

Student Email:
lynnewagner05@gmail.com

Send
d. Student Consent to Release Records

**STUDENT CONSENT TO RELEASE EDUCATION RECORDS**

In compliance with the Federal Family Education Rights and Privacy Act of 1974, the University is prohibited from providing certain information from your education records to a third party, such as information on grades, billing, tuition, and fees assessments, financial aid (including your grants, scholarships, work-study, or loan amounts) and other student record information. This restriction applies, but is not limited, to your parents, your spouse, or a sponsor.

You may, at your discretion, grant the University permission to release information from your education records to a third party by submitting this completed Student Consent to Release Educational Records authorization. You must complete a separate form for each third party to whom you grant access to your education records. The specified information will be made available only if requested by the authorized third party. The University does not automatically send information to a third party.

If you wish to release records from either Student Health Services or the University Counseling Center, please contact either of those offices to complete and submit a release form for your medical and treatment records.

This completed form will be maintained in the Registrar’s Office, at the address above. Please note that your authorization to release information has no expiration date; however, you may revoke your authorization at any time in writing at the Registrar’s Office. A third party designee must have the student’s ID number when he or she contacts any administrator and may be asked to provide picture ID to authenticate their identity.

The consent form can be completed online:

Complete form [here](#).

You can also complete the paper copy in the Registrar’s Office.
e. **Student Consent web form** – this form prepopulates based on user authentication.

**STUDENT CONSENT FORM**

This completed form will be maintained in the Registrar's Office. Please note that your authorization to release information has no expiration date; however, you may revoke your authorization at any time in writing at the Registrar's Office. A third party designee must have the student's ID number when he or she contacts any administrator and may be asked to provide picture ID to authenticate their identity.

**Student First Name:**
Lynne

**Student Last Name:**
Wagner

**Student Email:**
lynnewagner05@gmail.com

**Telephone Number:**
(555) 000-0000

Please select one or more of the lines below to grant authorization to different types of information:

- [x] Student & Accounts Receivables Office: Billing statements, charges, credits, payments, loan distribution, past due amounts, collection activity, and communication history
- [ ] Registrar's Office/Academic and Learning Support Services/Appropriate Assistant Dean: Grades/GPA, registration, academic progress status, enrollment information, and access to academic records
Please describe the specific types of education records that you wish to release:

Third Party Designee:

Please complete new form for each Designee.

First

Last

Relation to Student

Current Mailing Address Street or P.O. Box Number, Apt. Number, City, State, ZIP Code

Email Address

Certification

I authorize the above third party, named in Section B, to access the above indicated education record. This authorization does not permit the third party to make changes.
f. Submit – the two web forms update the internal WordPress database

i. Opt Out form:

```
inbound message
```

ii. Student Consent

```
inbound message
```
III. Parent Page

What are your rights as a Parent under FERPA?

Is your child under the age of 18?

Is provided with evidence that there is a court order or State law that specifically provides to the contrary. Otherwise, both custodial and noncustodial parents have the right to access their children's education records, the right to seek to have the records amended, the right to consent to disclosure of personally identifiable information from the records (except in certain circumstances specified in the FERPA regulations, some of which are discussed below), and the right to file a complaint with the Department.

Is your child age 18 or older?

When a student reaches 18 years of age or attends a postsecondary institution, he or she becomes an “eligible student,” and all rights under FERPA transfer from the parent to the student.

What can I do?

It is ultimately the decision of your child. At the age of 18, your child is a legal adult with all of the responsibility and agency that comes with it. There are however, ways in which a parent is entitled to accessing confidential records:

- If the knowledge of the information is necessary to protect the health or safety of the student or other students
- The student is under age 21 and has violated any Federal, State, local law or policy concerning the use or possession of alcohol or a controlled substance.
- The student is claimed as a dependent for Federal income tax purposes. Parents claiming a student as a

When a student reaches 18 years of age or attends a postsecondary institution, he or she becomes an “eligible student,” and all rights under FERPA transfer from the parent to the student.

What can I do?

It is ultimately the decision of your child. At the age of 18, your child is a legal adult with all of the responsibility and agency that comes with it. There are however, ways in which a parent is entitled to accessing confidential records:

- If the knowledge of the information is necessary to protect the health or safety of the student or other students
- The student is under age 21 and has violated any Federal, State, local law or policy concerning the use or possession of alcohol or a controlled substance.
- The student is claimed as a dependent for Federal income tax purposes. Parents claiming a student as a dependent must present a copy of their income tax statement claiming the student as a dependent to the University Registrar’s Office, in person or via fax, 215-951-1602.
- The student completes the Student Consent to Release Records Form

For any other questions, please contact the Office of the Registrar at 215-951-1020
IV. Faculty & Staff Page

FERPA for Faculty and Staff

FERPA is the regulatory body in which La Salle University operates. Faculty and Staff are expected to understand the law and act in accordance with it. You can find information on FERPA on the site here: https://www.lasalle.edu/privacy

Acceptable Use and Privacy Policy

Student Records Policy

Please refer to our Student Records Policy to understand what students and their parents have rights to. Students have a right to access most of their information in the system. If a parent contacts you, they need to be referred to the Dean’s Office first. Students need to consent to allow information to be shared with a guardian.

Posting grades/Sending grades to Students

The public posting of grades attached to a student’s name on ID number is a violation of FERPA. Grades should always be entered in the University approved systems: Canvas, Graded First, Bi-LUATUS. Students can access their grades in these ways. Instructors may not email grades. If a student needs a final grade report from their course, they can be directed to the University Registrar.

Letters of Recommendation

Teachers may write letters of recommendation with written consent from the student. No sensitive information should be included in the email (ID numbers, grades, GPA).

Request FERPA Training

FERPA Training for you or your department on FERPA and other data protection measures can be requested from the Office of the University Registrar.

Request Training from the Office of the Registrar

Fields marked with an * are required

Name *

Email *

Message *

I would like to request training on FERPA and other Data Protection resources.

Select Preferred Date

Submit
## a. FERPA Dictionary

### FERPA Dictionary

#### Directory vs. Sensitive Information

This is a list of Data Types that are considered Directory or Sensitive:

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>Description</th>
<th>Directory or Sensitive?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>All names on student record</td>
<td>Directory</td>
</tr>
<tr>
<td>Address</td>
<td>All local and home addresses that are listed as active</td>
<td>Directory</td>
</tr>
<tr>
<td>Phone</td>
<td>Local and Home phones that are listed as active</td>
<td>Directory</td>
</tr>
<tr>
<td>Photograph</td>
<td>Images taken and maintained by the University</td>
<td>Directory</td>
</tr>
<tr>
<td>Major/Minor/Concentrations</td>
<td>All fields of studies</td>
<td>Directory</td>
</tr>
<tr>
<td>Dates of Attendance</td>
<td>Periods of time in which the student attended</td>
<td>Directory</td>
</tr>
<tr>
<td>Enrollment Status</td>
<td>Undergraduate or Graduate, full time or part time</td>
<td>Directory</td>
</tr>
<tr>
<td>Degrees Received</td>
<td>Bachelors, Masters, Doctoral</td>
<td>Directory</td>
</tr>
<tr>
<td>Participation</td>
<td>In University Activities, societies, and events</td>
<td>Directory</td>
</tr>
<tr>
<td>Awards</td>
<td>Honors and Awards earned at the University</td>
<td>Directory</td>
</tr>
<tr>
<td>Place of Birth</td>
<td>City or State of birth as provided by the student</td>
<td>Directory</td>
</tr>
<tr>
<td>Country of Origin</td>
<td>Citizenship as provided by the student</td>
<td>Directory</td>
</tr>
<tr>
<td>Prior Institutions</td>
<td>Any prior degrees earned or attendance at other institutions</td>
<td>Directory</td>
</tr>
</tbody>
</table>

#### Directory

<table>
<thead>
<tr>
<th>Participation</th>
<th>In University Activities, societies, and events</th>
<th>Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awards</td>
<td>Honors and Awards earned at the University</td>
<td>Directory</td>
</tr>
<tr>
<td>Place of Birth</td>
<td>City or State of birth as provided by the student</td>
<td>Directory</td>
</tr>
<tr>
<td>Country of Origin</td>
<td>Citizenship as provided by the student</td>
<td>Directory</td>
</tr>
<tr>
<td>Prior Institutions</td>
<td>Any prior degrees earned or attendance at other institutions</td>
<td>Directory</td>
</tr>
</tbody>
</table>

| Social Security Number | Any SSN's | Sensitive |
| Driver's Licence Number | Any state ID numbers | Sensitive |
| Financial Account Numbers | Credit, Debit, or bank account numbers | Sensitive |
| International Numbers | Passport or Alien ID numbers | Sensitive |
| Grades/Transcripts    | Any form that lists a single or multiple grade for a student | Sensitive |
| Advising              | Any student advising record                    | Sensitive |
| Financial Aid         | Any list of loans, grants or scholarships      | Sensitive |
| Admissions            | Any recruiting information including high school gpas and SAT or other test scores | Sensitive |
| Health Information    | Any HIPAA related                              | Sensitive |
b. FERPA Quiz

Take this quiz to test your knowledge on FERPA.

You Scored 2/5 or 40%
I'm sorry but you did not achieve the required score.

SHARE YOUR RESULTS

Question #1: What does FERPA stand for?
- Federal Education Regulated Protection Act
- Family Educational Rights and Privacy Act
- First Education Regulated Privacy Amendment
- Federal Education Required Privacy Act

Question #2: Who is covered under FERPA?
- Any student who has been in attendance at a post-secondary institution
- Any student who has been in attendance at any kind of educational facility in the United States.
- Only students who have been in attendance at a post-secondary institution

Question #3: If an official comes to the College of Business with a signed document from the student that gives consent to release student grades and/or transcript, do you give that information to them?
- Yes
- No

All requests for student grade reports and transcripts are issued by the Office of the Registrar.

Question #4: You receive a call from your student's parent requesting to talk about her progress in your course. The parent status that the student has allowed them to discuss this information with their professors. What should you do?
- Contact the Registrar's Office to confirm that the student has in fact designated this parent to discuss their academic information with you.

Incorrectly answered questions are noted and an explanation to the correct answer is given.

Visit the Internet Protection Portal for information for Students, Parents, and Faculty & Staff to learn of different ways you can protect yourself and your data online.

SEARCH THE SITE:
Search...
Question #4: You receive a call from your student's parent requesting to talk about her progress in your course. The parent states that the student has allowed them to discuss this information with their professors. What should you do?

- Contact the Registrar's Office to confirm that the student has in fact designated the parent to discuss their academic information with you.
- Contact the student to confirm that they have in fact designated their parent to discuss their academic information with you.
- Discuss the academic information with the parent since that is not considered sensitive information under the laws of FERPA.
- Refer the parent to the Dean's Office; the student majors under where they will confirm that the student has in fact designated the parent to discuss their academic information, and they will coordinate the discussion between the parent.

There are four areas in which a student can allow a parent to have access to. Regarding academic information, the option regarding academic progress status; Registrar’s Office / Academic and Learning Support Services/Appropriate Assistant Dean; Registrar/IBPA registration, academic progress status, enrollment information, and access to academic records. Since the parent is inquiring on the student's progress in your course, they need to speak with the Dean's Office first.

Question #5: Directory Information is not considered confidential, and the University may decide to release this information without written permission from the student. All of the examples below are considered Directory Information except:

- Student local and home address, telephone numbers, and email addresses.
- Detailed student schedule by term including dates and instructors.
- Student degrees earned and dates they were conferred.
- Student enrollment status, i.e. Undergraduate versus Graduate, and Full-Time versus Part-Time.

Finish
V. Data Protection Portal

Here is the Link to the Encryption Video we created in the La Salle Instructional Recording Studio: Encrypt document containing sensitive data
a. Educause – the page opens into a new tab

b. SafeConnect
c. Spider Software Download

Visit Columbia University for their complimentary download of Spider Software:

CU Spider is an open-source forensic file scanning program that scans workstations for Social Security Numbers (SSN) and other Personally Identifiable Information (PII). According to Columbia University Policy, SSNs and other sensitive PII (as defined by the CU Data Classification Policy) should not be left unencrypted on workstation drives. You can use this tool, which is already installed on a large number of CU staff workstations, to locate and then remediate any SSN/PII you find.

CU Spider scans your computer, produces a list of files which appear to contain SSN information, and provides options for you to take immediate actions for remediation, including secure deletion, and redaction.

CU Spider is a modification and repackaging of Spider 2008 version 4.0.2 (Larotopex), an open-source program PII-scanning program developed by Cornell University and Wyman Miles (see below for a list of modifications and changes), and released under the GNU General Public License v2.

Clicking the Spider Link takes you to the Download Site of Columbia University.
Conclusion

The research performed during the course of this project enlightened us to challenges many educational institutions encounter. The road-blocks faced along the way forced us to reevaluate and adjust the project to ensure the outcome issued by the Executive Summary would be fulfilled. In meeting these challenges, we found ourselves enlightened with a new skillset or knowledge applicable to our professional lives. The resources and information pertaining to FERPA, privacy, and data security are extensive and can overwhelm individuals not familiar with them. Translating the convoluted legal terminologies and applying all the information in a practical application required in depth research into the end user experience, with which neither of us had any expertise. This was an opportunity to expand our professional skillset and
provides us with a new perspective in providing accurate and quality training to members of a university. Knowing the challenges students, parents, and educators face allows us to communicate with all parties better, especially in areas where each party may not have a great understanding.
References


Stone, K. J. (2002). Revisiting the Purpose and Effect of FERPA. Stetson University College of Law.

https://www2.ed.gov/policy/gen/guid/fpco/hottopics/ht12-17-08.html