EDUCATIONAL DATA GOVERNANCE

MANAGING YOUR DATA PROGRAM WITH COMPLIANCE

GOTOCOLLEGEFAIRS.com

Streamlining the College Fair Experience

INTRODUCTION

We live in a world full of data. Everything from our name and age to our food preferences is stored in a vault or a cloud, on a server somewhere, waiting to be retrieved and pinged across the globe to allow us to sign in to our email account or enable a cruise line to target us for a vacation advertisement.

Of course, agencies tasked with collecting this data are also expected to correctly store and manage access to it, but as the quantity of data has grown, this process has become increasingly challenging. One set of data that has grown exponentially over the years—to the point where the government has had to step in and create a policy for managing and protecting the data—is education records.

This white paper offers a "crash course" for educational institutions working to develop a sound data governance program. From how education records came into being, to what laws and policies have informed best practices, to the ten core components of a successful program, this whitepaper provides a blueprint to help you manage your data program with compliance.

Let's start by defining "Education Record."

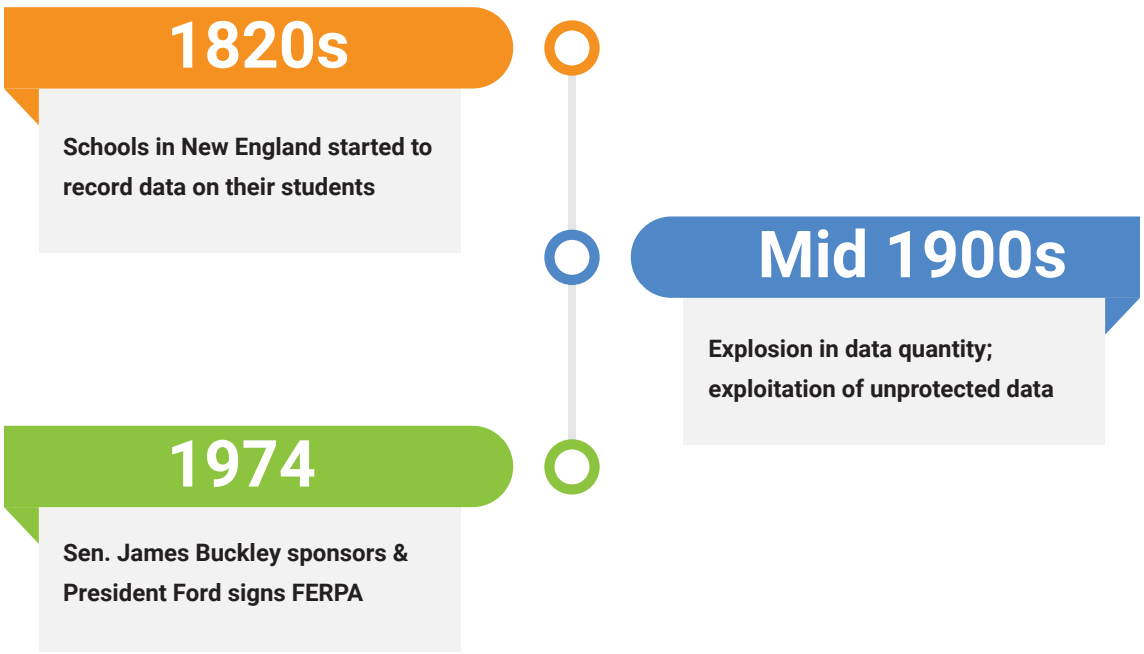
The term "education record" is defined as those records that are: (1) directly related to a student, and (2) maintained by an educational agency or institution (or by a party acting for the agency or institution). Because this definition is so broad, it's actually easier to say what an education record is not.

An education record is not:

- Legal records maintained by a law enforcement unit
- Medical records
- Employment information, unless employment is contingent upon being a student (e.g., work–study)
- Information obtained after leaving the institution (e.g., alumni records)

A HISTORY OF EDUCATION RECORDS

Education records started back in the 1820s, when schools in New England started to record data on their students. By the mid 1900s, those records had grown to monstrous proportions with little regulation. School officials could add nearly any comment or anecdote to a student's record at will, no matter how slanderous or damaging, and often without the student's knowledge. There was no process to have these judgments challenged or removed. Parents could be denied access to their student's records without explanation, while other third parties were given access with almost no questions asked. Finally, in 1974, FERPA was drafted and signed into law by President Gerald Ford in order to address these issues of privacy of and access to education records.



WHAT IS FERPA?

FERPA stands for the Family Education Rights and Privacy Act. It was signed into law in 1974 to protect the privacy of students' education records, an issue that was deemed important in order to protect students from discrimination, identity theft, or other malicious or damaging criminal acts. Under this law, federally funded education institutions are required to comply with certain procedures for maintaining and disclosing educational records.

WHAT INFORMATION WITHIN AN EDUCATION RECORD IS PROTECTED?

Educational information, including student transcript, GPA, grades, SSN, academic evaluations (but not peer grading), attendance records, special education records, school disciplinary records (see exceptions below), and some psychological evaluations.

Personally identifiable information can only be disclosed if the educational institution obtains the parent's or student's signature (if over 18 years of age) on a document that specifically identifies (a) the information to be disclosed, (b) the reason for disclosure, and (c) the parties to whom the disclosure will be made.

Directory information is not protected. Directory information is information contained in a student's education record that, if disclosed, would not generally be considered harmful or an invasion of privacy (e.g., student ID number, name, address, telephone number). Public notice must be given regarding the type of information to be disclosed, and every student must have the right, within a given period of time, to forbid disclosure.

Gray area includes reference letters and resumes. If these include a student's educational information (e.g., GPA, grades, etc.), then they are treated as educational or personally identifiable information

2 Other Laws That Affect Information Privacy in Schools

National School Lunch Act:

Administered by the USDA, this Act limits how school districts may use individual student and household information, which is obtained as part of the eligibility process; neither eligibility nor program ID information may be incorporated into a student's education record

Federal Drug and Alcohol Patient Records Confidentiality Law:

Administered by the USD HHS; states that information about assessment, diagnosis, counseling, treatment, or referral may not be disclosed without the patient's consent, including students who are minors

Exceptions are made for certain emergencies (i.e., if there is an articulable and significant threat to the health and safety of a student or other individuals) and registered sex offenders. Also subject to exception is disclosure of results of any disciplinary proceeding, by the institution, against a student who is alleged to have committed a crime of violence or a sex offense, to the alleged victim. Information that has been made anonymous (from which all personally identifiable information has been removed) may also be disclosed. Records must be kept of all such disclosures

Recommendations for Communicating with Students

- Annually advise students on their rights under FERPA
- Prior to disclosure, inform students as to what information will be considered directory information (and give them a reasonable time to forbid disclosure, or "opt out")
- Advise students regarding the implications of waiving their right to inspect their files or letters of recommendation

PRIVACY TECHNICAL ASSISTANCE CENTER (PTAC)

To assist institutions in complying with FERPA, the government founded PTAC: The Privacy Technical Assistance Center. This "center," or online collection of resources overseen by the federal Privacy Advisory Committee, provides educational agencies and institutions with guidelines and training to develop a data governance program that ensures the privacy, confidentiality, and security of students' data from preschool through postsecondary education and into the workforce.

At its essence, a data governance program is a set of rules and procedures that determine how data should be treated from the time it is acquired (when you fill out a form, register for an account, etc.), through its use (you use your email to log on to an online account, one company sells another company their mailing list, etc.), and culminating with its disposal (your record is deleted, your account is deactivated, etc.).

The benefits of developing a strong data governance program are fourfold. The data will be more accurate (meaning that it is thorough and reflects reality). It will be more usable (better organized, more easily accessed). It will be timelier (available without delay). And finally—arguably most importantly—it will be more secure.

According to PTAC, there are four key steps to creating and maintaining a good data governance program. These "steps" are best framed as questions:

1. Who will be responsible for the program and for making decisions about its governance?
2. What are the rules and methods for managing the data?
3. How will these rules and methods be implemented?
4. Is the program (a) doing what it is meant to do, and (b) being followed by all stakeholders?

If you are able to adequately answer each of these questions, then your organization probably has a solid data governance program already in place. If not, PTAC provides a guide to the 10 components that you should follow to develop a comprehensive data governance program. These components are grouped into three overarching "themes": (a) rules of engagement, (b) organizational bodies and individuals, and (c) data governance processes.

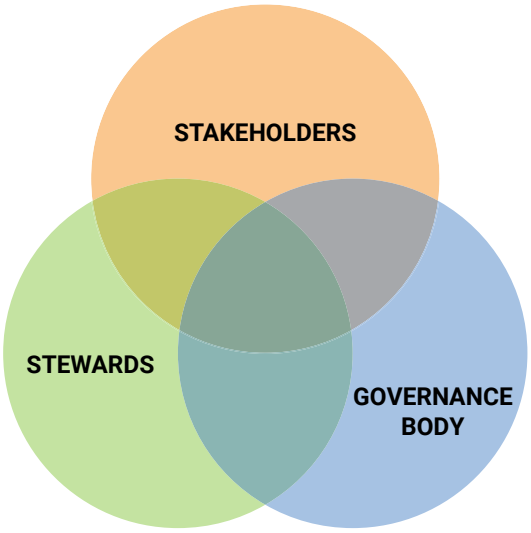
A. Rules of Engagement

First and foremost, a data governance program needs to fit with what the organization, as a whole, is trying to achieve. Likewise, it also needs to fall in line with what stakeholders expect from the organization. Finally, it must be reasonable—that is, the organization must have the resources necessary to put such a program in place, and to then sustain it. Therefore, here are PTAC's six primary "rules of engagement":

1. **Mission and vision** – what is the organization's overall mission/vision, and how do the expectations of data governance play into that?
2. **Goals**, governance metrics, success measures, and funding strategies – what are the goals of the data governance program, how will they be tracked and measured, and how will the program be financially supported?
3. **Data rules and definitions** – what data is being collected, and how will different types of data (e.g., personally identifying data vs. anonymous data) be treated differently?
4. **Decision rights** – who is permitted to make a decision about what is done with the data?
5. **Responsibilities and enforcement and compliance mechanisms** – who is responsible for the implementation and success of the program, and how will its rules be enforced?
6. **Security controls for risk management** – what happens in the case of a data breach or data mismanagement?

B. Organizational bodies and individuals

Next, a data governance program must address who is "in charge"—i.e., who is responsible for making sure the program is implemented efficiently and effectively—as well as the rights and responsibilities of other involved parties. These individuals are:



7. **Data stakeholders** – these include data owners and users, and their rights and/or responsibilities should be spelled out
8. **A data governance body** – this committee should include management and legal representatives, along with data system administrators, data providers, data managers, privacy/security experts, and data users
9. **Data stewards** – these are individuals who possess specific roles and responsibilities within the data governance program

C. Data governance processes

The final, tenth piece of the data governance program is a set of procedures for implementing and modifying the program. These procedures should specify a number of "how to's": how to implement the program, how to manage data over the long term, how to judge the program's success, and how to handle cases when data quality or security is jeopardized. These "how to's" fall into three main categories: proactive (setting standards prior to collecting any data), reactive (correcting any security policies in response to a data breach), and ongoing maintenance (regular operating procedures to keep the program intact and functioning smoothly).

If you work to incorporate these ten components into your data governance program, you will end up with a secure system that presents you with more accurate, timely, usable data.

Additional resources
The full PTAC guide: http://ptac.ed.gov/toolkit

National Center for Education Statistics technical briefs:
https://nces.ed.gov/programs/ptac/Toolkit.aspx?section=Technical%20Briefs

USDOE Family Compliance Office website:
https://www2.ed.gov/policy/gen/guid/fpco/index.html

USDOE Protecting Student Privacy – Data Governance resources:
https://studentprivacy.ed.gov/content/data-governance