

# DATA ETHICS

National  
Forum  
on Education  
Statistics



THE FORUM GUIDE TO

# DATA ETHICS





## National Cooperative Education Statistics System

The National Center for Education Statistics (NCES) established the National Cooperative Education Statistics System (Cooperative System) to assist in producing and maintaining comparable and uniform information and data on early childhood education, and on elementary and secondary education. These data are intended to be useful for policymaking at the federal, state, and local levels.

The National Forum on Education Statistics (the Forum), is an entity of the Cooperative System and, among its other activities, proposes principles of good practice to assist state and local education agencies in meeting this purpose. The Cooperative System and the Forum are supported in these endeavors by resources from NCES.

Publications of the Forum do not undergo the same formal review required for products of NCES. The information and opinions published here are those of the Forum and do not necessarily represent the policy or views of the U.S. Department of Education or NCES.

### February 2010

This publication and other publications of the National Forum on Education Statistics may be found at the websites listed below.

The NCES World Wide Web Home Page is <http://nces.ed.gov>

The NCES World Wide Web Electronic Catalog is <http://nces.ed.gov/pubsearch>

The Forum World Wide Web Home Page is <http://nces.ed.gov/forum>

### Suggested Citation

National Forum on Education Statistics. (2010). Forum Guide to Data Ethics (NFES 2010–801). U.S. Department of Education. Washington, DC: National Center for Education Statistics.

### For ordering information on this report, write:

U.S. Department of Education  
ED Pubs  
P.O. Box 1398  
Jessup, MD 20794–1398

Or call toll free 1–877–4ED–PUBS or order online at <http://www.edpubs.org>

### Technical Contact

Stephen Q. Cornman  
(202) 502–7338  
[stephen.cornman@ed.gov](mailto:stephen.cornman@ed.gov)

# TASK FORCE MEMBERS

This guide was developed through the National Cooperative Education Statistics System and funded by the National Center for Education Statistics (NCES) of the U.S. Department of Education. A volunteer task force of the National Forum on Education Statistics produced this document.

## Chair

**Tom Purwin**

Jersey City Public Schools, New Jersey

## Task Force Members

**Cheryl McMurtrey**

Mountain Home School District 193, Idaho

**Lee Rabbit**

Newport Public Schools, Rhode Island

**Stephen Metcalf**

Montpelier School District, Vermont

**David Uhlig**

Charlottesville City Public Schools, Virginia

**Janice Petro**

Colorado Department of Education

## Consultant

**Tom Szuba**

Quality Information Partners

## Project Officer

**Stephen Q. Cornman**

National Center for Education Statistics

# ACKNOWLEDGMENTS

The members of the Data Ethics Task Force of the National Forum on Education Statistics would like to thank everyone who reviewed drafts of this document or otherwise contributed to its development. This includes the Forum Steering Committee and Technology (TECH) Committee, and members of the National Forum on Education Statistics.

# FOREWORD

The National Forum on Education Statistics (the Forum) is pleased to present this *Forum Guide to Data Ethics*. One goal of the Forum is to improve the quality of education data gathered for use by policymakers and program decisionmakers. An approach to furthering this goal has been to pool the collective experiences of Forum members to produce “best practice” guides in areas of high interest to those who collect, maintain, and use data about elementary and secondary education. The ethical use and management of education data is one of those high interest areas.

Each and every day, educators collect and use data about students, staff, and schools. Some of these data originate in individual student and staff records that are confidential or otherwise sensitive. And even those data that are a matter of public record, such as aggregate school enrollment, need to be accessed, presented, and used in an ethically responsible manner. While laws set the legal parameters that govern data use, ethics establish fundamental principles of “right and wrong” that are critical to the appropriate management and use of education data in the technology age. This guide reflects the experience and judgment of experienced data managers; while there is no mandate to follow these principles, the authors hope that the contents will prove a useful reference to others in their work.

## In This Guide

- Part I introduces the concept of data ethics in the field of education and describes the document’s purpose, intended audience, and layout and design conventions.
- Part II presents the Forum Code of Data Ethics through real-world examples (vignettes) and explanatory text (discussion).
- Appendix A lists other publications from the Forum that may be useful to school, district, or state education agency staff who are considering data ethics issues.
- Appendix B provides a sample “whistleblower” policy as adapted from a document developed by a local education agency.
- Appendix C explains how memoranda of understanding and acceptable use statements can be valuable tools for describing and enforcing data usage agreements between two or more parties—and are often used to formally agree to behavioral practices.
- Appendix D provides a summary of the federal Family Educational Rights and Privacy Act (FERPA).



## The National Cooperative Education Statistics System

The work of the Forum is a key aspect of the National Cooperative Education Statistics System (Cooperative System). The Cooperative System was established to produce and maintain, with the cooperation of the states, comparable and uniform educational information and data that are useful for policymaking at the federal, state, and local levels. To assist in meeting this goal, the National Center for Education Statistics (NCES), within the U.S. Department of Education, established the National Forum on Education Statistics (the Forum) to improve the collection, reporting, and use of elementary and secondary education statistics. The Forum deals with issues in education data policy, sponsors innovations in data collection and reporting, and provides technical assistance to improve state and local data systems.

## Development of Forum Products

Members of the Forum establish task forces to develop best-practice guides in data-related areas of interest to federal, state, and local education agencies. NCES provides management oversight of this work, but the content comes from the collective experience of the state and school district task force members who review all products iteratively throughout the development process. Documents prepared, reviewed, and approved by task force members undergo a formal public review. This public review consists of focus groups with representatives of the product's intended audience, review sessions at relevant regional or national conferences, or technical reviews by acknowledged experts in the field. In addition, all draft documents are posted on the Forum website prior to publication so that any interested individuals or organizations can provide feedback. After the task force oversees the integration of public review comments and reviews the document a final time, publications are subject to examination by members of the Forum standing committee sponsoring the project. Finally, the entire Forum (approximately 120 members) reviews and formally votes to approve all documents prior to publication.

# TABLE OF CONTENTS

Task Force Members .....	iii
Acknowledgments .....	iii
Foreword .....	iv
<b>Part I: Introduction to Data Ethics</b> .....	1
<b>Part II: The Forum Code of Data Ethics</b> .....	7
<b>The Integrity Canons</b> .....	8
Canon 1. Demonstrate honesty, integrity, and professionalism at all times .....	8
Canon 2. Appreciate that, while data may represent attributes of real people, they do not describe the whole person .....	11
Canon 3. Be aware of applicable statutes, regulations, practices, and ethical standards governing data collection and reporting .....	13
Canon 4. Report information accurately and without bias .....	15
Canon 5. Be accountable, and hold others accountable, for ethical use of data .....	18
<b>The Data Quality Canons</b> .....	20
Canon 6. Promote data quality by adhering to best practices and operating standards .....	20
Canon 7. Provide all relevant data, definitions, and documentation to promote comprehensive understanding and accurate analysis when releasing information .....	23
<b>The Security Canons</b> .....	25
Canon 8. Treat data systems as valuable organizational assets .....	25
Canon 9. Safeguard sensitive data to guarantee privacy and confidentiality .....	28
<b>Appendices</b> .....	31
Appendix A: Related Resources .....	31
Appendix B: Sample Whistleblower Protection Policy .....	35
Appendix C: Memoranda of Understanding and Other Data Use Agreements .....	39
Appendix D: Family Educational Rights and Privacy Act (FERPA) .....	41

# DATA ETHICS

- Ethics:**
1. A set of principles of proper conduct.
  2. The rules or standards governing the conduct of a person or the members of a profession.

Ethics have always been important, but they rarely get much attention until someone behaves in an unethical manner. Business ethics become headline news when financiers put their own personal interests ahead of their clients' financial well-being. Sports ethics arouse public debate when an athlete is accused of steroid use, cheating, or gambling.

Ethics are especially relevant in the public sector. Political leaders, courts, government employees, and schools are—justifiably—expected to conduct business in a manner that efficiently and effectively uses public resources, while at the same time guaranteeing our rights as citizens. In other words, they are expected to perform their responsibilities in an ethical manner.

Ethics are manifested in many ways in an education organization. Principals are obliged to treat each child fairly; teachers are bound to create a classroom atmosphere conducive to learning; cafeteria workers are responsible for protecting the identity of children receiving free- or reduced-price meals; board members are charged to help schools function in accordance with laws, standards, norms, and best practices in the field; and administrators are obligated to ensure that school resources are used as they were intended without mismanagement, fraud, or abuse.

Each and every day, educators collect and use data about students, staff, and schools. Some of these data originate in individual student or staff records that are confidential or otherwise sensitive. And, even information that is a matter of public record (aggregate school enrollment, for example) needs to be accessed, presented, and used in a responsible manner.

**While laws may set the legal parameters that govern data use, ethics establish the fundamental principles of “right and wrong” that are critical to the appropriate management and use of education data.**

An education organization should ensure that all data handlers understand and adhere to ethical standards related to their responsibilities in the organization.

“Ethics” include appropriate behavior and appropriate expertise. For example, it is unethical to disclose private information about a staff member (inappropriate behavior), and it is unethical to hire a data manager who does not understand individual privacy rights (inappropriate expertise).

The exponential growth of information systems that provide ready access to education data—often drawing upon individual student records—has heightened the importance of training data users about their ethical responsibilities regarding how they appropriately access, use, share, and manage education data. Technology makes data readily available to many staff members in an education organization. While improved access helps staff perform their jobs more effectively, it also raises issues about the appropriate use of data because the power to transmit information electronically multiplies the consequences of irresponsible behavior. How much more vulnerable are we to the inappropriate disclosure of information (for example, a student’s assessment results, grades, medical history) in the age of downloads, copy and paste, and web posting than we were when cumulative folders could be locked away in a file cabinet? How much easier is it now to create a technically accurate but misleading presentation to policymakers or the public (for example, manipulating the axes on graphs to give the wrong impression about data trends)? Laws may set the legal parameters in which data users operate, but ethics go deeper and are often more stringent—after all, it is usually not illegal to change the axis on a graph, but it is unethical to intentionally represent data in a manner that is likely to be misunderstood.

## Purpose of This Guide

A February 2010 web search of the phrase “data ethics” yielded 103,000 results (<http://www.google.com>)—clearly too many choices for anyone seeking practical guidance about behavior in the education data community. Education organizations need a simple, comprehensive set of standards for establishing plans that encourage the ethical use and management of data.

In response to this need, this document presents a code of ethics for data management and use in education settings. All core principles (called “canons”), examples, descriptions, and recommendations in this document reflect situations that arise in real schools, school districts, and state education agencies. The best practices presented in part II are intended to supplement existing policies in education organizations, or serve as a template when organizations create new policies.

*The Forum Guide to Data Ethics* is written for a broad range of stakeholders in the education data community. It addresses ethical issues related to the management and use of education data. The Code of Ethics is presented in a format that encourages discussion and, hopefully, adoption by schools, school districts, and state education agencies. While formal and systematic training is necessary to fully implement the recommendations in this guide, the goal of this document is to make ethical principles understandable and actionable to education staff as they work with data in their organizations.

## The Challenge to Leadership

Although the world is full of good people, ethical behavior does not just happen automatically in an organization. Education is a complex endeavor. While most people see schools as the setting for teaching and learning, others view schools as political entities, or business opportunities, or agents of social change. Each perspective is likely to carry its own biases. And when an individual’s interest is at stake, people may be tempted to engage in unethical behavior—to knowingly manipulate or misrepresent statistics to make a point; misuse data for personal gain; or convince themselves that privacy and confidentiality requirements don’t need to be observed.

Collecting, maintaining, reporting, and using data in an appropriate manner that



is consistent throughout the organization, and in all decisions, will not happen unless education leaders support data ethics as an important organizational priority. School leaders can set expectations that make ethical behavior an organizational norm or, alternatively, they can accept or even encourage behavior that routinely falls short of high standards. Ethical behavior oftentimes can be encouraged through organizational structures and operational expectations. For example, a responsible system of checks and balances precludes finance officers from signing their own expense reports without anyone else's oversight. By establishing standard procedures for collecting data, generating and reviewing reports, releasing publications, and communicating with the public, an education organization limits the opportunities for inappropriate behavior.

Establishing organizational structures and practices that encourage ethical conduct is not enough. Organizations must actively ensure that all data handlers adhere to all policies and procedures related to data ethics. Good communication throughout the organization and effective training can go a long way to foster this culture. To help data handlers understand and exhibit standards of ethical behavior, education organizations should

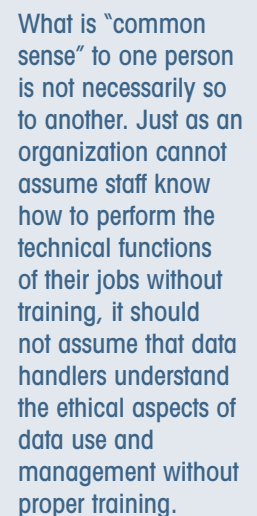
- train staff about their ethical responsibilities;
- publicize the expectations for ethical behavior;
- create explicit policies and procedures pertaining to data ethics;
- state clearly the consequences of unethical behavior; and
- enforce these rules uniformly so that everyone is accountable.

Ethics training requires a resource commitment from school leaders: securing skilled trainers, tailoring curricula to the organization's and learners' needs, and allocating professional development time for staff to learn and practice new behaviors. In addition to describing ethical concepts, training should discuss why ethics matter (ethical issues are real and have significant consequences) and how ethics play out in everyday situations in the organization (that is, how they affect the routine activities of the training participants). Realistic examples customized to the learners' roles and responsibilities are a good way to communicate the real-life implications – and unexpected complexities – of the principles in the guide.

## Code of Data Ethics Audience

The responsibility for data ethics ultimately rests with an organization's leadership. Nonetheless, appropriate ethical behavior in accessing, using, and managing education data is the responsibility of each and every individual with access to information in an education organization. This includes, but is not limited to, your organization's

- ▶ superintendent;
- ▶ chief information officer;
- ▶ principal(s);
- ▶ teachers;
- ▶ registrar(s);
- ▶ counselor(s);
- ▶ school board members;
- ▶ data manager;
- ▶ technology director;
- ▶ information systems staff;
- ▶ data steward(s);
- ▶ technical staff;
- ▶ office staff;



What is “common sense” to one person is not necessarily so to another. Just as an organization cannot assume staff know how to perform the technical functions of their jobs without training, it should not assume that data handlers understand the ethical aspects of data use and management without proper training.

- ▶ paraprofessionals;
- ▶ volunteers; and
- ▶ vendors.

## Layout and Conventions

Each ethical canon in this document is presented in the following manner:

**CATEGORY:** A broad classification used to organize the canons in this document. The categories (personal/professional integrity, data quality, and security) can be thought of as the overarching drivers of ethical behavior. These categories are used to organize the document’s content, and there is overlap across categories.

**CANON:** The core ethical principle being presented and discussed.

**Vignette:** An example that illustrates how an ethical canon is relevant to the real world. These fictional examples cite various settings and circumstances related to data handlers because this group has been identified as the *Guide’s* primary audience.

**Discussion:** An explanation of the canon that provides context for understanding the ethical principles being addressed.

**Recommended Practices and Training:** A bulleted list of activities and tasks that would contribute to achieving the ethical principles represented by the canon. The lists of recommended practices are illustrative rather than exhaustive, and they are intended to represent some of the most fundamental activities that can be undertaken to advance a canon.

## Terms You Will See in This Guide

Some terms that are used interchangeably in conversation have very specific, and distinctive, meanings as they are used in these Canons.

**Personally Identifiable Information:** Data that can be used to identify a person, or that can be used in conjunction with other information (e.g., by linking records) to identify a person. This includes a student’s name; the name of the student’s parent or other family member; the address of the student; a personal identifier, such as the social security number or student number; a list of personal characteristics that would make the student’s identity traceable; or any other information that would make the student’s identity traceable.

**Private Information:** Data that are classified as uniquely personal and, therefore, neither available for public release nor accessible without a verified “need to know” for the purposes of providing approved educational services. Private information in a school record often includes course selection, academic performance, aptitude scores, health information, and discipline data.

Even relatively minor ethical mistakes in an education organization can become high profile public events—something that schools, districts, and state education agencies should try to avoid.

**Confidential Information:** Data that have been guaranteed to be maintained confidentially (i.e., that will not be released), regardless of their nature (as private or sensitive).

**Sensitive Information:** Those data that are confidential and/or vital to an organization as it carries out its mission. For example, data about class assignments are both confidential (data about student course selection are private) and vital to the school’s core instructional mission (principals should know where students need to be at every moment of the day).

**General Information:** Those data that are generally helpful, but not confidential and/or vital, to an organization as it carries out its mission. For example, a data file with “help” instructions for website users is a “general” support component within a data system. While the files are important to users facing a web problem, the data are not vital to running a school or school system; nor are they private in nature or otherwise subject to confidentiality restrictions.





The following key principles of ethical conduct related to education data were identified by the Data Ethics Task Force of the National Forum on Education Statistics (the Forum). While this list encompasses a wide range of ethical considerations and scenarios, it cannot represent every ethical issue that educators and the education data community will face.

## THE FORUM CODE OF DATA ETHICS

### INTEGRITY

1. DEMONSTRATE HONESTY, INTEGRITY, AND PROFESSIONALISM AT ALL TIMES.
2. APPRECIATE THAT, WHILE DATA MAY REPRESENT ATTRIBUTES OF REAL PEOPLE, THEY DO NOT DESCRIBE THE WHOLE PERSON.
3. BE AWARE OF APPLICABLE STATUTES, REGULATIONS, PRACTICES, AND ETHICAL STANDARDS GOVERNING DATA COLLECTION AND REPORTING.
4. REPORT INFORMATION ACCURATELY AND WITHOUT BIAS.
5. BE ACCOUNTABLE, AND HOLD OTHERS ACCOUNTABLE, FOR ETHICAL USE OF DATA.

### DATA QUALITY

6. PROMOTE DATA QUALITY BY ADHERING TO BEST PRACTICES AND OPERATING STANDARDS.
7. PROVIDE ALL RELEVANT DATA, DEFINITIONS, AND DOCUMENTATION TO PROMOTE COMPREHENSIVE UNDERSTANDING AND ACCURATE ANALYSIS WHEN RELEASING INFORMATION.

### SECURITY

8. TREAT DATA SYSTEMS AS VALUABLE ORGANIZATIONAL ASSETS.
9. SAFEGUARD SENSITIVE DATA TO GUARANTEE PRIVACY AND CONFIDENTIALITY.

# I. THE INTEGRITY CANONS

School districts use data in countless ways, and data-related integrity issues arise quite frequently. For example, in just one grading period, a school district dealt with several concerns related to professional integrity:

- ▶ A parent who had requested that his child’s directory information not be disclosed by the school received a commercial advertisement that clearly referenced data that had been collected as a part of the school registration process.
- ▶ A school guidance counselor used a few isolated pieces of information to make broad generalizations about a student’s educational and career potential.
- ▶ A well-respected charitable organization requested access to confidential data to help identify students who might benefit from its help and services.
- ▶ A local school received a high profile national award based on erroneous data and faulty analysis.
- ▶ A school administrator wanted to manipulate data in a legal but misleading manner to help improve the district’s public image.

How should staff respond to these situations?

What principles should guide this decisionmaking?

## I. DEMONSTRATE HONESTY, INTEGRITY, AND PROFESSIONALISM AT ALL TIMES

A parent had requested that the school not disclose his child’s directory information to the public. Upon receiving a series of advertisements from a local photographer—with his child’s middle name misspelled in exactly the same way as in school mailings—the parent asked a school board member whether the district shared contact information with commercial organizations. The board member asserted that the district would never do such a thing, but agreed that the identical misspelling was suspicious and decided to notify the superintendent. The superintendent’s investigation revealed that the wife of the district’s database manager was a photographer who specialized in children’s photos. The database manager’s employment was terminated after he admitted that he had shared the data without following proper procedures for the release of student information.

While this example focused on a database manager, honesty, integrity, and professionalism are critical requirements for any person whose job duties or volunteer responsibilities include handling education data. We expect no less than absolute honesty, integrity, and professionalism at all times from everyone trusted to work in our schools.

The people who handle data in our education system are expected to do many things—and do them all well. Most of these individuals are trained educators who provide instruction to students or supervise instruction at the school, district, or state level. Other data handlers have non-instructional leadership or administrative support roles. Still others provide highly skilled technical or data expertise that contributes to the effective and efficient operation of the education enterprise. Regardless of an individual’s job title, working in an education environment demands unwavering adherence to codes of appropriate conduct, operating expectations, and professional standards.

A “data handler” is defined in this document as anyone involved in the education enterprise—employee, appointee, volunteer, or vendor—who has access to education data or who contributes to the collection, management, use, or reporting of education data. Data handlers who are honest can be trusted to maintain objectivity and uphold an organization’s data procedures and protocols even when it requires extra effort, is not convenient, or otherwise runs counter to their own personal interests.

## Integrity and Professionalism

People with integrity do not cheat, steal, or lie, even when they will not get caught. They do not “borrow” data that they should not access; “cherry pick” data to misrepresent meaning; or misuse information in conflict with legal norms, ethical expectations, or common sense. Honesty and integrity are personal traits that are expected of any person, regardless of job title, role, responsibility, or function within an organization.

“Professionalism,” on the other hand, is commonly defined as the conduct, aims, or qualities that characterize or mark a profession. Thus, “professional conduct” complies with standards of behavior that apply to a specific role or position. Although common use of the word “professional” implies a specialized knowledge and academic preparation associated with certain types of skilled employment, “professionalism” as a concept can be extended to all roles and positions in an organization that handle data, regardless of job type. For example, superintendents behave “professionally” when they accurately report data to the school board, no matter the consequences. School board members demonstrate “professionalism” when they make sure that they understand the meaning and context of data before making decisions. Similarly, data entry clerks display “professionalism” when they take pride in their work and are careful to minimize entry mistakes.<sup>1</sup> Volunteers behave professionally when they respect that certain things seen and heard in a school building are private and should not be shared outside of their duties at the school.

Regardless of a data handler’s role in an education organization, consistently and continuously demonstrating honesty, integrity, and professionalism are of paramount importance. These qualities, more than any other characteristic or trait, serve as the foundation of ethical behavior.

## Recommended Practices and Training

- 1) Create an organizational culture that encourages honesty, integrity, and professionalism by adopting and enforcing the following practices:
  - a. Emphasize, through staff training, that the organization expects its employees to be honest, have a sense of integrity, and behave professionally. Convey these same expectations to vendors, consultants, volunteers, and anyone else who performs paid or unpaid work for the organization.
  - b. Explicitly require “honesty, integrity, and professionalism” in all job descriptions, staff contracts, volunteer policies, performance evaluations, and labor agreements.
  - c. Inform employees, contractors, and the general public of established policies, procedures, and expectations regarding honesty, integrity, and professionalism.
  - d. Commend and reinforce behavior that exemplifies high ethical expectations.

Ethical data professionals never intentionally bias data, manipulate meaning, or otherwise influence interpretation—they present data as accurately and objectively as possible.

Staff who consistently demonstrate honesty, integrity, and professionalism are the foundation of ethical behavior in an education organization.

<sup>1</sup>This is described more thoroughly in the Forum Guide to Building a Culture of Quality Data: A School and District Resource (see appendix A).

- e. Never tolerate dishonest, corrupt, or unprincipled behavior in the workplace, regardless of job type or level of authority.
- 2) Use data as they were intended.
    - a. Say what you mean, and mean what you say. For example, deceiving respondents by implying that you are collecting data for the district when it is really for your master's thesis is ethically untenable under all but the rarest of circumstances.
    - b. Be very cautious about using data for purposes other than their original intent. Be sure that doing so does not violate individuals' right to privacy or any agreements of anonymity that you, or your agency, have made. Aggregations of data may be published if personally identifiable information has not been disclosed.
  - 3) Avoid at all costs any release of data that could lead to physical, mental, or emotional harm to others. Establish and enforce security procedures and mechanisms necessary for protecting all sensitive data (e.g., academic, behavioral, health, employment, and financial information) from inappropriate release and use.
  - 4) Train all data handlers in the fundamental principles of data ethics—the “rights and wrongs” that are not legal mandates but are critical to the appropriate management and use of education data. Customize training efforts by job type as appropriate for communicating concepts and translating instruction into practice. Data clerks, teachers, and parent volunteers have different access to student data and face different situations in which they must know how to “do the right thing.”
  - 5) Use training activities that encourage learners to discuss and internalize the concepts of honesty, integrity, and professionalism. For example, ask participants to develop a statement describing the professionalism of their role in the organization; ask them to list, as a group, the work situations that call for honesty, integrity, and professionalism; develop a job-specific code of ethics, for example, “As a parent volunteer, it is my ethical responsibility to \_\_\_\_\_;” create and discuss scenarios in which these ethical qualities might be tested.





## 2. APPRECIATE THAT, WHILE DATA MAY REPRESENT ATTRIBUTES OF REAL PEOPLE, THEY DO NOT DESCRIBE THE WHOLE PERSON

Advising kids about their future educational opportunities and career choices was Mrs. Johnson's passion. Some of the students in her middle school had the ability to do just about anything they set their minds to, and she was always sure to tell these kids that the sky was the limit. But with other students, well, that was another story.

Colette, an eighth grader with a history of barely passing math courses, walked excitedly into Mrs. Johnson's office and told her that over the weekend she had taken an elevator ride to the top of the tallest building in the city. Clearly the experience had changed Colette's vision of her future. "I've decided to become an engineer who builds skyscrapers!" Mrs. Johnson quickly reviewed Colette's math scores, attendance history, and family situation, and decided that the data suggested another path. "You know, Colette, becoming an engineer requires a lot of specialized education, and college is very expensive. Maybe you shouldn't set your sights so high. I like your haircut. Have you ever thought about cosmetology?" Colette looked dejected. "Are you telling me that I can't build skyscrapers? What if I started studying really hard?" Mrs. Johnson decided not to sugarcoat her analysis. "No, dear, higher math can be quite challenging and your academic record isn't very strong." Colette chose to stand up for her new dream, "But I haven't even gotten to high school yet, Mrs. Johnson. Couldn't I take geometry next year and improve my grades?" Mrs. Johnson smiled condescendingly and said, "That's very ambitious, Colette, but geometry is much more difficult than it sounds. Why not register for general math and use the extra time to get a part-time job so that you have more experience when you start looking for a job?"

There are limits to how well data can portray people - who have complex thoughts, needs, and emotions. Data collected in schools are indicators of uniquely personal events, conditions, outcomes, and ambitions. Each piece of data in a student or staff database represents a particular attribute of a real person, and may be used to make important, lasting decisions. The data may be dry facts to the people who look at them, but to the people whose educational and professional experiences are being recorded, they are the pieces of a very personal academic career and individual history, recording their achievements and disappointments.

However, teachers, counselors, administrators, and others who use student records should be careful to focus on the student sitting before them as well as the student's history documented in a database. Some information could be incorrect, if data integrity is not maintained. Some could be misleading, if taken out of context. Did a disciplinary incident occur when the student was facing problems at home? Does the new student who's doing so poorly in math need to have his vision checked to be sure he can see the chalkboard?

And, perhaps most important, people can change. After all, that's the point of education! The double warning in this canon is that data cannot represent the total person whose life they record, and they cannot predict with absolute precision what that person will become in the future.

### *Recommended Practices and Training*

- 1) Accept that there are limits to how well data can describe people—people with complex thoughts, needs, and emotions; people with physical or psychological challenges that may not be well understood; or people who, through no fault of their own, live in circumstances that are unhealthy, unsafe, or unstable.

Each piece of data in a student or staff database represents an attribute of a real person, but these data cannot adequately portray all aspects of a multifaceted individual.

- 2) Be especially careful about making personal or professional judgments about people based solely on data. Be particularly alert to data that may be flawed, narrow in scope, or otherwise of limited applicability.
  - a. Just because data can be used to answer a question or inform an opinion does not mean that the information is entirely accurate, reliable, and unbiased.
  - b. Be very cautious about using data for purposes other than their original intent. Be sure that doing so does not violate individuals' right to privacy or any agreements of anonymity that you or your agency has made. Aggregations of data may be published if personally identifiable information has not been disclosed.
  - c. Effective, data-driven decisionmaking draws from multiple sets of data that support the same interpretation. Do not draw from a single source, if at all possible, and look at data from multiple sources over time to see if the findings are consistent.
- 3) Be willing to challenge commonly held assumptions and prejudices related to descriptive data.
  - a. For example, do not equate disability status with decreased intellectual aptitude or potential. In some cases, disability status reflects variation in learning styles rather than academic capacity, and some students with disabilities do not show differences in their ability to function in a school or life setting. In other instances, accommodations may permit students with disabilities to function at high academic levels.
  - b. Do not automatically equate school success with life success. Academic success is important, especially within the context of the education system, but people can find happiness, prosperity, and success in life without being the highest achiever in school.
- 4) Train data handlers to understand the limitations of data as a tool for describing individuals and categories of people by age, gender, racial/ethnic group, language of origin, job type, and other categories. Customize training efforts by job type as appropriate for communicating concepts and translating instruction into practice. Lead a discussion in which you ask if anyone has ever been treated unfairly because of data in a school or work record. Alternately, lead a discussion in which participants are asked to describe a situation in which outcomes showed the data about them to be poor predictors of success. Another activity is to provide participants with a scenario and ask them to fill in the missing parts. For example, prepare a short hypothetical resume that shows a break of several years in work history, or a string of jobs lasting no more than a year, and ask "applicants" to explain these to a job interviewer. See if the "off the record" information changes the interviewer's opinion of the applicant's credentials.

### 3. BE AWARE OF APPLICABLE STATUTES, REGULATIONS, PRACTICES, AND ETHICAL STANDARDS GOVERNING DATA COLLECTION AND REPORTING

The local business club had a reputation for doing good works throughout the community, so the district's data manager wasn't surprised when the superintendent told him to pitch in with the organization's latest charitable activity. Club members had asked for student socioeconomic data to help identify families in need so that they could offer financial help with books, school snacks, extracurricular activities, and other worthy initiatives. The data manager wanted to support these laudable efforts, but knew that he couldn't disclose the confidential data. When he informed the superintendent, his boss asked him to bend the rules this one time, "You know they're trying to do something good here. I really don't want us turning away people who want to help our neediest kids." The data manager agreed that everyone's intentions were pure, so he asked if his boss might consider an opt-in program, whereby all families would be notified of the program and invited to sign up if they were interested. The superintendent agreed that it was a fair idea, but noted that the yield on opt-in programs was usually low. "Can't we just bend the rules this one time to try to do a good thing?" The data manager knew that he faced quite a dilemma—doing good versus doing right.

The temptation to break the rules arises now and again. And ignorance of a legal requirement does not cancel the ethical obligation to meet it. Good ethics require that educators make themselves aware of existing and emerging statutes, regulations, practices, and ethical standards regarding data collection and data reporting. Anything short of staying up-to-date is neither a reasonable data practice nor an acceptable management option.

Organizations should make sure that staff and volunteers are familiar, to the extent their roles require, with any laws and policies governing the collection and reporting of data. Staff should be aware of any circumstances under which exceptions can be made. For example, can confidential information be shared with authorities if a student is in danger? When does a situation warrant disclosure?

Laws can change over time. Education organizations and the people who work with them should know their responsibilities regarding the protection of student data under the Family Education Rights and Privacy Act (FERPA), the Individuals with Disabilities Education Act (IDEA), and the Health Insurance Portability and Accountability Act (HIPAA). (See appendix D for more information on FERPA.)

Everyone who collects, handles, or reports data on individuals has legal and ethical responsibilities for this information. Organizations should provide training on these responsibilities to teachers, data clerks, and volunteers, among others. Everyone should know the district's policy on releasing student directory information and how to respond to requests for confidential information. The federal laws protecting staff data are not as stringent as those governing student records. Organizations should determine what state laws, and state or local policies, are applicable to staff data and information about parents or other community members. Which staff data are confidential, and which are public record? If data confidentiality is requested (or required) can its guarantee be honored?

Finally, the organization should be sure that everyone who is part of it is aware of who has the right to access different data. Teachers, counselors, administrators, support staff, and volunteers do not all have the same right of access to data. Knowing what

Ignorance is unethical. Good ethics demand that educators make themselves aware of changing statutes, regulations, practices, and standards.



information is private (not mine to know) is as important as knowing what information is confidential (not mine to share).

### *Recommended Practices and Training*

- 1) Encourage leadership within the organizational hierarchy (e.g., federal, state, and local education agencies, including board members) to know and effectively communicate current statutes, regulations, guidelines, accepted practices, and appropriate behavior regarding data access and disclosure to all employees.
- 2) Give educators access, in some reasonable format, to professional publications, instructional guides, trade journals, and other development materials necessary to stay abreast of relevant statutes, regulations, guidelines, accepted practices, and ethical standards.
- 3) Engage in professional development and staff training on relevant statutes, regulations, guidelines, accepted practices, and ethical standards concerning privacy and confidentiality. This training should be customized to meet the needs of different job responsibilities within the organization. Under most circumstances, this includes staff education about best practices for maintaining the privacy of individual student and staff information, including provisions of the federal Family Educational Rights and Privacy Act and similar state and local statutes (see the *Forum Guide to the Privacy of Student Information: A Resource for Schools*, at [http://nces.ed.gov/forum/pub\\_2006805.asp](http://nces.ed.gov/forum/pub_2006805.asp); and the *Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies*, at [http://nces.ed.gov/forum/pub\\_2004330.asp](http://nces.ed.gov/forum/pub_2004330.asp)).
- 4) Schedule periodic reviews to evaluate the effectiveness of communications and training efforts, as well as staff compliance with applicable statutes, regulations, guidelines, accepted practices, and ethical standards. Ensure that staff responsible for supervising the employees who perform data collection and reporting are, themselves, cognizant of state-of-the-art education data practices.
- 5) Train all data users in a routine and ongoing manner about data management, use, privacy, and exchange to ensure that they are aware of changing expectations and standards. Customize training efforts by job type as appropriate for communicating concepts and translating instruction into practice. One approach is to discuss the organization's rules about data disclosure and ask training participants to give examples of how each rule applies to their work. Develop several scenarios involving data confidentiality and ask the participants to talk about how they would handle them. For example, situations might include someone identifying himself as a prospective employer, who telephones and asks for information from a student's academic record; an in-service training session in which the presenter's visuals include names and other information about real students; talking with a volunteer who you have been informed divulged information about a student's health condition; or talking with a non-custodial parent who wants a copy of his or her child's grades. In order to encourage open discussion, do not ask training participants to report on instances in which they themselves have broken confidentiality regulations.

These and other free Forum best practice guides are described in appendix A and are available for downloading, printing, or ordering at <http://nces.ed.gov/forum/publications.asp>.

## 4. REPORT INFORMATION ACCURATELY AND WITHOUT BIAS

The community was thrilled to learn that the local high school had been named one of the top 10 schools in the country by a major news magazine. However, when examining the methodology behind the award, the district superintendent questioned the finding and decided that she needed to know how the rankings were determined. An inquiry to the magazine found that the data had been “checked and double-checked,” but no one at the publication was willing to divulge what data were used to determine the rankings. Additional investigation by district staff revealed that the magazine had used an incorrect enrollment figure, causing the participation percentage on a national test to be tremendously inflated. The superintendent understood that, if she reported this to the magazine, the high school would surely drop from the top tier to the second tier of “best schools.” Still, the error had to be corrected—it was the right thing to do. Despite the decline in national prominence, the superintendent was surprised to learn that her community—including parents, students, alumni, and the local media—were very proud that the school district chose to report the error rather than receive recognition it didn’t deserve. Ensuring accuracy over fame had actually confirmed to community members that they really did have one of the top school systems in the country.

With improved technologies for generating and presenting data, policymakers and the general public have become more number-savvy and more accustomed to looking for statistics to back up a position. Our ability to provide data that are more accurate and more relevant is stronger than it ever has been. As organizations focus on producing high-quality data, they should also raise expectations for high-quality data reporting and presentation. In the story that introduces this canon, a principled school administrator uncovered a mistake caused by faulty information. However, even after data quality has been established, data can still be subject to misuse. One common way of distorting data is by manipulating the way in which information is presented.

Data are often presented in graphs or charts that demonstrate, for example, if test scores are improving, administrative costs are decreasing, or student populations are changing. These visuals are effective when they summarize a host of numbers and complex analyses into a single, immediately understandable, “information snapshot.” However, unethical (or incompetent) data handlers can bias perception with formatting tricks that change the way data look in graphic form. One way to accomplish this, for example, is to change scales on a graph to influence interpretation (see figure 1 on the following page).

Not all data users possess the same level of analytical expertise. Community members, for example, may want a single graph, or a table that presents the findings as simply and straightforwardly as possible, while statistical researchers would probably prefer to see all the data and analyses laid out in detail. Despite the need to tailor reports to its audiences, organizations will benefit from adopting standard protocols to guide data reporting and minimize the potential for biased presentation that might skew interpretation.

Policies governing operations can also affect data accuracy. For example, a district rule that says “all students are considered present if a teacher fails to collect attendance” could tempt some school staff members to “forget” to take roll. Such a policy might lead to the appearance that student attendance rates were improving over time (as teachers continue to “forget” to take roll), even though the data collection policy had no meaningful effect on actual student attendance.

This ethical principle is tested when data show that something is not working well. Data handlers are expected to report information accurately and without bias, even when the news is bad!

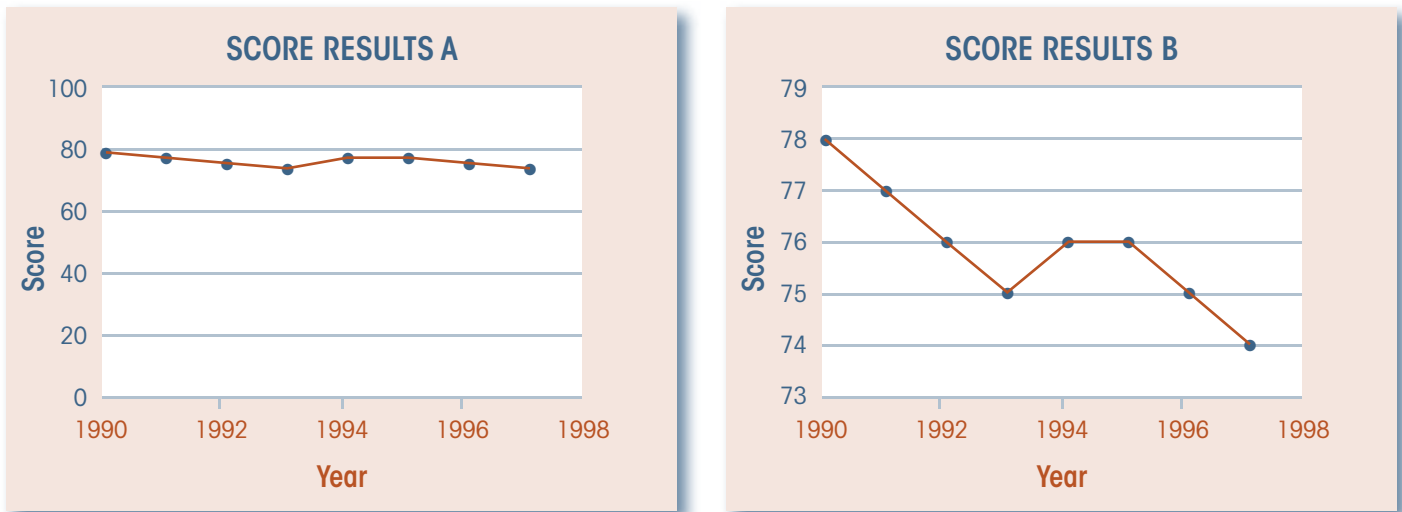


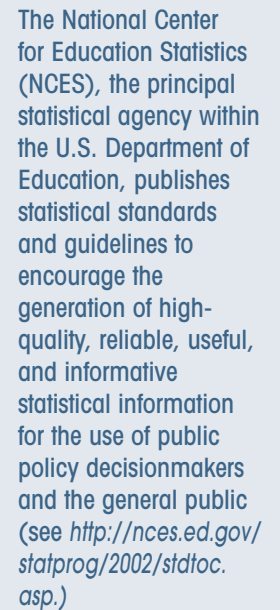
Figure 1. The same data values are represented in both graphs, but the choice of scale for the y-axis (score) might substantially influence the way a viewer interprets trends over time.

Finally, and very importantly, this canon comes into play when data represent bad news. People are rarely tempted to skew data that already make them and their organization look good. This ethical principle is likely to be tested when data show that something is not working well or is behind schedule. When this happens—and the news is bad—data handlers find out how strong their commitment to ethical behavior really is.

### *Recommended Practices and Training*

- 1) Develop a standard reporting framework to improve the consistency of reports and minimize the likelihood of bias in data presentation.
  - a. Develop and apply statistical standards and guidelines for writing data reports and presenting data tables. For example, many issues related to axis scales, years reported, and graphing style (e.g., line chart, pie chart, or stacked bars) can be standardized regardless of data values.
  - b. Include, in all reports, an explanation of how past reporting was presented and any changes in data methods (e.g., an assessment tool) or presentation (e.g., a report format); state the reasons why changes were made.
  - c. To the extent possible, use the same presentation standards in all report products. If information is presented in a standard format across years and across studies, audiences will learn to read reports easily – they can concentrate on the information rather than on the way in which it is presented.
  - d. Before releasing a report, undertake an independent review to assess whether the data are presented objectively and without bias, especially when they describe a situation that is not favorable to those responsible for producing the report.
- 2) Incorporate improvements to research design and methodology in data reporting, but do not let these changes mislead data interpretation. For example, if your dropout formula is adjusted and you see a correction in one direction or another because of the modification, do not declare that there was a meaningful change in your school's retention efforts unless you can crosswalk or otherwise compare the two methods. Similarly, a recalibrated assessment may offer neither positive nor negative evidence of change in student performance.

- 3) Correct errors that are identified in previously reported data. If published data are discovered to be inaccurate and correcting the data is feasible, the data should be corrected with an explanation and documentation in subsequent reports or releases of the data. Establish procedures for making corrections to ensure that revised releases include clear statements about the impact the revisions may have on previously reported statistics.
- 4) Train data reporters and users to follow standard data preparation and presentation methodologies so that data are presented as accurately and consistently as possible. Customize training efforts by job type as appropriate for communicating concepts and translating instruction into practice. For example, one exercise for technical staff would be to present them with an array of tables or graphs representing the same information but presented in ways that would mislead a reader. The task would be to find the “bad” presentations and talk about how each biased the data. Non-technical users, such as instructional staff or board members, could discuss these same tables or graphics after the trainer has highlighted the flaws in presentation. Another approach that might help staff who prepare presentations would be an open discussion (without names!) of situations in which they have been encouraged, or tempted, to bend the rules in showing data a little more favorably.



The National Center for Education Statistics (NCES), the principal statistical agency within the U.S. Department of Education, publishes statistical standards and guidelines to encourage the generation of high-quality, reliable, useful, and informative statistical information for the use of public policy decisionmakers and the general public (see <http://nces.ed.gov/statprog/2002/stdtoc.asp>.)



## 5. BE ACCOUNTABLE, AND HOLD OTHERS ACCOUNTABLE, FOR ETHICAL USE OF DATA

District leaders were worried about the outcome of the state reading assessment. The stakes were so high that the district's data steward and testing coordinator were even more careful than usual to make sure that the results, no matter what they might be, were accurate. Thus, they were surprised when the superintendent stopped by on a Friday afternoon for an unprecedented "friendly" chat. "So," he began. "I know you two are trusted staff members who are full of integrity, and I would never ask you to be anything but that way—but I do want you to know that these test scores are very important to our community, and any way we can view the glass as half full rather than half empty would be greatly appreciated. For example, even though we might not have made our testing targets, we did show some growth, which is what our public reporting needs to show. Do you understand that?" He was clearly implying that the public and even the school board shouldn't see all of the test results. The data steward and testing coordinator understood that the failing subgroups represented only a small portion of the students who were tested, but they also knew that it was disingenuous to show only the favorable results—and they prepared themselves for an ethical dilemma in the face of such pressure from their boss.

In a perfect world, ethical issues would never arise in an education setting. Unfortunately, ours is not a perfect world, and school personnel should be prepared for murky situations. Policies and procedures for dealing with breaches in ethical conduct need to be formulated, and staff members need to be trained to respond to ethical miscues when—not if—violations occur.

What happens, for example, when a staff member notices questionable behavior in the district office? Ideally, the incident would be reported and corrected, and the individual who brought it to light would be thanked. The more realistic scenario, however, is that the person who sees the infraction is likely to weigh the costs and benefits of reporting the violation: on the one hand, "this misconduct, whether intentional or not, needs to be corrected and I will make sure it is"; versus, "hmm, I know what my colleague is doing is wrong, but is it serious enough to get him in hot water? What will happen to me if I report the behavior?" Reporting ethical violations is easier when the offense is egregious or the consequences of reporting it are minimal. The dilemma is even greater when workers must decide whether to report that someone with authority over them is not behaving in accordance with accepted standards.

Fortunately, good leaders usually find a way to help others do the right thing. This has been the case with the advent of "whistleblower" laws in many states. Under these statutes, individuals who report violations of acceptable conduct are proactively shielded from retribution through administrative and legal protections. Such protective policies are also applicable for encouraging responsible reporting of illegal, unethical, or incorrect data use. To be effective, however, staff members need to understand how to report suspected violations and be confident they will be protected from retribution should they, in fact, register a concern.

### *Recommended Practices and Training*

1) Determine whether appropriate policies, processes, and procedures are in place in



your organization for reporting an ethical violation.

- a. If “whistleblower” protections are not available in the organization, create them (see appendix B).
  - b. If policies exist, examine them to determine whether they adequately protect whistleblowers.
  - c. Hold a staff meeting to discuss with your data handlers whether they would feel confident reporting ethical violations if necessary. Offer confidential meetings with selected staff members who represent different roles and responsibilities in the organization to ensure that they can express their concerns without fear of retribution.
  - d. Train data handlers to understand the steps they need to take to report illegal, unethical, or incorrect behavior. Make sure that they understand that they are procedurally protected from retribution.
  - e. Establish mandatory ethics training courses for all staff members.
- 2) Establish guidelines for data use policies that are aligned with applicable laws, regulations, and best practices (see appendix A). This includes guidelines related to data collection, governance, access, use, exchange, and reporting.
- a. Ensure that all guidelines are aligned with local laws, policies, and best practices.
  - b. Ensure that all guidelines are aligned with state laws, policies, and best practices.
  - c. Ensure that all guidelines are aligned with federal/national laws, policies, and best practices.
- 3) Establish and enforce data use agreements, including memoranda of understanding, nondisclosure agreements, and other mechanisms for ensuring appropriate data use (see appendix C).
- a. Require all data handlers, including staff and external users, to sign data use agreements and/or nondisclosure agreements prior to being granted access to any data files that aren’t already publicly available.
  - b. Establish a process for evaluating complaints about inappropriate use. Identify who is authorized to determine whether data use policies have been violated, what criteria are used for such a determination, how the process will be conducted fairly, and reasonable consequences related to policy violations.
  - c. Establish and enforce sanctions for the violation of data use agreements. An agreement that is unenforceable or lacks consequences is rarely effective.
- 4) Train all data users to ensure that they understand how to report violations of ethical behavior.
- a. Explain “whistleblower” protection policies to ensure staff feel confident that doing the right thing—reporting unethical behavior—will not negatively affect their job status or working conditions.
  - b. Review in detail the procedures for reporting a possible violation: who should be informed of the incident, what responsibilities the reporter may have for documenting the questioned behavior, what the repercussions could be to the observer who fails to report misconduct.
  - c. In training sessions, present hypothetical situations of both accidental and intentional data misuse to staff and encourage them to discuss how they would act if they became aware of them.

It can be a frightening proposition for workers to report that someone with authority over them is not behaving by accepted standards. Organizations may consider implementing “whistleblower” protections (see appendix B) to assure staff that they can report suspected violations without fear of reprisal.



## II. THE DATA QUALITY CANONS

School districts use data in countless ways, and data quality issues arise quite frequently. For example, in a single grading period, one school district dealt with several ethical concerns related to producing accurate, useful, and timely data:

- ▶ The district found itself with disparate sources of free- and reduced-lunch eligibility data, and administrators realized that the absence of a single, authoritative source was leading to inconsistent, and even biased, reporting because one set of data or the other was being used depending on how the results looked to the person providing the data.
- ▶ Standardized test scores appeared to have improved, but the district realized that it would be wrong to let people assume the results measured improved academic achievement when, in reality, they probably reflected a change in the assessment tool.

How should staff respond to these situations?

What principles should guide their decisionmaking?

### 6. PROMOTE DATA QUALITY BY ADHERING TO BEST PRACTICES AND OPERATING STANDARDS

All students enrolling in the district were flagged in the student information system (SIS) as either “eligible” or “ineligible” for free- and reduced-price meals. In addition to these data, food services maintained its own record of students receiving free- and reduced-price meals to support the daily management of the cafeterias. Because of these redundant sources for similar data (“eligible” and “participating” counts were easily confused), the district was erratic in its free- and reduced-price meals reporting—the number of students reported for the program varied depending on whether the data were reported by the SIS or food services staff. Moreover, because there were two different counts, district staff faced the temptation to use the number that better met their reporting needs. Sometimes the count of participating students made the district look better, and sometimes the count of eligible students was beneficial. It didn’t take long for the staff to realize that this confusion between eligible and participating counts was leading to ethical dilemmas.

Two new data governance policies were enacted to remedy the situation. The first stated that the student information system was the authoritative source for all data in the district. The second policy was an offshoot of the first, declaring that only data staff could respond to data requests, and program or service staff were no longer permitted to provide data independently. Thus, if a count of students receiving free- or reduced-price meals was needed, the report would clearly distinguish it from the number of students eligible for this program.

Effective instruction, efficient school management, and quality data are related. The importance of quality in the information used to develop an instructional plan, run a school, create a budget, or place a student in a class cannot be overvalued. Most data experts would agree that the following characteristics are critical to this essential component of good schools:

- ▶ **Utility:** Data should provide information that is useful to the organization in a practical way. If data are not useful, there is no reason to collect them.
- ▶ **Accuracy and validity:** Data should measure what they purport to measure. In other words, data values should be correct and free of bias.

- ▶ **Reliability:** Data should be consistent, reproducible, and dependable. Data are not reliable if the values would change if they were collected more than once, or by more than one person. Properly documenting revisions to data values, definitions, and other characteristics is also necessary to ensure data reliability.
- ▶ **Timeliness:** Data should be readily available for decisionmaking. For example, do teachers and curriculum developers receive test results in time to inform instructional planning? If data are not available when they are needed, they lack in value and quality.
- ▶ **Cost-effectiveness:** Collecting and maintaining data requires resources, and this burden should be evaluated against the data’s utility and necessity. In other words, the value to instructional and non-instructional decisionmaking and reporting should outweigh the costs of collection and storage.

Just as canon 3 asserts that data handlers are ethically responsible for knowing the laws, regulations, and policies that govern access to the information for which they are responsible, this canon asserts that they are ethically responsible for ensuring high data quality to the best of their ability.


There are many accepted practices and operating standards that promote good data quality. For example,

- ▶ office staff should set aside a regular time for data entry tasks, which should be conducted in an area free from distractions such as foot traffic and noise;
- ▶ technologists should offer a help desk and/or an online help area for data entry staff;
- ▶ data stewards should resolve data discrepancies before reports are forwarded to senior staff for review and approval;
- ▶ principals should develop a calendar for data reporting deadlines;
- ▶ teachers should ask for instructions and guidance for improving data use in the classroom;
- ▶ superintendents should support a culture of quality data through a robust professional development program; and
- ▶ school board members should recognize data collection, management, and use as a routine cost of doing business – and, as much as possible, provide the resources for this work.

For more information about supporting data quality, see the *Forum Guide to Building a Culture of Data Quality*, listed in appendix A.

### *Recommended Practices and Training*

- 1) Use best practice resources to design your data systems and train data handlers. The topic is beyond the scope of this Guide, but there are a number of Forum publications that may be especially helpful (see appendix A):
  - a. *Forum Curriculum for Improving Education Data: A Resource for Local Education Agencies*—for lesson plans, instructional handouts, and related resources for helping schools develop a culture of data quality.
  - b. *Managing an Identity Crisis: Forum Guide to Implementing New Federal Race and Ethnicity Categories*—to guide implementation of the new federal race and ethnicity categories.
  - c. *Every School Day Counts: The Forum Guide to Collecting and Using Attendance Data*—to improve the quality, comparability, and utility of attendance data.
  - d. *Accounting for Every Student: A Taxonomy for Standard Student Exit Codes*—to improve the quality, comparability, and utility of exit data.
  - e. *Forum Guide to the Privacy of Student Information: A Resource for Schools*—to help apply federal, state, and local privacy laws.

- 
- f. *Forum Guide to Education Indicators*—to help construct and apply commonly used education measures.
  - g. *Forum Guide to Decision Support Systems: A Resource for Educators*—to develop a robust decision support system in an education organization.
  - h. *Creating a Longitudinal Data System*—to learn more about the ten essential elements of a state longitudinal data system, as available from the Data Quality Campaign at [http://www.dataqualitycampaign.org/files/Publications-Creating\\_Longitudinal\\_Data\\_Systems-Lessons\\_Learned\\_by\\_Leading\\_States.pdf](http://www.dataqualitycampaign.org/files/Publications-Creating_Longitudinal_Data_Systems-Lessons_Learned_by_Leading_States.pdf).
- 2) Data system improvement is more than this *Guide* can address, but organizations are encouraged to develop a comprehensive and coordinated plan for improving and ensuring data quality, addressing issues such as
- a. assigning unique student identifiers;
  - b. using prepopulated forms for assessments when appropriate;
  - c. performing data verification, validation, editing, as necessary to assess and improve data quality;
  - d. integrating systems to reuse data for multiple appropriate purposes (payroll, human resources, etc.) rather than collecting and rekeying information already owned by the organization;
  - e. incorporating industry standards across disparate systems, such as the Schools Interoperability Framework standards available at (<http://www.sifinfo.org>);
  - f. utilizing applications that allow for easy import and export of existing student data; and
  - g. identifying the authoritative source of data items when multiple systems include the same data items.
- 3) Update data practices to reflect changing policy needs. For example, the routine use of a surname as a family identifier may not be sufficient when the traditional family unit definition is expanded to include other family members, such as parents, stepparents, grandparents, or child advocates.
- 4) Train all data users about the concepts and practices surrounding the generation, maintenance, and use of high quality education data.



## 7. PROVIDE ALL RELEVANT DATA, DEFINITIONS, AND DOCUMENTATION TO PROMOTE COMPREHENSIVE UNDERSTANDING AND ACCURATE ANALYSIS WHEN RELEASING INFORMATION

The data looked good. Scores on the ninth grade state mathematics assessment had gone up substantially. But rather than celebrate, the administrative staff stared at each other. The testing coordinator said what everyone was thinking: “You know, we could get away with reporting that our scores have improved—the assessment has the same title and the scores are higher. But we know that the test was redesigned and it would be wrong not to mention that in our reports, right?” Fortunately, the superintendent went even further, and asserted, “Not only will we state that the assessment has changed, we will emphasize the point given the high likelihood that people will be confused unless it is addressed explicitly”.

Data handlers are ethically obligated to provide sufficient information for data users to reasonably interpret the meaning of data shared in reports and other publications. In some cases, this can mean including additional information (e.g., relevant differences between the old and new assessments) or pointers to other data sets. In others, it might mean sharing caveats about appropriate data use and quality limitations that might not otherwise be understood or assumed by a data user. Under almost all scenarios, data users need access to data definitions, formulas, methodologies, documentation, and other contextual information that influence use and interpretation. This is a delicate process; too much detail, or too technical an explanation, can lead readers to throw up their hands (and the report!) in frustration.

**Education indicators are too often interpreted out of context. For guidance on appropriate indicator use and presentation, see the *Forum Guide to Education Indicators*. Also, see the *Forum Guide to Metadata for information related to “data about data.”* (Both guides are listed in appendix A.)**

No isolated piece of data is meaningful without related data that explain further, provide a comparative or complementary perspective, or otherwise serve as context for guiding interpretation. In fact, most data are value neutral unless interpreted in light of their context. For example, “test score” is a piece of information used frequently (and with high stakes) in schools. But what does a value of “68” mean? Is it an individual’s score, a class average, or a national median? What is the passing score? Is the exam in a core subject matter area or in an elective class? Is passing the test required for graduation? Value judgments—whether a “68” on an exam is a good score—depend greatly on the related data that provide context in which meaning is assessed.

Just as canon 2 asserts that data can never completely represent an individual, no single piece of data can supply all the information needed to answer a policy question confidently. Assessing any aspect of a complex education enterprise usually requires a sizable body of data so that decisionmakers can inspect the issue within a well-integrated, multidimensional context. For example, consider two school districts: the first with a 90 percent graduation rate and the second with a 40 percent graduation rate. Two years later, these rates have improved 3 points at the first school, to 93 percent; and 20 points at the second school, to 60 percent. Without the original

Defining the terms in reports goes a long way toward ensuring they are understood. Best practice definitions for many data elements can be found in the *NCES Handbooks Online* at <http://nces.ed.gov/programs/handbook>.

No single piece of data can provide meaningful information in the absence of related data that provide context.

graduation rates, one might assume that the school with the 20-point increase is retaining students more effectively than the school with the 3-point increase. Looking at data over time provides a context in which data users would see that the difference in improvement is probably affected to some degree by the starting points—it becomes harder to improve as any rate approaches the 100 percent ceiling. Other information could advance the interpretation even further. Say, for example, that the school with the 40 percent graduation rate was the alternative school for students at risk for dropping out. In that case, progressing from a 40 to 60 percent graduation rate would be a significant achievement.

### *Recommended Practices and Training*

- 1) Establish statistical standards and guidelines for data presentation in all public reports.
  - a. Include explanations of any preparatory or statistical procedures used while developing the report.
  - b. Prepare documentation to summarize research methodology and issues involved in collecting, analyzing and publishing the data.
  - c. Include file structure, record layout, codebook, metadata, and data dictionary guidance or databases as appropriate.
  - d. Include definitions for all technical, data, and educational terms and jargon; as well as any surveys and formulas referenced in the report.
  - e. Include related information that encourages a broader, more comprehensive, and accurate interpretation of the data in the report.
  - f. Add an explanation when readers may misinterpret data. For example, if dropout rates are being reported, state whether the data represent a cohort rate or annual rate, and define the rate, rather than assuming it will be intuitively understood.
  - g. Provide technical contact information on all reports so that readers with questions about methodology, definitions, or documentation know where to turn for additional information and clarification.
- 2) Subject draft reports to multiple reviews and share reviewers' comments with the authors.
- 3) Train all data handlers to provide additional data and metadata in reports and correspondence as appropriate to improve data use and interpretation.

### III. THE SECURITY CANONS

School districts use data in countless ways, and data-related security issues arise quite frequently. One school district recently dealt with several ethical concerns related to data security:

- ▶ A technician's error caused a server to crash after the network manager had forgotten to backup files, resulting in several thousand dollars being spent to restore lost data.
- ▶ A personal friendship between a school board member and school principal led to informal data exchanges and, eventually, the inappropriate public release of confidential student data.

How should staff respond to these situations?

What principles should guide this decisionmaking?

#### 8. TREAT DATA SYSTEMS AS VALUABLE ORGANIZATIONAL ASSETS

The network manager called the chief information officer at 11:00 p.m. "You're never going to believe this, but a tech assistant fried our database." The CIO rolled her eyes. "How many times do we need to tell people they can't touch that equipment?" "Well, to be fair, it was a new employee—but you're right, it is an ongoing problem." The CIO then asked, "But why are you calling me? You know how to access the offsite backup files as well as I do." "That's the second part of the problem," the network manager confessed. "I know there is no excuse for it, but I wanted to leave a little early on Friday and figured I could have the backup tapes sent in on Monday. I meant to do it first thing Monday morning, but a data request from the superintendent came in and I just lost track of time. I know I fouled up, but we don't have an offsite backup for the last two weeks." The CIO was very angry, but knew that the network manager appreciated the magnitude of the mistake and that a reprimand wouldn't help. "Well, we're going to need to hire specialists and get the system fixed." "But that's going to cost several thousand dollars," the network manager interjected. "I know," the CIO said. "But tell me our other options?"

Education organizations spend a great deal of money on systems for collecting, storing, accessing, using, and sharing data. In addition to these infrastructure expenses, there are significant human resource costs for collecting and managing data. Collection instruments, including assessments and survey forms, for example, must be carefully designed by highly skilled professionals. The administration of these assessments and surveys—beginning with the delivery of the materials and ending with verification and validation activities—requires many staff hours and represents a substantial investment. Moreover, many education organizations build or rent climate-controlled facilities, contract with offsite backup storage services, employ elaborate encryption algorithms, mandate restrictive user authentication schemes, conduct criminal background checks on staff, and engage in robust destruction techniques at the end of a piece of data's useful life. Education data are clearly a valued asset or they would not warrant this much attention.

This canon is probably violated unintentionally as often as it is willfully broken. Failure to follow procedures that protect data and data systems – or failure to anticipate potential threats to these – can cause as much damage as any deliberate sabotage.

For more information about data security, see the *Forum Unified Education Technology Suite* (appendix A).

In addition to the loss of resources when a data system must be replaced or repaired because of negligent behavior, there is the issue of data security. It is practically impossible to retrieve data after they have been released electronically. Once someone's private information has been shared over the Internet, it will never again be private. Moreover, when information is lost, damaged, or otherwise unavailable when needed, there can be serious effects on the operation of an education organization. What happens when a teacher cannot download a lesson plan in time to inform instructional choices for students sitting in his classroom? Or when a school nurse cannot find a sick kindergartner's home telephone number quickly? What would happen in the aftermath of a tornado or other catastrophe if a school principal could not access the morning's attendance information to account for every student after a building evacuation?

A wide range of people and events threaten data, including

- ▶ natural conditions such as fire, flood, lightning, or humidity;
- ▶ intentional acts, including malicious hackers and computer viruses;
- ▶ routine or unintentional actions, such as unwittingly placing a coffee cup on a server or leaving a password taped to a computer monitor.

Data must be protected from these and other threats by means of a wide range of physical, software, hardware, and access security measures. Countermeasures include a host of processes and products intended to prevent, deter, contain, and detect problems, as well as recover data when needed. However, while we rely on traditional technical and data management solutions to security concerns, these security procedures are implemented by individuals who must follow a professional ethic that recognizes their responsibilities as stewards of the organization's information resources.

**When information is lost, damaged, or otherwise unavailable when needed, it can have a serious effect on the operations of an education organization.**

### *Recommended Practices and Training*

- 1) Document all security procedures including
  - a. passwords;
  - b. system access procedures;
  - c. encryption procedures and algorithms;
  - d. data exchange protocols with partners (schools, districts, state education agencies, intermediate units, application service providers, etc.);
  - e. metadata (data about data) concerning technologies, methods, operations, and data elements; and
  - f. other security procedures you may have.
- 2) Establish a thorough and robust security plan based on an extensive risk assessment, threat analysis, and countermeasure strategy for the entire organization.
- 3) Establish procedures that ensure adherence to security procedures for all forms of data, including digital and print records.
  - a. Employ physical security measures without exception. For example, never prop open the door to the server room when it is supposed to stay locked, and install locks and other surveillance tools to prevent unauthorized entry into secure areas.



- b. Follow all security requirements related to the use of mobile data storage devices, including laptop computers, handhelds, portable disk drives (e.g., jump drives), etc.
  - c. Use required transmission protocols for all forms of data exchange, including transfers of data tapes and email. This often includes the use of encryption and password privileges.
  - d. Back up data responsibly. Although the organization may engage in offsite storage, individual users must be sure to store data in proper formats, in designated locations, and with appropriate testing and verification.
  - e. Never allow data handlers to access data that are not required for their work.
  - f. Never allow data handlers to share their passwords or other authentication information with other users who may not have the same access privileges.
  - g. Never allow data handlers to use shortcuts or unauthorized channels for accessing the organization's systems and networks, whether onsite or remotely.
  - h. Destroy data that have reached the end of their useful life.
  - i. Review and reauthorize user access privileges at least once a year.
- 4) Train all data users about their data security responsibilities.
- a. Thoroughly orient new employees to security procedures, and make sure they understand their responsibilities and repercussions for failing to observe procedures.
  - b. Include security training for staff and volunteers who have access to the organization's information system. This should include what to do to protect hardware and software as well as protecting information.



## 9. SAFEGUARD SENSITIVE DATA TO GUARANTEE PRIVACY AND CONFIDENTIALITY

A school board member was a personal friend of the principal at the local elementary school. When the board member needed information, she would email the principal and get a reply with the data attached. Both school leaders knew they were circumventing official procedures for sharing data, but rationalized that, since they both had privileges to obtain the data from the data steward, this more direct and informal approach only expedited an exchange that was otherwise permissible anyway. They didn't see any harm in this practice until the board member made a public presentation that inadvertently revealed that the one and only Asian female student in the 4th grade had a learning disability. The student's parents were in the audience and took offense to the public display of private information. The district's information security officer informed both the board member and principal that sharing data so haphazardly violated the district's policies and procedures. Had proper procedures been followed, the data steward would have masked all personally identifiable information and the private information would not have been accidentally disclosed.

*Sensitive information is that information that, if lost or compromised, might negatively affect the subject of the information.*

A data handler does not have the right to look at her neighbor's child's grades simply because she has access privileges to student information. There must be a legitimate "need to know" that stems from officially assigned work responsibilities.

Within a data system, there is a distinction between "general information" (i.e., those data that are generally helpful to your organization as it carries out its mission) and "sensitive information" (i.e., those data that are confidential and/or vital to your organization as it carries out its mission). For example, a data file with "help" instructions for website users is a "general" support component within your data system. While the files are important to users facing a web problem, the data are not vital to running a school or school system; nor are they private in nature or otherwise subject to confidentiality restrictions. On the other hand, data about class assignments are both confidential (data about student course selection are private) and vital to the school's core instructional mission (principals should know where students need to be at every moment of the day).

Ethical standards for protecting sensitive information are higher than those for general information. With the exception of some directory information that may be considered a part of the public record, individual student information (e.g., transcripts and other individual records) are substantially a private matter and, as such, are required to be maintained in a confidential manner. They are not the public's business, nor a data handler's business, unless there is a legitimate "need to know" the information to carry out officially assigned responsibilities.

Canon 3 addresses the need to be aware of laws and policies governing data collection and reporting, including the confidentiality of private data about individuals. The principle in canon 9 addresses the responsibility of organizations to establish and enforce procedures that will put these safeguards in place.

### *Recommended Practices and Training*

- 1) Identify which data are considered to be sensitive (private and/or vital to operations).
- 2) Develop and implement a robust data security plan that includes specific precautions for sensitive data, such as the following.
  - a. Limit access privileges strictly to data handlers who "need to know" the information to conduct their official duties and responsibilities.
  - b. Review and reauthorize user access privileges on an annual basis.

- c. Limit remote access privileges so that data in a secure location cannot be exported to a site that is not secure (e.g., downloads from a secure database into an Excel or PDF file at home).
  - d. Maintain high standards for verifying data requests and data sharing. Due diligence prior to sharing data is more than just identifying who wants the data. Ask questions such as: Why do they want it? How will they use it? Will they destroy it properly? How can proper handling be verified? Will they sign an acceptable use agreement? Note that it is often helpful to have these questions answered in writing.
  - e. Mandate password rules that make it difficult for hackers to guess. For example, passwords should be six or more characters in length and include at least one letter and one number, as well as an asterisk, exclamation point, or other special character. Passwords should not be names or words that appear in a dictionary.
  - f. Require the use of secure transmission technologies, including secure servers, authentication tools, and encryption algorithms.
  - g. Store data securely. This requires appropriate physical security, software security, access security, network security, and related behavioral management security.
  - h. Establish and enforce security expectations for portable data storage media, including laptop computers, external hard drives, portable drives, etc.
- 3) Establish and enforce policies governing the release of student data (both private and directory information) in compliance with FERPA, as well as related state and local privacy laws and regulations.
- a. Train all data handlers to understand their responsibilities with respect to FERPA and other applicable statutes and regulations.
  - b. Require written permission from a parent to release non-directory information subject to the exceptions identified in FERPA.
- 4) Train all data handlers to identify which data are general information and which are sensitive.
- a. Ensure that data handlers understand the expectations and consequences of FERPA, HIPAA, and related state or local privacy laws.
  - b. Train individuals based on their access privileges to sensitive data. Non-technical staff with access privileges—such as teachers, administrators, or data clerks—need to understand the data system’s security safeguards and how they can follow them. Include discussions about the “why” of security as well as the “how,” so that learners can internalize this ethical principle and apply it to their work.

Protecting the confidentiality of individually identifiable data is imperative. The primary difference in how individual student and staff data should be secured stems from protections specific to student data, as detailed in FERPA (see appendix D).

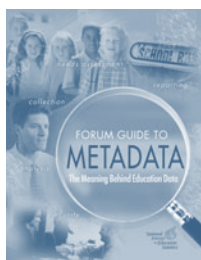


## APPENDIX A

# RELATED RESOURCES

These materials may be useful to school, district, or state education agency staff considering data ethics.

### **Forum Guide to Metadata: The Meaning Behind Education Data**



[http://nces.ed.gov/forum/pub\\_2009805.asp](http://nces.ed.gov/forum/pub_2009805.asp)

This document was developed to empower staff to use data more effectively as information. It explains what metadata are, why they are critical to the development of sound education data systems, what components comprise a metadata system, what value metadata bring to data management and use, and how to implement and use a metadata system in an education organization.

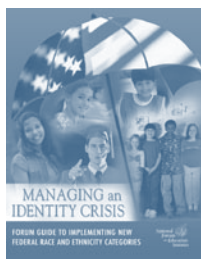
### **Every School Day Counts: The Forum Guide to Collecting and Using Attendance Data**



[http://nces.ed.gov/forum/pub\\_2009804.asp](http://nces.ed.gov/forum/pub_2009804.asp)

This Forum guide offers best practice suggestions on collecting and using student attendance data to improve performance. It includes a standard set of codes to make attendance data comparable across districts and states. The publication also presents real-life examples of how attendance information has been used by school districts.

### **Managing an Identity Crisis: Forum Guide to Implementing New Federal Race and Ethnicity Categories**



[http://nces.ed.gov/forum/pub\\_2008802.asp](http://nces.ed.gov/forum/pub_2008802.asp)

This best-practice guide was developed to assist state and local education agencies in their implementation of the new federal race and ethnicity categories, thereby reducing redundant efforts within and across states, improving data comparability, and minimizing reporting burdens. It serves as a toolkit from which users may select and adopt strategies to help them quickly begin the process of implementation in their agencies.

## Forum Guide to the Privacy of Student Information: A Resource for Schools



[http://nces.ed.gov/forum/pub\\_2006805.asp](http://nces.ed.gov/forum/pub_2006805.asp)

This free publication was written to help school and local education agency staff members better understand and apply the Family Educational Rights and Privacy Act (FERPA), a federal law that protects privacy interests of parents and students in student education records. It defines terms such as “education records” and “directory information”; and offers guidance for developing appropriate privacy policies and information disclosure procedures related to military recruiting, parental rights and annual notification, videotaping, online information, media releases, surveillance cameras, and confidentiality concerns related specifically to health-related information. Much of the guidance relating to privacy policies would be of interest to organizations generating business rules about the topic.

## Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies



[http://nces.ed.gov/forum/pub\\_2004330.asp](http://nces.ed.gov/forum/pub_2004330.asp)

This free guide presents a general overview of privacy laws and professional practices that apply to information collected for, and maintained in, student records. The publication also provides an overview of key principles and concepts governing student privacy; summarizes federal privacy laws including recent changes; identifies issues concerning the release of information to both parents and external organizations; and suggests good data management practices for schools, districts, and state education agencies. Much of the guidance relating to privacy policies would be of interest to organizations generating business rules about the topic.

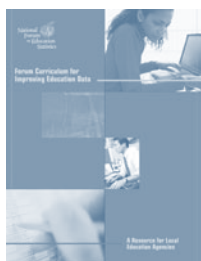
## Forum Guide to Building a Culture of Quality Data: A School and District Resource



[http://nces.ed.gov/forum/pub\\_2005801.asp](http://nces.ed.gov/forum/pub_2005801.asp)

This free publication asserts that good data, like good students, are produced in schools. While it is undeniably harder to teach a student than it is to collect statistics, certain procedures can help to achieve both goals. Recently, awareness has grown about the link between effective teaching, efficient schools, and quality data. The quality of the information used to develop an instructional plan, run a school, plan a budget, or place a student in a class depends on the school data clerk, teacher, counselor, and/or school secretary who enter data into a computer. With that in mind, the focus of this report is on data entry and getting things done right from the beginning.

## Forum Curriculum for Improving Education Data: A Resource for Local Education Agencies



[http://nces.ed.gov/forum/pub\\_2007808.asp](http://nces.ed.gov/forum/pub_2007808.asp)

This curriculum supports efforts to improve the quality of education data by serving as training materials for K–12 school and district staff. It provides lesson plans, instructional handouts, and related resources, and presents concepts necessary to help schools develop a culture for improving data quality.

## Forum Guide to Education Indicators



[http://nces.ed.gov/forum/pub\\_2005802.asp](http://nces.ed.gov/forum/pub_2005802.asp)

This publication provides encyclopedia-type entries for 44 commonly used education indicators. Each entry contains a definition, recommended uses, usage caveats and cautions, related policy questions, data element components, a formula, commonly reported subgroups, and display suggestions. This publication will help readers better understand how to appropriately develop, apply, and interpret commonly used education indicators.

## NCES Nonfiscal Data Handbook for Early Childhood, Elementary, and Secondary Education (2007)

Handbooks Online

An online resource for standard education terms, definitions and classification codes.

<http://nces.ed.gov/programs/handbook>

The *NCES Handbooks* are a valuable source of metadata for organizations and individuals interested in education data. These print and online resources define standard education terms for students, staff, schools, local education agencies, intermediate education agencies, and state education agencies. The *Handbooks* are intended to serve as a reference for public and private organizations, including education institutions and early childhood centers, as well as education researchers and other users of education data. In order to improve access to this valuable resource, NCES has also developed the *NCES Handbooks Online*, a web-based tool that allows users to view and download *Handbook* information via an electronic table of contents, a drill down finder, element name and first letter searches, and advanced query options.





## APPENDIX B

# SAMPLE WHISTLEBLOWER PROTECTION POLICY

Whistleblower policies are critical tools for protecting individuals who report activities believed to be illegal, dishonest, unethical, or otherwise improper. This sample policy is adapted from a document developed by the Fairbanks (Alaska) North Star Borough.<sup>1</sup>

- I. The organization will not retaliate against a whistleblower. This includes, but is not limited to, protection from retaliation in the form of an adverse employment action such as termination, compensation decreases, or poor work assignments and threats of physical harm. Any whistleblower who believes he/she is being retaliated against must contact the Human Resources Director immediately. The right of a whistleblower for protection against retaliation does not include immunity for any personal wrongdoing that is alleged and investigated.
- II. Whistleblower protections are provided in two important areas: confidentiality and retaliation. Insofar as possible, the confidentiality of the whistleblower will be maintained. However, identity may have to be disclosed to conduct a thorough investigation, to comply with the law, and to provide accused individuals their legal rights of defense.
- III. Individuals protected include
  - a. the employee, or a person acting on behalf of the employee, who reports to a public body or is about to report to a public body a matter of public concern; or
  - b. the employee who participates in a court action, an investigation, a hearing, or an inquiry held by a public body on a matter of public concern.
- IV. The organization may not discharge, threaten, or otherwise discriminate against an employee regarding the employee's compensation, terms, conditions, location, or privileges of employment.
- V. The organization may not disqualify an employee or other person who brings a matter of public concern, or participates in a proceeding connected with a matter of public concern, before a public body or court, because of the report or participation, from eligibility to bid on contracts with the organization; receive land under a district ordinance; or receive another right, privilege, or benefit.
- VI. The provisions of this policy do not
  - a. require the organization to compensate an employee for participation in a court action or in an investigation, hearing, or inquiry by a public body;
  - b. prohibit the organization from compensating an employee for participation in a court action or in an investigation, hearing, or inquiry by a public body;

---

<sup>1</sup> Retrieved May 1, 2009, from <http://www.co.fairbanks.ak.us/humanresources/policies/65%20personnel-payroll/p%20%2065-14%20whistleblowers.pdf>

- c. authorize the disclosure of information that is legally required to be kept confidential; or
- d. diminish or impair the rights of an employee under a collective bargaining agreement.

VII. Limitation to protections

- a. A person is not entitled to the protections under this policy unless he or she reasonably believes that the information reported is, or is about to become, a matter of public concern; and reports the information in good faith.
- b. A person is entitled to the protections under this policy only if the matter of public concern is not the result of conduct by the individual seeking protection, unless it is the result of conduct by the person that was required by his or her employer.
- c. Before an employee initiates a report to a public body on a matter of public concern under this policy, the employee shall submit a written report concerning the matter to the organization's chief executive officer. However, the employee is not required to submit a written report if he or she believes with reasonable certainty that the activity, policy, or practice is already known to the chief executive officer; or that an emergency is involved.

VIII. Relief and penalties

- a. A person who alleges a violation of this policy may bring a civil action and the court may grant appropriate relief.
- b. A person who violates or attempts to violate this policy is also liable for a civil fine of not more than ten thousand dollars (\$10,000.00).

## Procedures

- I. If an employee has knowledge of or a concern of illegal or dishonest/fraudulent activity, the employee is to contact his/her immediate supervisor or the Human Resources Director. All reports or concerns of illegal and dishonest activities will be promptly submitted by the receiving supervisor to the Human Resources Director, who is responsible for investigating and coordinating any necessary corrective action. Any concerns involving the Human Resource Director should be reported to the chief executive officer.
- II. The whistleblower is not responsible for investigating the alleged illegal or dishonest activity, or for determining fault or corrective measures; appropriate management officials are charged with these responsibilities.
- III. Examples of illegal or dishonest activities include violations of federal, state, or local laws; billing for services not performed or for goods not delivered; and other fraudulent financial reporting. The employee must exercise sound judgment to avoid baseless allegations. An employee who intentionally files a false report of wrongdoing will be subject to disciplinary action.

## Supplemental information

### Definitions

1. “*Whistleblower*” is defined by this policy as an employee who reports, to one or more of the parties specified in this policy, an activity that he/she considers to be illegal, dishonest, unethical, or otherwise improper.
2. “*Employee,*” or “*public employee,*” means a person who performs a service for wages or other remuneration under a contract of hire, written or oral, express or implied, for the district.
3. “*Matter of public concern*” means
  - a. a violation of a state, federal, or municipal law, regulation, or ordinance;
  - b. a danger to public health or safety; and/or
  - c. gross mismanagement, substantial waste of funds, or a clear abuse of authority.
4. “*Public body*” includes an officer or agency of
  - a. the federal government;
  - b. the state;
  - c. a political subdivision of the state including a municipality or a school district; and
  - d. a public university in the state.





## APPENDIX C

# MEMORANDA OF UNDERSTANDING AND OTHER DATA USE AGREEMENTS

Memoranda of understanding (MOUs) and acceptable use statements are effective tools for describing and enforcing data usage agreements between two or more parties. They are frequently used to formally agree to desirable behavioral practices such as good data ethics.

A memorandum of understanding (MOU) is a written document describing a bilateral or multilateral agreement between two or more parties. It expresses a convergence of will and understanding between parties, indicating an intended common line of action. It most often is used in cases where parties do not intend to imply a legal commitment to each other, but do wish to engage in an agreement of principle all the same.

A MOU typically establishes the framework for collaboration, intended outcomes, audiences, and the purposes for which data will and will not be used. It may also describe ownership of resources, confidentiality aspects, and conditions for proper release of data (if any). A MOU may also specify the responsibilities of the parties coordinating the data collection, and any fees associated with collecting, compiling, and transmitting data. The document may also specify any timelines to be met.

A MOU is a common synonym for a letter of intent (LOI).

### Sample Memoranda of Understanding

Several examples can be found at:

<http://www.state.gov/r/pa/prs/ps/2007/mar/82496.htm>

<http://www.uscis.gov/files/nativedocuments/mou.pdf>

<http://www.uscis.gov/files/article/mou.pdf>

## Sample Agreements

### *Employee Acceptable Data Usage Statement*

I acknowledge that [name of organization]’s data usage policies, guidelines, and procedures have been made available to me for adequate review and consideration. I also certify that I have been adequately trained in the application of these requirements and given ample opportunity to have any and all questions about my responsibilities addressed. I am aware that I am accountable for all data usage policies, guidelines, and procedures that apply to my tasks at the organization. Moreover, I agree to use data in an appropriate and ethical manner as required by the organization’s data usage policies, guidelines, and procedures. I understand that failure to abide by any and all policies, guidelines, and procedures can result in organizational, civil, or criminal action; and/or the termination of my employment.

Signature: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Job Title: \_\_\_\_\_

Date: \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_

### *Contractor/Consultant/Outsider Acceptable Data Usage Statement*

I acknowledge that [name of organization] has provided me with adequate time to review and consider the data usage policies, guidelines, and procedures it deems applicable to responsibilities I am undertaking on its behalf, regardless of my employment status. I am aware that I am accountable for all data usage policies, guidelines, and procedures that apply to my tasks at the organization. Moreover, I agree to use data in an appropriate and ethical manner as required by the organization’s data usage policies, guidelines, and procedures. I understand that failure to abide by any and all policies, guidelines, and procedures can result in organizational, civil, or criminal action; and/or the termination of my relationship with [name of organization].

Signature: \_\_\_\_\_

Printed Name: \_\_\_\_\_

Affiliation: \_\_\_\_\_

Date: \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_

## APPENDIX D

# FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)

Many states and localities have enacted laws and regulations to protect a student's right to privacy. So, too, has the federal government, in the form of the Family Educational Rights and Privacy Act of 1974 (FERPA), which guarantees the privacy of educational records for students and their parents; the Education Sciences Reform Act of 2002 (ESRA); the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA); the Freedom of Information Act (FOIA); the Paperwork Reduction Act of 1995; and the Computer Security Act of 1987. In addition, the federal Health Insurance Portability and Accountability Act (HIPAA) established standards regarding the electronic exchange of health information. Certain activities performed by school staff, including school nurses, may be subject to provisions of HIPAA. For more information about the intersection of FERPA and HIPAA, see *Health and Healthcare in Schools*, The Impact of FERPA and HIPAA on Privacy Protections for Health Information at School: Questions from Readers (2003, Volume 4, Number 4).

This is a summary of the federal Family Educational Rights and Privacy Act (FERPA). Visit <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html> for more information.

## Family Educational Rights and Privacy Act (FERPA)

Statute: 20 U.S.C. § 1232g. Regulations: 34 CFR Part 99.

### I. FERPA General Overview

The Family Educational Rights and Privacy Act (FERPA) is a federal law that protects the privacy of student education records. 20 U.S.C 1232g; 34 CFR part 99. FERPA applies to all schools that receive funds from the U.S. Department of Education. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification is left to the discretion of each school.

Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions:

- ▶ school officials with legitimate educational interest;
- ▶ other schools to which a student is transferring;
- ▶ specified officials for audit or evaluation purposes;
- ▶ appropriate parties in connection with financial aid to a student;
- ▶ organizations conducting certain studies for, or on behalf, of the schools;
- ▶ accrediting organizations;
- ▶ to comply with a judicial order or lawfully issued subpoena;
- ▶ appropriate officials in cases of health and safety emergencies; and

- ▶ state and local authorities within a juvenile justice system, pursuant to specific state law. 34 CFR 99.31

FERPA confers rights to parents with respect to their children's education records. Local education agencies (LEAs) must annually notify parents and eligible students of their rights under FERPA. 34 CFR § 99.7. Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Parents or eligible students have the right to request that schools correct records they believe to be inaccurate or misleading.

## **II. Balancing the Interests of Privacy and Safety**

School officials are asked to balance the interests of safety and privacy for individual students. The U.S. Department of Education issued a guide pertaining to the safety issue in October of 2007. The provisions follow below:

### *A. Health or Safety Emergency*

In an emergency, FERPA permits school officials to disclose without consent education records, including personally identifiable records, to protect the health or safety of students or other individuals. In a health or safety emergency, records and information may be released to appropriate parties such as law enforcement officials, public health officials, and trained medical personnel. 34 CFR 99.31(a)(10) and 99.36. This exception is limited to the period of the emergency.

### *B. Law Enforcement Unit Records*

Many school districts employ security staff to monitor safety and security in and around schools. Investigative reports and other records created and maintained by these "law enforcement units" are not considered "education records" subject to FERPA. Schools may disclose information from the law enforcement unit records to anyone, including outside law enforcement authorities, without parental consent. 34 CFR 99.8.

Schools must indicate which office serves as the school's law enforcement unit. As an example, the U.S. Department of Education has posted a model notification at <http://www.ed.gov/policy/gen/gui/fpcoferpa/lea-officials.html>.

### *C. Security Videos*

Images of students captured on security videotapes maintained by school law enforcement units are not considered education records under FERPA.

According to the U.S. Department of Education, schools that do not have a designated law enforcement unit might consider designating an employee to serve as the "law enforcement unit," in order to maintain the security camera(s) and determine the appropriate circumstances in which the school would disclose recorded images.

### *D. Personal Knowledge*

FERPA does not prohibit a school official from disclosing information about a student if the information is obtained through the school official's knowledge or observation, and not from the student's education records. For example, if an official overhears a student making threatening remarks to other students, FERPA does not protect that information.



### *E. Transfer of Education Records*

School officials may disclose any and all education records, including disciplinary records and records that were created as a result of a student receiving special education services under part B of the Individuals with Disabilities Act, to another school or secondary institution at which the student seeks or intends to enroll. Schools must make a reasonable attempt to disclose that the information transfer has occurred, which can be part of the school's annual FERPA notification. Parents can request a copy of information disclosed, and they have an opportunity for a hearing.

### *F. Directory Information*

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow them a reasonable amount of time to request that the school not disclose directory information about them.

## **III. Protection of Pupil Rights Amendment**

The Protection of Pupil Rights Amendment (PPRA) affords parents certain rights regarding the conduct of surveys, collection and use of information for marketing purposes, and certain physical exams.<sup>1</sup> 20 U.S.C. § 1232h; 34 CFR Part 98. Parents or eligible students have the right to consent before students are required to complete a survey; receive notice and the opportunity to opt out; and inspect protected information. PPRA also requires written parental consent if a survey includes questions on the list of prohibited topics.

## **IV. Recordkeeping Requirements**

FERPA also requires that educational organizations maintain a record of each request for access to and each disclosure of personally identifiable information from the education records of each student (as long as a student's educational records are maintained by the education agency or institution). For each request or disclosure the record must include

- i) the parties who have requested or received personally identifiable information from the education records; and
- ii) the legitimate interests the parties had in requesting or obtaining the information.

---

<sup>1</sup>PPRA governs the administration to students of a survey, analysis, or evaluation that concerns one or more of the following eight protected areas:

- ▶ political affiliations or beliefs of the student or the student's parent;
- ▶ mental or psychological problems of the student or the student's family;
- ▶ sex behavior or attitudes;
- ▶ illegal, antisocial, self-incriminating, or demeaning behavior;
- ▶ critical appraisals of other individuals with whom respondents have close family relationships;
- ▶ legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;
- ▶ religious practices, affiliations, or beliefs of the student or student's parent; or
- ▶ income (other than that required by law to determine eligibility for participation in a program, or for receiving financial assistance under such program).

If the personally identifiable information is disclosed, the educational agency or institution must document

- 1) the names of any additional parties to which the receiving party may disclose the information on behalf of the educational agency or institution; and
- 2) the legitimate interests under FERPA 99.31 which each of the additional parties has in requesting or obtaining the information.

This does not apply if the request was from, or the disclosure was to

- 1) the parent or eligible student;
- 2) a school official under 99.31(a)(1);
- 3) a party with written consent from the parent or eligible student;
- 4) a party seeking directory information; or
- 5) a party seeking or receiving the records as directed by a Federal grand jury or other law enforcement subpoena, and the issuing court or other issuing agency has ordered that the existence or the contents of the subpoena or the information furnished in response to the subpoena not be disclosed.

## **V. Contact Information**

U.S. Department of Education  
Family Policy Compliance Office (FPCO)  
400 Maryland Avenue, SW  
Washington, DC 20202-5920  
(202) 260-3887

Informal inquiries may be sent to FPCO via the following email addresses: [ferpa@ed.gov](mailto:ferpa@ed.gov) and [ppra@ed.gov](mailto:ppra@ed.gov). The FPCO website address is: [www.ed.gov/policy/gen/guid/fpcoc](http://www.ed.gov/policy/gen/guid/fpcoc).

