Forum Guide to Staff Records

National Forum on Education Statistics

Forum Guide to
Staff Records

National
Forum
on Education
Statistics

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, 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 (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 NCES, the Institute of Education Sciences, or the U.S. Department of Education.

August 2021

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

The NCES Home Page address is http://nces.ed.gov

The NCES Publications and Products address is http://nces.ed.gov/pubsearch

The Forum Home Page address is http://nces.ed.gov/forum

This publication was prepared in part under Contract No. ED-IES-16-Q-0009 with Quality Information Partners, Inc. Mention of trade names, commercial products, or organizations does not imply endorsement by the U.S. government.

Suggested Citation

National Forum on Education Statistics. (2021). *Forum Guide to Staff Records* (NFES 2021094). U.S. Department of Education. Washington, DC: National Center for Education Statistics.

Technical Contact

Ghedam Bairu

(202) 245-6644

ghedam.bairu@ed.gov

Foreword

The National Forum on Education Statistics (Forum) is pleased to present the *Forum Guide to Staff Records*. The purpose of this resource is to help education agencies effectively collect, manage, utilize, and dispose of staff data; protect the privacy of these data; and ensure that requests for data access and data releases are managed appropriately. It introduces key concepts and discusses best practices drawn from the experiences of state education agencies (SEAs) and local education agencies (LEAs). Importantly, laws about maintenance and release of public records vary among states, and this resource does not provide legal guidelines.

Publication Objectives

In 2000, the Forum addressed the need among schools, LEAs, and SEAs for information about managing requests for information contained in staff records with the publication of *Privacy Issues in Education Staff Records: Guidelines for Education Agencies*. This new publication updates and expands information originally published in the 2000 document. It includes updated best practices for collecting, maintaining, and managing access to staff records, as well as case studies from SEAs and LEAs.

Intended Audience

This resource is intended primarily for staff in education agencies who are responsible for employee data. It also may be of use to other stakeholders, such as researchers, staff members who approve research proposals, vendors who work with staff data, and staff members who have an interest in knowing how their data are managed.

Organization of This Resource

This resource includes the following chapters and appendices:

- **Chapter 1: Overview of Staff Records** defines staff records, describes types of staff records and the levels of data contained in them, and marks the distinction between official and secondary records.
- **Chapter 2: Staff Records Collection and Management** discusses the ways in which staff and student data intersect, as well as best practices related to data governance, data quality, data standards, and disposal of staff records.
- **Chapter 3: Access to and Release of Staff Records** provides information about managing access to staff records within the agency, as well as evaluating and responding to external requests for staff records, including public records and FOIA requests.
- **Chapter 4: Case Studies** provides real-world information on practices used for effective staff records management in SEAs and LEAs.
- The **Appendices** provide information about relevant laws and examples of an LEA's acceptable use forms.

National Forum on Education Statistics

The work of the National Forum on Education Statistics (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 education 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 Institute of Education Sciences (IES)—a part of the U.S. Department of Education (ED)—established the Forum to improve the collection, reporting, and use of elementary and secondary education statistics. The Forum includes approximately 120 representatives from state and local education agencies, the federal government, and other organizations with an interest in education data. 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 working groups to develop guides in data-related areas of interest to federal, state, and local education agencies. They are assisted in this work by NCES, but the content comes from the collective experience of working group members who review all products iteratively throughout the development process. After the working group completes the content and reviews a document a final time, publications are subject to examination by members of the Forum standing committee that sponsors the project. Finally, Forum members review and formally vote to approve all documents prior to publication. NCES provides final review and approval prior to online publication. The information and opinions published in Forum products do not necessarily represent the policies or views of ED, IES, or NCES. Readers may modify, customize, or reproduce any or all parts of this document.

Working Group Members

This online publication was developed through the National Cooperative Education Statistics System and funded by the National Center for Education Statistics (NCES) within the Institute of Education Sciences (IES)–a part of the U.S. Department of Education (ED). The Staff Records Working Group of the National Forum on Education Statistics is responsible for the content.

Chair

Dawn Gessel*, Putnam County Schools (WV)

Members

Shuwan Chiu*, Illinois State Board of Education

DeDe Conner, Kentucky Department of Education

Larry Fruth II, Access 4 Learning

Marilyn King, Bozeman School District #7 (MT)

John Lindner*, South Washington County Schools (MN)

Raymond Martin*, Connecticut State Department of Education

Zenaida Napa Natividad, Guam Department of Education

Lee Rabbitt*, Pawtucket School Department (RI)

Annette Severson*, Colorado Department of Education

Cheryl L. VanNoy, Saint Louis Public Schools (MO)

Project Officer

Ghedam Bairu, National Center for Education Statistics

Consultants

Kristina Dunman and Andrew Scott Pyle, Quality Information Partners

* Working group members marked with an asterisk also contributed case studies and/or real-world examples to this guide.

Acknowledgments

Members of the Staff Records Working Group would like to thank everyone who reviewed or otherwise contributed to the development of the *Forum Guide to Staff Records*, including the following case study and real-world example contributors:

Case Study and Real-World Example Contributors

Mark Hobneck, Illinois State Board of Education

Allen Miedema, Northshore School District (WA)

Mary Rose, Ohio Department of Education

Contents

Glossary of Common Terms

Acceptable Use Policy (AUP). This is a document that defines the ways in which an individual may and may not use an online network or website to which they have access. Schools and districts may require students, teachers, or staff to sign an AUP in order to receive login credentials.

Confidentiality. Confidentiality refers to the obligations of those who receive personal information about an individual to respect the individual's privacy by safeguarding the information.[1]

Custodian. (see **Records Official**)

Data Breach. A data breach is the intentional or unintentional release of secure information to an untrusted environment.[2]

Data Destruction. Data destruction is the process of removing information in a way that renders it unreadable (for paper records) or irretrievable (for digital records).

Data Governance. Data governance includes establishing responsibility for individual data elements, datasets, and databases, and continuously improving data systems through the institutionalized development and enforcement of policies, roles, responsibilities, and procedures. Data governance identifies master data sources (authoritative data sources) and defines responsibilities for accessing and maintaining these data in order to safeguard the quality, integrity, privacy, and security of data.

Data Security. Data security is the means of ensuring that data are kept safe from corruption and that access to data is suitably controlled. The primary goal of any information and technology security system is to protect information and system equipment without unnecessarily limiting access to authorized users and functions.[3]

Data Steward. A data steward is an individual (or individuals) responsible for ensuring the quality of statistical information generated by an organization. Data stewards also generally assume responsibility for enhancing the information reporting process through staff development and by sharing data expertise with the various offices and programs that produce data and information in an organization.[4] For more information on data stewardship and ownership, please consult the *Forum Guide to Data Governance* (https://nces.ed.gov/forum/pub_2020083.asp).

Direct Identifier. Direct identifiers include information that relates specifically to an individual's identity, such as full name, home address, Social Security Number (SSN) or other identifying number or code, telephone number, or biometric record (fingerprints, retinal scan, dental information).[5] (see also **Indirect Identifier**)

[1] National Research Council. (2009). Protecting Student Records and Facilitating Education Research: A Workshop Summary. Washington, DC: The National Academies Press. https://doi.org/10.17226/12514. Cited in Statewide Longitudinal Data System Grant Program. (2010). SLDS Technical Brief: Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records. U.S. Department of Education. Washington, DC: National Center for Education Statistics. Retrieved December 18, 2020, from https://nces.ed.gov/pubs2011/2011601.pdf.

[2] Protecting Student Privacy (2019). "Glossary." Retrieved March 31, 2020, from https://studentprivacy.ed.gov/glossary#glossary-node-227.

[3] Protecting Student Privacy (2019). "Glossary." Retrieved March 31, 2020, from https://studentprivacy.ed.gov/glossary#glossary-node-227.

[4] *Forum Guide to Planning for, Collecting, and Managing Data About Students Displaced by a Crisis* (2019). Retrieved July 4, 2020, from https://nces.ed.gov/forum/pub_2019163.asp.

[5] Adapted from Protecting Student Privacy (2019). "Glossary." Retrieved March 31, 2020, from https://studentprivacy.ed.gov/glossary#glossary-node-227.

Disclosure. Disclosure means to permit access to or the release, transfer, or other communication of personally identifiable information (PII) by any means. Disclosure can be authorized or unauthorized, including inadvertent or accidental disclosure. An unauthorized disclosure can happen due to a data breach or loss, and an accidental disclosure can occur when data released in public aggregate reports are unintentionally presented in a manner that allows individuals to be identified.[6]

Discretionary Release. If a record is not restricted but no laws require its release, agency or school officials may decide at their *discretion* to act either way. However, the courts reserve the right to make the ultimate decision regarding the release of a requested record.

Freedom of Information Act (FOIA). Since 1967, the Freedom of Information Act (FOIA) has provided the public the right to request access to records from any federal agency. It often is described as the law that keeps citizens in the know about their government. Federal agencies are required to disclose any information requested under the FOIA unless it falls under one of nine exemptions that protect interests such as personal privacy, national security, and law enforcement.[7] Many similar laws are in force around the country at the state level.

Indirect Identifier. “Indirect identifiers” refer to information that can be combined with other information to identify specific individuals, such as, for example, a combination of gender, birth date, geographic indictor, and other descriptors. Other examples of indirect identifiers include place of birth, race, religion, weight, activities, employment information, medical information, education information, and financial information.[8] (see also **Direct Identifier**)

Mandatory or Statutory Release. If a record is subject to mandatory or statutory release, the record is considered open and available for release upon request. Such release would be mandated by federal or state laws and statutes.

Metadata. Metadata, or “data about data,” provide structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information source.[9] Metadata provide the context in which to interpret data.

Personally Identifiable Information. Personally identifiable information (PII) includes information that can be used to distinguish or trace an individual’s identify either directly or indirectly through linkages with other information.[10] (see also **Direct Identifier** and **Indirect Identifier**)

Privacy. Privacy refers to “an individual’s control over who has access to information about him or her.”[11]

[6] Protecting Student Privacy (2019). “Glossary.” Retrieved March 31, 2020, from https://studentprivacy.ed.gov/glossary#header-for-D. Note: even though the source of this definition is focused on FERPA and applies to student data, the same principles apply to staff data.

[7] https://www.foia.gov/about.html

[8] Protecting Student Privacy (2019). “Glossary.” Retrieved March 31, 2020, from https://studentprivacy.ed.gov/glossary#glossary-node-227.

[9] As defined by the National Information Standards Organization (NISO), a nonprofit association accredited by the American National Standards Institute (ANSI) to identify, develop, maintain, and publish technical standards. http://www.niso.org/publications/understanding-metadata-2017

[10] Protecting Student Privacy (2019). “Glossary.” Retrieved March 31, 2020, from https://studentprivacy.ed.gov/glossary#glossary-node-227.

[11] National Research Council. (2009). *Protecting Student Records and Facilitating Education Research: A Workshop Summary*. Washington, DC: The National Academies Press. https://doi.org/10.17226/12514. Cited in Statewide Longitudinal Data System Grant Program. (2010). *SLDS Technical Brief: Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records*. U.S. Department of Education. Washington, DC: National Center for Education Statistics. Retrieved December 18, 2020, from https://nces.ed.gov/pubs2011/2011601.pdf.

Public Agency. All states have a legal definition of a public agency. For the purposes of this guide, a public agency is a publicly funded entity according to the laws of the state. Since the public school system is funded by public funds, all public schools, districts, and state education agencies are considered public agencies. Issues discussed here are relevant to the public school systems providing education and services from pre-kindergarten to high school, as well as alternative, adult, and community education programs.

Public Record. Throughout this document, a public record is used to mean a record or file subject to public inspection under FOIA or any state-specific open records law. State laws have different definitions of public records and what information is a matter of public record.

Records Official (Custodian). Most state FOIAs require that each agency designate a "custodian" of agency records to whom requests for disclosure are made. For the purpose of this document, records official is used as a generic term referring to this custodian, or person designated by the state or local education agency (SEA or LEA), department or program head, or a school principal to have the management and operational responsibilities for staff records maintenance.

Staff Record. As used in this document, a staff record is a compilation of records, files, documents, and other materials containing information directly related to an employee of a school, LEA, or SEA. The term staff in this document includes professional and support staff; licensed or certified and non-licensed or non-certified personnel; permanent, temporary, and contracted employees; as well as salaried and non-salaried workers (volunteers).

Statutory Exemption. If an official is subject to a statutory duty not to release a piece of information, the information is considered confidential and unavailable for release. The piece of information or record is considered exempt by statute. Such protection of the record would be mandated by federal or state laws and statutes.

Chapter One:
Overview of Staff Records

Staff records are essential to the operation of education agencies. The data in staff records are used in the daily management of an education workforce—from recruitment and hiring, through placement, scheduling and payroll, to professional learning, evaluation, and separation. Data on agency staff affect decisions about human resources, funding, and other resource allocations; and they are used increasingly in education research. State and local education agencies (SEAs and LEAs) and schools are responsible for maintaining records on all staff and ensuring that the data contained in those records are of high quality. Agencies must therefore appropriately and effectively collect, manage, use, and, ultimately, dispose of staff data.

This Forum guide has been written to update and expand information included in the 2000 publication, *Privacy Issues in Education Staff Records: Guidelines for Education Agencies*. Because the means and process of collecting and managing data have changed greatly in the past 20 years, as have the volume and scope of staff data and the risks to data security, this guide augments the information contained in that earlier document with revised best practices for data collection, maintenance, and access, as well as case studies from SEAs and LEAs. As such, it is a useful resource for data collectors, managers, and other education agency staff whose work involves access to staff records data, as well as vendors, researchers, and other stakeholders who use staff records data.

Some staff information is considered to be a matter of public record, while other staff information is considered to be private, and must therefore be properly protected. Some information collected by LEAs is reported to the SEA and may be released to the public, such as aggregate information on the qualifications and education of the overall teaching force. At the same time, LEA records that are not reported to the SEA also may be a matter of public record. For example, salaries of public employees are a matter of public record—whether at a school district or at state level. However, much of the personal information collected in staff records, such as Social Security numbers (SSNs) and evaluations, typically is needed only at the local level. Education agencies are responsible for protecting the privacy of these personal data and ensuring that data collections, as well as requests for data, are conducted in compliance with all federal, state, and local laws and regulations.

Digital Record Security

Maintaining the security of digital records and communications is an indispensable practice for organizations handling student and staff data. For more information on cybersecurity best practices and setting up a policy that works, please see the *Forum Guide to Cybersecurity: Safeguarding Your Data* (https://nces.ed.gov/forum/pub_2020137.asp).

Protecting the private information in staff records is increasingly complicated. When the Forum published the original guide in 2000, staff records often were composed of paper records that could be safely stored in secure, fireproof locations or electronic files that were not connected to other systems.[12] Since the publication of that resource, numerous factors have changed the way staff records are handled, including the following:

- Computer systems are more advanced, often interconnected and interdependent, and media have evolved to match them.
- Data collections are much larger and have increasingly sensitive data within.
- Data storage media have become complex and subject to vulnerability.
- Data backups often are conducted using cloud storage.
- Demand for staff data has increased, especially to answer policy questions.
- External risks to data security have grown and diversified.

Staff Record Data Use

This resource discusses data privacy and collection. Use of staff data is beyond the scope of this document, but the Forum offers other resources about data use.

Forum Guide to Taking Action with Education Data
https://nces.ed.gov/forum/pub_2013801.asp

Traveling through Time: The Forum Guide to Longitudinal Data Systems, Book IV: Advanced LDS Usage
https://nces.ed.gov/forum/pub_2011802.asp

What is a Staff Record?

A staff record is a compilation of records, files, documents, and other materials containing information directly related to an employee of a school, LEA, or SEA. The term *staff* in this document includes professional and support staff; licensed or certified and non-licensed or non-certified personnel; permanent, temporary, and contracted employees; as well as salaried and non-salaried workers (volunteers). Unlike the information in student records, which belongs to students and their parents, many parts of staff records maintained by SEAs and LEAs are considered public records. Although these records are entrusted to the agency for use and management, the records are governed by each state's open records law and the federal Freedom of Information Act (FOIA). Staff accustomed to working with student records often find working with staff records involves fewer restrictions and less guidance.

Staff records include many different types of data that are used for many different purposes. Some of the information collected in staff records is personal, and education agencies are responsible for ensuring the privacy of these data. Staff records commonly include

- SSNs;
- demographic information;
- salary and benefits;
- residence, family members, and dependents;
- education, employment history (positions, locations, contract types, course assignments), years of experience in and out of the district or state, and evaluations;

[12] While many staff records are now electronic, some staff records are kept on paper. For example, an LEA could be required by law to keep federal tax forms on paper, or it could need a copy of a staff members' check for direct deposit.

- background checks and personnel actions (promotions, demotions, conduct investigations);
- job-relevant medical history data, such as drug testing results or vaccination records;
- professional learning history, licensure, certifications, and honors;
- attendance information, including leave history and absences;
- audio-visual material (such as security camera footage or recordings of classes or meetings);
- communications sent and received by agency-issued devices (such as laptops or smartphones);
- communications sent and received by agency-created accounts;
- automated security access logs (such as card swipes, passcode use, and others); and
- district- or school-level network activity (network ID, sign-in logs, file accession, and others).

While staff members often expect that information such as certifications, education, salary, and benefits are considered part of their staff record, they may be surprised that other, more personal data also are considered part of the staff record. For example, staff cannot always expect confidentiality of messages sent via agency email or an agency-issued device. These messages could be scrutinized by the agency or authorities. For example, if a staff member files a grievance against their supervisor, that grievance may be added to their record and the agency could compile all related emails as part of an investigation into the grievance. In special cases, investigators may require access to these communications to resolve questions or disputes.

Types of Staff Records

Staff records typically include financial data, as well as human resources data. Some staff data elements are used in association with more than one type of data. For example, a staff member's SSN typically is categorized as identity information, but it also is used in the collection of staff financial data for tax purposes.

Staff financial data include everything necessary for staff payment and accounting, such as salary, benefit, and bank account information. In addition to these data that typically are collected for all staff, many agencies find it useful to collect other types of data that may only apply to specific staff. For example, agencies may find it necessary or helpful to collect information about any payment above salary, such as a supplemental contract or stipend for a teacher who oversees the development of the school yearbook. Many of the staff financial data elements are linked to full-time equivalency (FTE); without knowing the percentage of time an educator is working, salary and benefits data cannot be compared or reported accurately. Other commonly collected data include credit for hot lunch, copies of reimbursement checks, wage garnishment information, benefits, and retirement benefits.

Linking Staff Data to Full-time Equivalency (FTE)

In Illinois, FTE salary is the basis for district salary reporting. This permits salary comparisons between districts and against the state, facilitates salary negotiations by the teachers' union, and supports evidence-based funding efforts.

Human resources data may include information about licensure and certifications, professional learning, and job performance information, as well as demographic data. Within the broad category of human resources data, agencies collect many different types of staff information, including the following:

- ***Demographic Data and Contact Information***

  Commonly collected **demographic data** include sex/gender and race/ethnicity. Other demographic data that may be collected include education level (which might be part of the staff member's professional certification) and age/birthdate (often needed for health insurance enrollment). **Contact information** collected may include telephone numbers, home addresses, other mailing addresses, fax numbers, and email addresses.

  ### Privacy and Confidentiality of Demographic Data and Contact Information

  Privacy and confidentiality statutes differ for demographic data and contact information. Contact information often is essential for the work of LEA staff, whereas demographic data are not critical. The state of Ohio stores demographic data and contact information in separate systems, with only the contact information system accessible by other systems.

  Rules regarding these data vary according to federal and state laws, agency policies, and the types of data. Some data can be shared while other data cannot, and some data can be shared only in aggregate form. For example, the data element "home address" is handled differently among agencies. In some states, home addresses may not be shareable, but states may use address data for state-level analysis. For example, information about teachers living inside and outside the districts where they teach can be used for such analysis as examining whether teachers can afford to live in the school districts in which they teach.

- ***Identity Information***

  Human resources commonly collect basic identifying information, such as an individual's name, and also may collect further information of a more personal nature, including past names, SSNs, photographs, biometric data (such as fingerprints, retinal scans), and public social media profiles. The levels of security around access to these data are variable, with SSNs and biometric data only released in extenuating legal circumstances. For example, a staff SSN may be shared with the Internal Revenue Service for tax preparation, with insurance providers, or under a court order. Public social media profiles, however, may be held to the same security standard as contact information. Social media users generally have the option to limit access to their profiles.

- ***Licensure and Certification Data***

  ### Managing Access to Licensure Data

  In some states, such as Ohio and West Virginia, licenses for all school personnel are issued by the SEA and therefore are stored in one place, making it easier to manage access.

  Many staff members must maintain licensure and certification according to state laws. These records may be regionalized, and they usually are maintained in a separate, off-site location by the state's certification or licensing authority. State licensure databases may include additional information, such as home address and employment and academic history, tests and assessment results, investigation history, hearings held, license revocation information, and criminal records. Staff member licenses to be recorded go beyond teacher certifications. Included in these data are certifications for school nurses, mental health workers, speech therapists, social workers, resource officers, and other professionals working outside the classroom. Agency or school officials are advised to examine their state's licensing or certification laws to determine which data need to be stored, which are subject to statutory release upon request, and which are protected from release by specific statutory exemptions.

- ***Staff Assignments***

  Staff records often include specific information about the role the staff member holds in the organization. These roles can be instructional or support and may require certification or not. For teachers, these data could include assignments, such as what courses or classes that staff member is assigned and what role that staff member has for that course. For example, a staff member might be a lead teacher primarily responsible for teaching students in the class. Other categories of assignment could include team teacher, who shares responsibility for teaching students, or a contributing professional providing support for teachers or students in the classroom.[13]

  ### Educator Pipelines

  Licensure and certification data, staff assignments, and staff education records play a vital role in assessing a state or district's educator pipeline. These data build a picture of where different areas of expertise are found within an education agency, allowing educators to be assigned effectively and showing where new hires are needed.

- ***Staff Education Records***

  Agencies also collect data about staff members' education (outside of state licensure databases). Such data might include the highest level of education completed, the names of institutions where staff members received degrees, degree or certificate title and type, higher education institution accreditation status, entry and withdrawal dates, dates any degree was conferred, the number of credit hours taken, and the method used to verify the employee's education.[14] Staff education records increasingly include skill achievement measures like new or enhanced certifications, leading to some overlap with professional learning (discussed below).

- ***Attendance Data***

  Staff attendance data and, more specifically, teacher attendance data are gaining attention as agencies aim to measure the time students are taught by substitute teachers or other staff members apart from their teacher of record. Many SEAs have begun reporting aggregate measures of staff attendance on state report cards. Agencies differ in how they collect and define attendance data. For example, agencies must determine whether a staff member on leave for maternity or military service is considered absent. Other debates around absences include whether to count time away from the classroom for professional learning as an absence.

  It is best practice for attendance data to be disaggregated by reason code at the LEA level. For example, it is useful to be able to note the difference between a teacher who is excused from the classroom for required professional learning and a teacher

[13] Common Education Data Standards (CEDS). Retrieved March 31, 2020, from https://ceds.ed.gov/domainEntitySchema.aspx?v=8&ex=Draft.

[14] Common Education Data Standards (CEDS). Retrieved March 31, 2020, from https://ceds.ed.gov/domainEntitySchema.aspx?v=8&ex=Draft.

who is absent due to illness. In addition to tracking teacher absences, educational agencies increasingly track how absences were covered (for example, whether the class was covered by a substitute with proper certification for teaching the subject). Some agencies also find it useful to track attendance by level; for example, differentiating between teacher, office staff, and administrator attendance, or between attendance for employees with 10-month and 12-month contracts.

- ***Evaluations***

  Job performance data typically are collected on all staff members for regular performance reviews and included in staff records. Teacher evaluations also may include data from observations, and teacher evaluations may be linked with student data, such as test scores. In some states, LEAs are required to report teacher evaluation data to the SEA, while in other states these data are kept locally. To inform and improve teacher preparation programs, some states, such as Colorado, share teacher evaluation data with higher education institutions in the state to inform and improve teacher preparation programs.[15]

  LEAs benefit from developing policies governing what types of evaluation data can be disposed of and what data must be maintained. For example, some agencies may consider a principal's observation notes as part of a "working file" that is disposed of after the principal provides feedback.

- ***Medical Information***

  Education agencies may collect medical data that have an impact on an employee's ability to perform their job, such as information on medical leave, drug testing, vaccinations/immunizations, or requests for disability accommodations. While employers may not be subject to the Health Insurance Portability and Accountability Act (HIPAA),[16] a conscientious employer's best practice is to treat this type of sensitive data with increased care.

- ***Disciplinary Data***

  Disciplinary data often are considered sensitive, and requirements for what data LEAs must retain, how long to retain them, and whether or not they are reported to the SEA typically are set by state policies. Reporting requirements may vary according to the severity of the action. For example, some LEAs are required to report to the SEA if they put an employee on administrative leave. However, data related to progressive discipline might be kept locally and disposed of after a period of time. For example, if a teacher regularly arrives late, then the LEA may require that the principal document a conversation with the teacher and retain the record of that conversation for a year, after which the record can be destroyed. Sometimes agencies are asked for disciplinary data on former employees. Best practice suggests providing only basic information that is available under open records laws, such as dates of employment and licensure information, and to refer requests for additional information to agency lawyers.

[15] Colorado Department of Education Educator Preparation Programs Report. Retrieved March 31, 2020 from https://www.cde.state.co.us/educatortalent/edprepprogram-report.

[16] U.S. Department of Health & Human Services (2004). "As an employer, I sponsor a group health plan for my employees. Am I a covered entity under HIPAA?" Retrieved March 31, 2020, from https://www.hhs.gov/hipaa/for-professionals/faq/499/am-i-a-covered-entity-under-hipaa/index.html.

- ***Professional Learning***

  LEAs and teachers must often track teacher professional learning. Some agencies use systems that integrate required training with a method for tracking staff completion. These systems reduce paperwork because staff do not need to submit proof that they have completed professional learning. Integrated training systems also make it easy for staff to review the training they have completed and see what requirements remain. Many agencies include their professional learning policies in the system so that they are easily accessible.

  ### Data Governance

  Data governance is a matter of core importance for SEAs and LEAs in keeping staff records secure. Within each agency, data governance roles and responsibilities may differ, but the key purpose is to provide a formal and comprehensive set of policies and practices designed to ensure the effective management of data within an organization. Data governance encourages robust data security, definition, collection, access, quality, and disposal. For more information, please consult the *Forum Guide to Data Governance*: https://nces.ed.gov/forum/pub_2020083.asp.

  Types of professional learning tracked and recorded may include

  - ○ courses taken to build on existing certifications;
  - ○ new certifications obtained;
  - ○ staff awards and honors;
  - ○ mandatory medical or survival training (CPR, emergency medical administration, drownproofing);
  - ○ computer/information technology (IT) training (cybersecurity, digital safety, and digital literacy);
  - ○ mandatory mental health or social responsibility; and
  - ○ awareness of and duty to report suspected or potential child abuse, endangerment, or neglect.

Levels of Data

Schools, LEAs, and SEAs each have different needs related to staff data, and therefore the amount of data collected, reported, and maintained varies at each level. Staff data in an LEA may include both building-level data and central office data. LEAs often have personnel record data that they do not provide to the SEA because those data are intended to support operations at the LEA level. For example, certain medical information relevant at the building level (such as vaccinations and drug tests) would not be relevant to the SEA's needs and therefore would not be reported to the SEA. Other information collected by the LEA but not reported to the SEA might include staff bank account information for direct deposit, leave history (such as sick or family leave), or security footage.

The collection of staff data also may differ among types of staff. For example, teacher certification data are important at both the SEA and LEA levels, but professional certification information for custodial staff might not be required at the state level.

Official and Secondary Records

Staff records often are used and housed in different systems. For example, staff data may be used in a state retirement system, a student information system, and an employee information system. It is important to have an authoritative source for each type of data so that there is a clear answer when discrepancies arise between systems. For example, in this kind of system, when teachers change their names or addresses, entering the new information in one system or portal will be sufficient to record this information across all systems that use those data.

Establishing a Single Source for Staff Data

Some states, such as Ohio and Connecticut, maintain a central directory database for staff data, including personally identifiable information (PII). Multiple state-supported apps connect to this database, so staff information must be entered and stored only once.

Some agencies find that it is useful to distinguish between official records and secondary records. Official records are considered the authoritative source for specific data. The state of Montana defines an official record as "The record or set of records that need to be retained due to their ongoing administrative, legal, financial and historic values, not necessarily an original. By law, an official record has the legally recognized and enforceable quality of establishing some fact." Montana defines a secondary record as "a duplicate record or set of records, generated by another agency or user who, as the originator, has the responsibility for retaining the official 'record copy,' and if the secondary copy has no business value to the receiving party, the record(s) is a duplicate copy and subject to deletion at will."[17]

[17] Montana Secretary of State. (n.d.) "Glossary of Records Management Terms." Retrieved December 18, 2020, from https://sosmt.gov/records/glossary/.

Chapter Two:
Staff Records Collection and Management

A sound and efficient data collection effort includes clearly defined parameters for which data are to be collected, why these data are needed, and how the data will be managed, protected, reported, and destroyed. Laws and policies at the levels of the local education agency (LEA), state education agency (SEA), and the federal government provide guidance on which data are required. However, SEAs, LEAs, and individual schools may collect data beyond these requirements, to meet their agency's needs.

Interface Between Staff and Student Data

Best Practices for Making Decisions about Defining Staff Data

✓ Follow all federal and state laws and agency policies that address staff data.

✓ Ensure that all vendor contracts or agreements that pertain to data sharing include data privacy agreements, or are augmented with memoranda of understanding (MOUs) protecting data privacy.

✓ Designate a staff member or committee to ensure that best practices are followed and updated as needed.

✓ Determine what types of data are needed at all levels (school, LEA, and SEA) and for different types or levels of staff.

✓ Identify types of data needed for reporting and analysis, including federal reporting.

✓ Identify and define official and secondary records and document their location.

Agencies link staff and student data for many different purposes. Such links help with logistical decisions, such as determining the distribution of class supplies and assessments, or how many textbooks or computers are needed in each classroom based on course enrollment. Staff and student data are commonly linked in online grading systems and may be linked in professional learning software. This type of software examines the outcomes of classes and then suggests professional learning to the teacher based on student performance. Linked data also can help to answer questions about education equity, such as the number of students taught by out-of-field, ineffective, or inexperienced teachers. Staff and student data also are linked often to determine or support evaluation factors–for example, in some states, teacher evaluations include information on student assessments or student discipline data.[18]

[18] *Forum Guide to the Teacher-Student Data Link: A Technical Implementation Resource*. Retrieved March 31, 2020, from https://nces.ed.gov/forum/pub_2013802.asp.

Given the sensitivity of student data, role-based access is a strongly recommended feature of any systems linking staff and student data. Stringent privacy and security measures are necessary to ensure that staff only are able to view data that are relevant to their needs and that student data are protected according to the requirements of federal, state, and local laws and regulations.[19]

Data Retention and Disposal

State laws usually specify schedules for document retention, and agencies can face penalties for not maintaining records as required. For example, in Montana, the schedule is set by the Montana Secretary of State.[20] If not already specified in state law and regulations, a best practice for agencies is to establish policies regarding how long each type of data will be maintained in the staff records, how often data will be updated, and how data are to be destroyed when they are no longer needed or required. Such data disposal policies are to be agreed upon and fixed before any data are provided.

In some cases, it is necessary or appropriate to maintain records beyond the minimum required time. Common scenarios include the need to retain data for a retiree who receives a pension or for a former staff member who left or retired but who may return. It also is good practice for agencies to retain sufficient data to verify employment history for someone who no longer works for the agency, but it is important to keep only the necessary data.

Some agencies will engage with vendors to assist in managing and utilizing staff records. Occasionally, an agency may face a situation in which the vendor who has the agency's records has changed. It is important that the contract between an agency and a vendor have language specifying what happens to the shared records when the cooperative arrangement ends. In cases where the vendor contract does not contain language governing data disposal or when the agency or vendor feels the language is insufficient, a best practice for an agency is to have a Memorandum of Understanding (MOU) specifying what happens when the working relationship is terminated.[21]

Considerations for developing data disposal policies include the following:

- Any personally identifiable information (PII) pulled from staff records that are held by vendors or researchers is to be destroyed after the contract or project is completed.
- Disposal of paper records begins with shredding.
- Effective disposal policies ensure thorough deletion of all expunged digital files, including copies and backups stored in different locations. Many existing laws and policies were written for paper records and may not apply to digital records. Erasing digital files from the system where they are stored may not be sufficient because digital files often are saved on backup systems.[22]
- Comprehensive disposal policies address how to manage requests for destruction of records.

[19] Additional information on protecting student data privacy is available in the F*orum Guide to Education Data Privacy* (https://nces.ed.gov/forum/pub_2016096.asp) and through the U.S. Department of Education's Privacy Technical Assistance Center, or PTAC and Student Privacy Policy Office (https://studentprivacy.ed.gov/).

[20] Montana Secretary of State. (n.d.) Retention Schedules. Retrieved December 18, 2020, from https://sosmt.gov/records/toolkit/rim-retention/.

[21] *The Forum Guide to Supporting Data Access for Researchers: A Local Education Agency Perspective*, available at https://nces.ed.gov/forum/pub_2014801.asp, includes a Data Destruction Certification Form. See Appendix J, page 79.

[22] For more information, see the U.S. Department of Education's Privacy Technical Assistance Center (PTAC) publication, *Best Practices for Data Destruction*, available at https://studentprivacy.ed.gov/resources/best-practices-data-destruction.

Because some methods of data destruction are more complicated, time-consuming, or resource-intensive than others, the method selected is determined by the underlying sensitivity of the data being destroyed or the potential harm they could cause if they are recovered or inadvertently disclosed. For very low-risk information, this may mean deleting electronic files or using a desk shredder for paper documents. However, these destruction methods can be undone by a determined and motivated individual, making these methods inappropriate for more sensitive data. For more sensitive data, stronger methods of destruction at a more granular level would ensure that the data are truly irretrievable.[23]

Interoperability with Standards

Data standards allow data to transfer across systems and agencies. Within each state, elements such as an individual identification (ID) code help to coordinate data on individuals across different systems. For example, standard IDs allow human resources (HR) systems and student information systems (SISs) to align teachers with the courses they are endorsed to teach. While some states create new codes for each teacher, others use existing licensure numbers. In other states, such as Rhode Island, students in the state who later become teachers in the state can retain their student ID as their teacher ID.

Common Education Data Standards (CEDS): Standard K12 Staff Data Elements

CEDS is an education data management initiative designed to streamline the understanding of data within and across P-20W institutions and sectors. The CEDS initiative includes a common vocabulary, data models that reflect that vocabulary, tools to help education stakeholders understand and use education data, an assembly of metadata from other education data initiatives, and a community of education stakeholders who discuss the uses of CEDS and the development of the standard. Within the CEDS Domain Entity Schema (https://ceds.ed.gov/domainEntitySchema.aspx), the K12 section includes a section of standard K12 staff elements. For more information about CEDS, visit ceds.ed.gov.

States with systems that still rely on Social Security numbers (SSNs) find transferring data between systems more cumbersome. For example, some state retirement systems use SSNs while the SEA's staff data system has switched to individual IDs. To transfer data from the staff data system to the retirement system, such SEAs must rely on a third system, such as the certification system, to re-match the individual's SSN with their ID. In this case, data quality and security are crucial: Any errors in the SSN, state ID, or licensure number can impact an individual's retirement, and a data breach could expose the individual's SSN.

Data Quality

It is useful to consider data quality whenever staff data are collected. Regular reviews of existing data collections are strengthened by including procedures for checking the quality of the data. In addition, when deciding whether to conduct new collections or add new information to staff records, it is a good practice to revisit the question of why the data are needed and also determine the possibility of collecting good quality data. Key considerations for determining if data are high quality include:

Data Quality

Data quality tends to improve when collectors and respondents understand the value of the data. Indicators of high-quality data include

- a legal requirement to collect;
- a reward or penalty associated with collection;
- public reporting and usage; and
- time dedicated to the collection.

[23] Protecting Student Privacy (2019). *Best Practices for Data Destruction*. Retrieved December 18, 2020, from https://studentprivacy.ed.gov/resources/best-practices-data-destruction.

- **Accuracy.** Is the information available correct and complete? Data entry procedures and data checks must be reliable to ensure that a report will have the same information regardless of who fills it out.
- **Security.** Can the agency ensure the confidentiality of staff records and be certain that data are safe (for example, protected from potential data breaches)?
- **Utility.** Can the data be used to provide the right information to answer the question that is asked?
- **Timeliness.** Are deadlines followed and are data entered in a timely manner so the data can inform strategic decisionmaking and prompt action?[24]

Data Quality

The Forum has developed several resources to help agencies improve the quality of education data, including

Forum Guide to Building a Culture of Quality Data: A School and District Resource
https://nces.ed.gov/forum/pub_2005801.asp

Forum Curriculum for Improving Education Data: A Resource for Local Education Agencies
https://nces.ed.gov/forum/pub_2007808.asp

Data Quality Online Courses:

- Improving Education Data Part 1 https://nces.ed.gov/forum/dataqualitycourse/dataquality.asp
- Improving Education Data Part 2 https://nces.ed.gov/forum/dataqualitycourse/dataquality.asp#course2

Best Practices for Staff Data Collection and Management

Collect only the necessary data. State laws and board of education policies contain specific requirements for information that must be collected and maintained. Prioritize data for which there is a demonstrated need–if a piece of information is not specifically required by law or regulation, it is critical to ask: “Why does the agency need this information?” Some of the reasons to ask such a question include:

- data collection requires budgeting of time, money, and human resources, which are limited;
- a focus on necessary data only increases the likelihood of gathering high-quality data; and
- an agency curbs the risks to staff members’ privacy when an agency limits the range of its data collection.

Consider ways to minimize data stored by the agency. The collection and maintenance of licensure and certification information often are mandated by law. If an agency is developing a licensure or certification database at the state level, the state licensure laws or board policies will outline the types of data required. Within this context, agencies can determine exactly how much information to maintain in order to meet the statutory requirement without collecting unneeded data. For example, if state laws require that a teacher pass a certain test to be certified, the SEA may decide to collect the pass/fail indicator from the testing authority rather than the exact score received. This allows the agency to collect and maintain the information

[24] *Forum Guide to Data Governance*. Retrieved March 31, 2020, from https://nces.ed.gov/forum/pub_2020083.asp.

needed while still minimizing the amount of data collected and protecting the privacy interests of the teachers.

Review staff data collections at regular intervals to ensure that the SEA is not requiring data collections that are no longer needed and, in turn, that the LEA is not collecting unneeded or unrequired data. Such reviews may result in deleting specific data fields and retiring obsolete collections. These actions must be approached and considered carefully because data that are no longer needed by one agency office or program may be critical to another. To reduce the risk of eliminating data that are needed, all stakeholders are advised to review data elements that are under consideration for deletion and agree on them before action is taken.

Train staff who work with staff data about appropriate data collection and management practices. Staff who are familiar with student data protections may be unfamiliar with whether and how similar protections apply to staff data. Training topics may include

- types of staff records;
- federal, state, and agency regulations on the use of staff records;
- cybersecurity best practices;
- federal and state open records laws;
- validity of data requests (internal and external); and
- auditing of records for preservation and disposal.

Chapter Three:
Access to and Release of Staff Records

The data included in staff records are used by both internal and external agency stakeholders. Some staff data are considered public records, under either the federal Freedom of Information Act (FOIA) or an open records law at the state level, and must be publicly reported or released upon request. Other data only can be released in aggregate reports, and some data are private and cannot be released. State and local education agencies (SEAs and LEAs) have developed best practices for evaluating and responding to requests for staff data access and managing the use of these data.

Physical Security of Staff Records

Some school districts rely on physical media for data storage (print and paper) and have yet to make the transition to electronic data. When hard-copy is the format of record, physical security measures comparable to secure logins are required. An example of a physical security measure is locked metal cabinets for records, with keys available only to approved staff members, and required sign-in/sign-out sheets for document work. See the Pawtucket, Rhode Island, case study on page 27 for information about the physical-digital conversion process for staff records.

Best Practices for Providing Internal Access and Use

Encourage staff members to verify their information. Many agencies offer data portals and other methods for staff to access their records. Staff then can verify the accuracy of the information and, if needed, request amendments or changes to correct any data they believe to be inaccurate. While agencies often can manage much of the data included in staff records within SEA and LEA systems, some information, such as certifications, may be stored outside an agency. Amendments, updates, and other changes to these data may require coordination with the agency that holds the official record.

Establish processes for making additions and changes to staff records. Clear processes for amending staff records help to ensure that data are accurate, that staff understand the requirements for making changes, and that all changes and additions are properly documented and communicated. For example, any evaluation, complaint, or suggestion requires a date and signature from the person adding the information before it may be placed in a staff record. It also is good practice to allow employees to acknowledge additions to their files and to inspect the information to be added in advance.

Determine who has a legitimate professional interest before granting access to staff records. Most agencies use strict role-based access controls to manage internal access to staff records. For example, at the SEA level in Connecticut, data collection staff have limited access to the state certification system and cannot view certain sensitive information (background checks, pending or ongoing investigations, and more). It is good practice to share these policies so that staff are aware of the guidelines for who in the agency may access their information and for what purposes. When a staff member's role changes, it is highly advisable to reassess what records they can access.

Teach and encourage staff to value data privacy and security. While role-based access controls limit who may see and edit staff data, actively protecting the privacy and security of data remains crucial. For example, staff data portals can be compromised when staff use passwords that can be guessed easily, and staff may need reminding that they cannot leave information that they are transmitting in an area where it is visible to others (whether on screens or in printouts). Staff members benefit from reminders not to share their login credentials with others. For their part, agencies benefit from training staff in common data security practices, such as the use of multi-factor authentication and strategies for preventing phishing[25], to help to ensure the security of staff data.[26] Having a data breach policy that applies to staff data is also useful.

Limiting Access to Records

Staff may need to access records in full or only in part, and a sound system will accommodate this. For instance, personnel staff may need to see an employee's degree, certifications, and years of experience to determine the appropriate pay level but have no need to access the employee's bank account information. Likewise, schools may need to know address information for preferred vendors but not tax identification information or purchase history.

Develop and require Acceptable Use Policies (AUPs). AUPs typically are used to outline staff members' responsibilities for using agency technologies. However, they also are a useful tool for clarifying to staff that information they transmit via agency devices and resources may be considered part of the staff record. In addition, AUPs can include prohibitions on sharing information about others, including other staff members, and requirements for maintaining data privacy and security. AUP examples for staff who do and do not supervise students are included in Appendices B and C.

Public Records and Freedom of Information Act (FOIA) Requests: External Access to Staff Data

A public record is a record or file subject to public inspection under FOIA or any state-specific open records law. State laws have different definitions of public records and what information is a matter of public record. Not everything included in staff records is subject to a FOIA request or other state open records law request. In addition, each state has exceptions, definitions, and practices. It can be useful to think of staff records in two categories:

Records Requests from Former Employees

The protections of the external record request process extend even to former employees themselves. For their protection, former staff must provide proof of identity even when requesting their records. If the former employee has changed names or addresses, they must prove beyond doubt that they are the same person who worked at the school previously.

- personnel records, which contain information that a district collects and keep on file for day-to-day work–these data may be as general as an employee's name, or as sensitive as Social Security numbers (SSNs) and banking information; and

[25] "Phishing" refers to the use of false communications, particularly emails or text messages, designed to compel the recipient to release private information that can be used for purposes of theft or fraud. These messages can be very convincing in appearance. For example, a scammer can mock up an email using the logo of a known bank to trick customers into releasing account information.

[26] More information on data privacy in schools is provided in *The Forum Guide to Education Data Privacy*, available at https://nces.ed.gov/forum/pub_2016096.asp. While the scenarios discussed in the Guide focus on student data, the best practices for data protection apply to staff data, as well.

- public records (also commonly called FOIA or open records), which contain information such as pay rate, licensure, and certifications that an agency may be required to release.

In addition to differentiating between personnel records and public records, agencies commonly use several other terms to differentiate between types of data that must be protected when staff data are requested, including the following:

- Personally identifiable information (PII) includes any data that could allow a requester to trace an individual staff member's identity. As such, access is generally restricted. PII consists of identifiers, both direct and indirect.
- Direct identifiers are data that reveal or disclose an individual's identity. These data include the individual's full name(s), home address, telephone number, email address, and more sensitive information (SSN, fingerprints, other biometric data).
- Indirect identifiers are data that do not make specific reference to an individual but which requesters could collect and use to deduce an individual's identity. Some examples of indirect identifiers are gender, date/place of birth, race, religion, medical/educational history, and financial information. Data suppression policies are vital in curbing the ability of indirect identifiers to compromise data security.

At the federal level, FOIA provides nine exemptions to data release. These exemptions are intended to protect personal privacy and law enforcement investigations, and federal agencies may withhold information when disclosure would harm one of the entities listed in these exemptions. Exemptions that may be relevant to education agencies include the following:[27]

Exemption 1: Information that is classified to protect national security.

Exemption 2: Information related solely to the internal personnel rules and practices of an agency.

Exemption 3: Information that is prohibited from disclosure by another federal law.

Disclosure Types

Disclosure can be authorized or unauthorized, including inadvertent or accidental disclosure. An unauthorized disclosure can happen due to a data breach or loss, and an accidental disclosure can occur when data released in public aggregate reports are unintentionally presented in a manner that allows individuals to be identified.

Exemption 4: Trade secrets or commercial or financial information that is confidential or privileged.

Exemption 5: Privileged communications within or between agencies, including those protected by the:

1. Deliberative Process Privilege (provided the records were created less than 25 years before the date on which they were requested)
2. Attorney-Work Product Privilege
3. Attorney-Client Privilege

Exemption 6: Information that, if disclosed, would invade another individual's personal privacy.

[27] FOIA Frequently Asked Questions, retrieved March 31, 2020, from https://www.foia.gov/faq.html.

Exemption 7: Information compiled for law enforcement purposes that:

- 7(A). Could reasonably be expected to interfere with enforcement proceedings
- 7(B). Would deprive a person of a right to a fair trial or an impartial adjudication
- 7(C). Could reasonably be expected to constitute an unwarranted invasion of personal privacy
- 7(D). Could reasonably be expected to disclose the identity of a confidential source
- 7(E). Would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law
- 7(F). Could reasonably be expected to endanger the life or physical safety of any individual

For more information about FOIA, visit https://www.foia.gov/.

Best Practices for Managing the Release of Staff Data Outside an Agency

Designate a custodian or records official. Under FOIA or open records laws in most states[28], a custodian or records official is designated for each public agency that maintains public records. The custodian is responsible for keeping public records accessible to the public and confidential information private. In some states, a state FOIA office performs this function. The data held by the records official are the official data.

Require that any staff who receive a records request refer the request to the records official. A consistent process for handling records requests helps a public agency avoid confusion and maintain public trust. When employees are hired by a public agency, data about the individual may be collected and stored in multiple systems and locations, including the accounting and payroll system, the retirement system, the student information system (SIS), the school principal's office, the department or program office, or the supervisor's file cabinet. Personnel who manage these different systems and work in these different offices must understand that if they receive an external request for staff records, the request is to be deferred to the designated records official. This can prevent both the unintentional disclosure of information statutorily exempt from release and the withholding of information considered public. For example, a board of education member may request access to an employee's complete file. While the board member may be provided with data that are released under FOIA or other open records laws, in most cases it would not be appropriate to provide the board member with access to the employee's complete personnel file.

Create standard request forms for staff data. Creating standardized forms for researchers and other stakeholders to use when submitting data requests can help to streamline both the request and evaluation processes. Provided that they are reviewed and approved by the relevant board or authority[29], forms help requestors provide the information the agency needs to accurately and fairly evaluate the request. Forms and processes for open records requests and research requests may differ.

[28] It is important to note that while FOIA is widely known as an instrument for public access to government documents, FOIA is only applicable to federal agencies. States may have open records acts that closely mirror FOIA, but the federal act does not confer right of access to state or local documents; these must be accessed through requests to the state or local agency's relevant body. It is best practice for these agencies to have designated authorities who perform functions analogous to a FOIA Records Official and are fully familiar with their state's requirements.

[29] Additional information on managing requests for agency data can be found in the two *Forum Guides to Supporting Data Access for Researchers*. The SEA-focused guide is available at https://nces.ed.gov/forum/pub_2012809.asp, and the companion LEA guide is available at https://nces.ed.gov/forum/pub_2014801.asp. While both of these publications focus on requests for student data, the best practices are also relevant to requests for staff data.

Some states have created web portals for data requests:

- The Illinois State Board of Education (ISBE) has created a web portal for FOIA requests (https://www.isbe.net/foia). The portal provides an overview of the request process, information on the timeline for responding to requests, frequently asked questions, and a submission area for requests. The portal helps to ensure that requests are received in a standard format and routed through a central location.
- The Kentucky Department of Education has developed a web portal for all data requests (https://education.ky.gov/districts/tech/Pages/DataRequests.aspx). It provides links to publicly available data sets and reports, electronic data request forms, and data-sharing agreement templates, including the memorandum of understanding (MOU) template for non-student data requests.

Securely transmit any non-public data that are approved for release. Once a data access request has been reviewed and approved, agencies must ensure that the data are released appropriately. Data (and relevant metadata) are to be provided in a format and medium that have been explained to the requestor. Secure delivery and transmission are essential for non-public data. The types of media used to share data are important to data security. For example, email is considered secure only when data are appropriately encrypted and otherwise protected before attachment and delivery. Similarly, the exchange of physical media, such as portable storage devices, discs, and tapes, requires transport by entities that can effectively guarantee safe and secure delivery to authenticated recipients. Traditional file transfer protocols (FTP) were not designed to be a secure mechanism for the safe movement of data, although secure FTP (SFTP) may be appropriate.[30]

Document all requests and releases. Agencies or schools are advised to maintain detailed logs of access, retrieval, or release of staff records, including the names of people retrieving records and the purposes of each release. Maintaining a record of requests that have been denied or only partially filled, as well as a list of personnel authorized to have access to the files, is good practice. Such information can be used for periodic reviews of agency confidentiality and data release policies. State statutes for reporting and notification requirements can be very specific and require careful review.

Questions to Consider when Evaluating an External Request for Staff Records

- Is your agency considered a public agency by state law?
- Is the information requested considered a public record as defined by state law, and is your agency legally required to release it?
- Who is requesting the disclosure? What is the public interest in this request?
- What is needed to meet this interest? Can it be met without releasing personal information?
- What is the specific information requested? Is this information available from other public sources?
- Is the requested information personally identifiable?
- Is it possible to release the information without identifiers or other information that will identify the individual?
- Is there a statutory exemption that applies to this request?

[30] Adapted from the *Forum Guide to Supporting Data Access for Researchers: A Local Education Agency Perspective* (https://nces.ed.gov/forum/pub_2014801.asp).

- Is this information considered confidential and generally maintained in a personnel file? Does the information contain intimate details of a highly personal nature?
- Is there a personal privacy interest? Is this interest substantial and identifiable, rather than merely speculative?
- Would disclosure constitute an unwarranted invasion of personal privacy? Would an ordinary person agree? Does this interest override that of the public purpose in knowing?
- Is there a statutory duty not to release the information under state privacy acts? Do you have an affirmative duty not to release the information?
- Will the data be handled securely and in compliance with confidentiality laws once released? Has the requestor confirmed their familiarity with these laws and agreed to comply?
- Will the agency incur any costs for copying the report? If so, can the requestor be charged?

Colorado: A Suppression Process for Staff Data

Data confidentiality concerns entail that a student information system (SIS) has a data suppression process in place for student records. If information requests reveal that certain data only apply to a small number of anonymous students, the reduced sample size makes it possible to deduce the identities of those students. Such a process is now standard for an education agency's SIS. However, similar suppression practices for staff data are less common. The Colorado Department of Education (CDE) has instituted a staff data suppression process.

CDE determined that staff data suppression guidelines were necessary to maintain data consistency across all requests, in addition to confidentiality concerns. With the student data suppression process as a model, some changes were required to adapt it for staff. For instance, in Colorado's student model, collected data are suppressed when they are found to apply to fewer than 16 students in the relevant building–because a school contains far more students than staff, the suppression threshold for staff data was reduced to five.

The process has been a success and continues to develop as the CDE team works with it. The team's data custodian was the original leader of the effort with the aim of maintaining consistency. The recent addition of a dedicated data request lead to the team indicates the volume of requests to be handled and suggests further updates and refinements to come.

Chapter Four: **Case Studies**

Illinois State Board of Education: Collecting and Leveraging High-Quality Data

The Illinois State Board of Education (ISBE) has made great strides in the past seven years regarding the collection, storage, and use of teacher data for staff records. Improvements in technology and communication strategies have allowed the ISBE to more effectively manage teacher data on a more carefully timed basis. The state education agency (SEA) is thus able to leverage these data to monitor teacher quality, assess staffing and subject matter needs, keep track of teacher certifications, and thoroughly and securely comply with federal reporting requirements.

The Need: A Comprehensive View of the State of the SEA

Until 2013, ISBE used the salary data districts provide to the Illinois Teacher Retirement System (TRS). In this way, ISBE collected employment and demographic data, as well as other relevant teacher information. When the Administrator and Teacher Salary and Benefits law came into force, new requirements for salary data meant that ISBE could no longer use the teacher salary records from TRS. An additional issue was the annual nature of the data collection–each year's data would not be finalized until the following fall, while U.S. Department of Education (ED) data submissions were required in May. Thus, ISBE had to submit data to ED in a preliminary state, before they could be checked, refined, and finalized, and resubmit the final data in the fall.

The Challenges: Data Quality, Security, and Transparency

In 2013, ISBE launched its new Employee Information System (EIS) as an ongoing live data collection system. The EIS collects data relating to 68 educator positions and allows LEAs to review and correct data from previous years. The data collected by the EIS about teachers in Illinois include:

- attendance;
- position;
- evaluations;
- base salary;
- benefits;
- working locations;
- employer;
- experience;
- grade level assignments; and
- employment contract types (full- or part-time, percent of full-time employment).

ISBE also extends its data collection efforts into the state's colleges and universities. All students pursuing post-secondary degrees in education and courses in teacher prep are tracked. This permits ISBE to fill the pipeline for coming teacher needs and shape future plans with an eye to resources that will be available.

All of these data are conveyed to the SEA for use in federal and state reports, including state report cards and reports to the governor on measures of education equity.[31] Attendance data are especially useful for understanding the available supply of teaching talent as measured against education needs in the state–this is vital for keeping teachers in positions where they can be most effective and reducing the number of unfilled positions.

To manage the security of these data, ISBE placed tight controls on access to the EIS. Access is strictly role-based, and the number of people at any level who can make changes to data is small. SEA access to the system is extremely limited, and access at the local education agency (LEA) level is determined in each district. For all information requests that come in, from within the educational system or from individuals under the Freedom of Information Act (FOIA), authorized SEA staff follow review protocols to heighten security. Every request is submitted to the SEA's legal division for a full review to determine its legitimacy. While this review is in progress, the SEA redacts the requested data to remove all sensitive information. If, and only if, the legal review deems the request legitimate, the redacted data are released.

Knowing that staff would be willing to provide data of high quality if they understood the value of those data, reasons for their collection, and the importance of their use, the SEA relied on a policy of providing transparency, accessibility, and openness regarding data collections. All data collections are based on the Illinois school code, and communications with districts regarding data collections frequently reference the school code. For example, the exact terms of what does (and does not) constitute an educator absence have been decided after close collaboration and discussion with the state teacher's union, and subsequently detailed in the state school code.[32]

Attendance data collection may move beyond teachers and educational staff in the future. The Employee Information System has the capability to track administrative attendance, as well, in the event that the state school code is modified to include that requirement.

Webinars are one way in which the Illinois State Board of Education fulfills its commitment to data education for the districts. These are made available for review as recordings (registration required) and as PDFs for download. Webinars and materials going back to fall 2018 may be found here: https://www.isbe.net/Pages/DSA-Webinars.aspx.

The SEA also provides all districts with clear and concise instructions for staff data collection, again with references and direct links to the school code, along with a data collection calendar. This highlights the established need for data while removing any guesswork from the collection process. Once collected, the SEA offers districts the ability to review and clean up their data through a data quality dashboard, with a subsequent phone call to discuss any data quality issues. The SEA also reaches out to districts with regular webinars on the collection process and provides assistance by phone and website. Staff are engaged, informed, and aware that the support of the SEA is always there.

The Results: A More Connected, More Responsive System

ISBE's implementation of the EIS has led to consistently strong engagement with LEAs throughout the state. SEA staff hold regular meetings with districts, including a standing meeting with Chicago public schools, the largest district in Illinois, and workshops with the city's charter schools. Expansions and updates to the system are planned to further refine the data collected. To bring the process full circle, the TRS has taken an interest in the data in the EIS and may begin to work with the SEA.

[31] Illinois' Educator Equity Plan may be viewed here: https://www2.ed.gov/programs/titleiparta/equitable/ilequityplan11615.pdf.

[32] The SEA makes the Illinois School Code freely available for consultation online. Please view it here: http://www.ilga.gov/legislation/ilcs/documents/010500050K10-17a.htm (105 ILCS 5/10-17a(2)(E)).

The key to these improvements has been consistent and attentive communication from all parties, in all directions. Illinois views the school code as a grounding and template for asking the state's educators how they can work together to ensure compliance with minimal burdens. In this model, data collection is a form of active listening–when LEA staff know that their messages are being received, they will continue to provide the data that bring constant improvement to the SEA.

Connecticut State Department of Education: Integrating Systems

A key to improving data management is to streamline processes in ways that reduce collection and reporting burdens while also ensuring the quality, privacy, and security of data. The Connecticut State Department of Education was able to achieve this by automating the connections between the data systems used to manage staff licensure and assignments. As a result, the SEA has improved data quality and utility, reduced burdens on LEA staff, and maintained data privacy and security.

Linking Two Systems: Staff Assignment and Certification

Teacher data at the SEA level in Connecticut are handled by two separate systems, one used for purposes of educator assignment tracking (here called the staff system) and another for keeping track of educator certifications and licensure (here the certification system). The systems are managed by different offices. Until a few years ago, the systems' linkages were behind the scenes and limited. To gain access to the joined data, SEA staff needed information technology (IT) support and to perform additional outside analyses. This made it burdensome and difficult for the SEA certification office to perform its annual certification compliance verification (an annual check that educators are working within their certification performed in December). Furthermore, if an LEA needed reporting of this kind at any other time of the year, it would have to file a special request with the SEA to receive data. This staggered process and once-yearly full output proved inefficient and frustrating to staff at both the LEA and SEA levels.

This changed for the 2013-2014 academic year, with the launch of a new staff system with greater integration with the certification system. Now, designated LEA staff can access information and generate reports on their educators when and as needed, year-round, without going through intermediaries. These reports allow LEAs to quickly identify staff working outside of their certification, as well as find potential data entry coding errors, improving data quality. In addition, the SEA provides LEAs with more reports to help with staff management, such as reports on educators who need to renew their certifications. Two banks of data have been joined, streamlined, and made available in a secure way.

Secure Identifiers

Maintaining the privacy of data subjects is paramount for any system, especially one designed for easy access. In addition to limiting this access to users who occupy certain roles in Connecticut's LEAs, the SEA's integrated system masks educator identities end to end through the flow of data. Each educator in the state is assigned a unique educator ID number. The two systems exchange information electronically by using this number in conjunction with date of birth. All of an educator's courses, activities, certifications, and service requirements are linked to this secure identifier and tracked throughout their career in the SEA.

Timely and Accurate Data

The staff system devotes a page on the site to each educator in the LEA. This enables LEAs to more effectively manage data for compliance and staffing. Authorized parties easily can

- track the key elements of a teacher's assignments, including courses taught, grades served, school served, and effective dates of this service;
- access a teacher's active certificates to ensure that teachers have the correct certifications and endorsements for the courses they are teaching;
- determine that classes are not being taught by teachers without such certifications; and
- note which teachers are certified in more than one subject area, which they potentially could teach (as an example, a French teacher who also is certified to teach Spanish).

Ensuring that all courses are taught by certified teachers is always a crucial responsibility but carries significant added weight for teachers in Connecticut–educators working outside their certification fields can lose retirement credit.

The staff system also permits LEA staff to assist teachers in keeping their certifications current. If a teacher's certificate is due to expire, the district can advise the teacher on necessary steps and deadlines, including education and professional learning.

A Smoother Process for the Future

Frequent data entry mistakes that can make their way into reports through human error are now easy to isolate and correct. For example, teaching positions may be confused with similar school positions outside the classroom and incorrectly reported. It is not uncommon for reports to mistakenly identify a psychology teacher as a licensed school psychologist, and vice versa.

After the inevitable growing pains that accompany any change in process, Connecticut has experienced improvements in data management, data accessibility, and LEA user ease of use since the introduction of the integrated system. Furthermore, the SEA continues to improve the integration of the systems to reduce data burden on LEAs and streamline its processes. In the past few years, the staff system has added modules for reporting of completion of the SEA's teacher induction system, as well as a way for LEAs to indicate if a teacher's prior year service met their standards (a key element in advancing an educator's certification). While it is still early in their use, these two new modules hold the promise of significant time savings at the LEA and SEA levels.

Ohio Department of Education: Protecting Sensitive Information with Regular Review of Access Rights

The Ohio Department of Education (ODE) manages a large volume of data from many sources, including data from public schools in more than 600 LEAs, more than 300 charter schools, and various other education institutions. These data include confidential personal information (CPI) and personally identifiable information (PII) pertaining to staff members across the state. ODE's rigorous system of checks and audits ensures that such information is accessed only by those with proper permissions and only when those individuals have a legitimate professional interest in the information.

Data managers for staff data and the Office of Educator Licensure at ODE collaborate in a regular review of access to CPI and PII in the department's data system for educator licenses. ODE developed the process in accordance with state statute, to occur on a regular timetable, without the burden of extra meetings or other unnecessary bureaucracy. Multiple offices in the agency have roles in the review process, including data managers (sometimes known as data stewards), IT staff, and staff and leadership in the Office of Educator Licensure and the Office of Professional Conduct, who are the owners of the data in the licensure system.

Legal Requirements

The Ohio law that defines confidential public information and specifies limits on its use and access, Ohio Revised Code 1347.15, defines CPI as "personal information that is not a public record," and it places requirements on the development of computer systems to protect such information, requirements to notify people when their records have been accidentally exposed to those without access rights, and requirements to review public employee access to those types of records. Ohio's Office of Budget and Management (OBM) conducts regularly scheduled audits related to this statute, along with other issues of compliance.

Process and Review

In the course of a scheduled compliance audit, Ohio's OBM advised developing a review process for employee access to sensitive information in Ohio's educator licensure database. The goal was to develop a process that would ensure that

- only appropriate staff members have access to CPI and PII stored in the database;
- the information accessed by these staff members is used solely in the execution of their professional responsibilities; and
- the list of approved staff members is kept current with staffing and access is revoked promptly when employment with ODE ends.

Tools of Review: Business Rules, Metadata, and Attestations

ODE's data managers collaborated with data owners at the department's Office of Educator Licensure to develop the review process. Together, they updated the licensure database to provide reports on metadata. These reports include the identities and roles of all employees with access to CPI and PII in staff records and all instances of employees accessing staff records outside normal business hours. In addition, recognizing that it might at times be necessary to access the database at odd hours, data owners allowed employees to memorialize their reasons for doing so by creating a form for them to sign. These metadata already are stored by data owners in the database in accordance with state statute.

Once metadata reports were ready, ODE developed the following process, to be carried out once per quarter:

- Data managers generate the metadata reports.
- Data owners check over the list of employees and revoke the access rights of any who have left the agency or who have moved to other roles within the agency that do not require such access.
- Data owners review the list of instances of after-hours access, and the relevant employees sign the form, thereby attesting that they viewed the records for professional purposes only.
- Signed attestations are reviewed and stored by the Office of Educator Licensure.

Importantly, the revocation of access for departing/transitioning staff members is not limited to this quarterly review. This occurs at the time of their exit from the position. The review process is meant as a safeguard to catch any instances that may have been missed. It ensures ODE's security around CPI and PII without burdening staff with unnecessary meetings or paperwork.

Pawtucket School Department (Rhode Island): Going Digital

The Pawtucket School Department (RI) (PSD) undertook a joint effort with the city of Pawtucket, Rhode Island, to convert all staff records to a new data system. The LEA has a longstanding relationship with the city for the management of staff records. In the past, the LEA and the city shared payroll, but human resources records were separate. With the conversion, the two entities share one comprehensive system with separate access. The conversion was necessary because the previous data system was becoming obsolete. The conversion offered the city and the LEA an opportunity to review and refine their staff records collection and maintenance processes, while also introducing a new staff portal with a dashboard for data viewing and updates. The portal enables the LEA to automatically report data to the Rhode Island Department of Education (RIDE) on a nightly basis. It also links to a public portal showing the certifications of teachers in the LEA.

Data Privacy and Quality

The new data system required the development of a comprehensive rule set to determine who would have access to the data and how that access would be limited based on data sensitivity and confidentiality. The LEA set up a system of role-based access, where the ability to add, view, and use data is determined by an individual's role in the LEA. Staff implementing the new system then reviewed each data element and assigned appropriate roles.

The process of converting to a new system allowed the LEA an opportunity to conduct data quality checks on existing data and data elements, and to build checks into the new system. For example, the LEA's earlier data system had been in use for such a long time that some of the certifications it contained were outdated. In the event of a teacher layoff or relocation, that teacher's certifications in the earlier system had to be cross-checked against RIDE's data bank, where certification information was more correct and current. With the introduction of the new system, the LEA was able to update the list of certification options so that it only includes currently used certifications, thereby eliminating the need for cross-checks with RIDE.

Beyond the conversion and upload of data from the previous system, the LEA expanded the system to include new data elements and allow for interoperability with other systems. The new system includes elements for data required by the SEA, which has made it possible to automate reporting to RIDE—a feature that greatly reduces reporting burdens. In addition, the new system allows for the management of data from documents that previously were handled on paper. To improve the comparability of data, the LEA used standardized data elements, such as the National Center for Education Statistics (NCES) college numbering system whenever possible.

The LEA offered extensive training on the new system and continues to add end-user training to ensure that staff are using the system effectively and efficiently. In addition, the LEA and the city ran the old system and the new system in parallel to check for any issues in the new system and verify that the reports produced by the new system matched those from the old.

Challenges and Lessons Learned

The amount of work undertaken to check and convert existing data and data elements, then add new data elements, has reduced the burdens of record-keeping by removing paper from the equation and automating complex reporting tasks with an expanded and aligned dataset. The LEA has found the following to be important for educational agencies seeking to upgrade their data systems:

- Clear and frequent communication: Standing meetings between affected departments or divisions within a district (human resources and payroll, for example) make it possible to locate, document, and reconcile any data issues that may occur. When multiple parties are contributing data to the system, communication is crucial.
- Organization: Opacity between different entities within an LEA is not helpful. These entities may have unique ways of identifying data that are to be shared (unique teacher numbering systems, for instance). To merge these data into a common system, all contributing entities must be able to understand one another.

- Resource allocation: Be mindful of the many working hours required to thoroughly check and convert data from one system to another, as well as the time needed to effectively establish role-based access and ensure data privacy and security.
- Documentation and backups: Ensure that information concerning crucial duties is not limited to one or two people. A large-scale data effort on a timeline cannot depend on such a small base of expertise. Make sure that an adequate number of staff are trained in essential activities and that full documentation and data backups are available to let new staff step in if current resources become unavailable.

The COVID-19 pandemic has provided an example of the need for thorough documentation in case of changes to or reductions in staffing. When all staff were sent home to work remotely full-time, some staff were charged with new tasks for which they were not fully prepared. A siloed staff working on-site easily can ask questions and seek help when challenged by new expectations–the disconnect of a telecommuting situation makes this difficult, if not impossible. It is therefore helpful to keep all crucial processes thoroughly documented and easily available.

Putnam County Schools (West Virginia): Secure Data Access Across Multiple Systems

Putnam County Schools (WV) has taken a proactive approach in the management of staff records through technology. The LEA uses numerous data systems, each one optimized for the storage and transmission of a certain type of data, and is working to integrate these systems for heightened utility, tighter security, and ease of access. The ongoing effects of the coronavirus disease (COVID-19) pandemic have made the need for this integration all the more urgent.

System Integration

The LEA's staff records are used by numerous systems, including the following:

- a learning management system (LMS) for classroom and academic data;
- a performance analytics system;
- a software platform for email and other communications;
- a system for career applications and hiring management;
- a system to record teacher absences and engage substitutes automatically;
- a system to track and manage professional learning; and
- a customized program to broaden the current human resources (HR) system into a complete database of all personnel.

The diversity of systems using staff data can pose a challenge for any staff responsible for accessing or updating these data. Changes such as a new name, an adjustment in marital or identity status, a new degree or professional specialization, a new job description, or any number of other possibilities can impact several systems. Moreover, every new hire needs to be incorporated into these systems, and every staff member who leaves the LEA needs to be removed promptly. The solution: integrating the systems so that data are pulled from a single, authoritative source and so that multiple systems can be accessed with a single sign-on.

A Single Sign-on

A single sign-on has proven to be the most efficient way to combine access to many of the LEA's necessary systems. By associating an employee's payroll system information and county-specific employee ID with a single set of sign-on credentials, Putnam County creates a universal passkey containing the identifying information and credentials required by multiple systems. Payroll is used as the anchor for the single sign-on not only because a staff member's file is certain to include some vital identifying information (such as date of birth), but because of its use as a monitor for data security. By tying staff access to the basic indicator of who is and is not drawing a paycheck from the agency at any given moment, data managers ensure that only current staff can engage with the data and that all permissions are revoked at the end of employment. Not all of the above systems have been integrated yet under this universal sign-on, but several have, and the integration continues.

The single sign-on covers the professional learning system, the LMS, the analytics system, and the HR database, with additional integrations in progress. This allows staff who work with different aspects of these systems to easily access the resources and data they need. For example, once a teacher is provided with a sign-on, they automatically have access to their grade book, training software, and any application software needed for their work. Soon, teachers also will have access to the staff attendance system, permitting them to easily notify the school if they are absent and need to request a substitute teacher.

Authoritative Data Sources

Integrated systems improve the flow of data—rather than collecting and storing the same data in multiple systems, each system pulls data from one source. Putnam County engages in required data exchanges with the West Virginia Education Information System (WVEIS). WVEIS provides an authoritative source for many of the data needed by the LEA, including payroll data, but it does not include all of the information needed by the LEA. For example, dates of educator seniority, duty pay, and contract signings are needed only at the local level and therefore are not shared via WVEIS. Putnam County's HR department created an HR database that imports data nightly from WVEIS, and these data then are combined with LEA-specific data. Putnam County's HR database is used frequently to validate data requested by the state.

The COVID-19 Effect

Ease of access became an issue of paramount importance in 2020 due to the COVID-19 pandemic and the resulting shift to widespread remote working, teaching, and learning. Navigating multiple data systems without a single set of sign-on credentials is time-consuming for educators and staff working on-site, where one can visit administrators and ask questions in person; trying to do so entirely online is even more challenging. Now, staff can access many of the resources they need from home using the single sign-on. Moreover, integrated systems have improved data management. Staff can enter information about a newly hired staff member once, and relevant information such as staff name can be updated simultaneously in multiple systems. This proved especially useful with onboarding new staff. Rather than having to set up accounts within the training software for each newly hired staff member, those staff soon will be able to access the training they need using the single sign-on.

Lessons Learned

Security must always be a top priority with education data. Apart from the usual common-sense security protocols for online data work (strong passwords, not sharing credentials), Putnam County advises that a key point for security is to pull together only the least amount of information needed in an integration. For example, while a training system may need to pull data on a teacher's name and credentials from the HR system, data that are not needed (such as the teacher's birthdate) are best excluded from the pull. A thorough data audit will show which data are stored in which system(s) and where these data are needed. Secure integrated data systems will not provide data that are not needed and will not ask users to input data already present; both of these activities pose clear data risks and are to be avoided. In addition, a single sign-on for all data systems is not a safe practice; the data contained in some systems may require additional security.

Northshore School District (Washington): Remotely Onboarding Staff During a Pandemic

In early March 2020, like much of the country, Washington's Northshore School District was required to adopt a remote learning model with almost no notice. Almost as abruptly, staff at district schools and in the central LEA office followed students and teachers into remote work environments. Instead of working in their offices and cubicles, staff began working from their living rooms, kitchen tables, basements, and spare bedrooms. Meetings moved from conference rooms to teleconferencing tools. This created a variety of challenges, and the process of onboarding staff was no exception. Northshore staff quickly adapted to ensure that the abrupt switch to remote work would affect the staff onboarding process as little as possible. A primary focus of this effort was maintaining the ability of HR staff to remotely access and work with staff records as necessary for their jobs, without compromising the privacy or confidentiality of those records. This effort also extended to adapting the application process and the onboarding process to ensure that staff records created during remote work would be handled with the same protections as existing ones and that potential staff and new staff were provided with the support needed to effectively perform their jobs.

Working with Staff Data in At-Home Work Environments

In almost all cases, Northshore's HR staff were restricted to accessing the hiring system and other HR data exclusively within the protection of the district's secure network. This restriction helped to ensure the security of data related to job applicants and existing staff. As a result of the pandemic, HR staff suddenly were faced with the need to work for an indeterminate amount of time from home, using home Internet connections of varying security levels. To protect the data in the hiring system, Northshore installed virtual private networking (VPN) tools on all HR staff workstations and trained staff on how to use those tools. For staff who previously had elected to work from desktop computers, this process also meant transitioning them to agency-assigned laptops and assisting them with secure connections to their home network. Before being able to accomplish a moment's work, some staff had to acclimate to a new workspace, new work computer, new software for accessing district systems, and new teleconferencing software.

In addition, since some staff also are parents of children who also were shifting to remote schoolwork, they often needed to update their home network to ensure reliable connectivity for everyone. And in the event of home networking issues, they also needed time with support staff troubleshooting the entire system over several sessions before their new at-home setup became a stable and secure work environment. Depending on home environments, the place chosen for this set-up (be it the kitchen table, the basement, or a spare bedroom) was not always well suited to working with confidential information or conducting meetings requiring an appropriate level of discretion. Northshore worked with staff to emphasize the importance of finding an environment in which they could both be productive and keep confidential records, materials, and communication secure.

Comfort and Ease of Access for Applicants

Several years ago, Northshore moved its entire application process online. To accommodate applicants without home access to a computer or the Internet, the HR department placed application kiosks on-site at the central office. This allowed applicants to access online applications while also being able to ask support staff questions, as needed. However, the move to remote work for staff made these kiosks a non-viable option.

Applicants without home computers and reliable Internet connections had to find alternate ways to connect with Northshore's HR staff. The LEA increased the availability of phone, email, and other support options to support applicants and continues to look for new methods of connecting with potential applicants.

Northshore also has worked to make the process of remote interviewing accessible to a wide range of applicants and continues to look for ways to make the process as equitable as possible for applicants with limited technological access or training. While remote learning and work have led to a reasonable level of proficiency with video conferencing tools among existing agency staff, the same is not true for all applicants. It also is not possible to make assumptions about the reliability of the interviewee's tech set-up or about the environmental conditions around the interview–in other words, it would be unfair to include dropped Internet connections, household noise, or the interruptions of pets in the criteria for evaluating applicants post-interview. Northshore holds a team meeting before each interview in which interviewers are reminded that environmental conditions such as those listed above are not part of the evaluation to keep the selection process fair and equitable. The interview team also is reminded that part of its task is to make the candidate comfortable and to keep its focus on the interview, rather than the circumstances of the interview.

In cases where lack of Internet access completely rules out a teleconference-based interview as an option, interviews under the same guidelines also may be conducted by phone.

Touching Base at a Distance

Challenges with remote work continue post-interview, once a new hire has accepted an employment offer and the onboarding process begins. Initial challenges include carrying out onboarding professional development and meeting new colleagues via teleconference. In addition, onboarding's less documented aspects pose significant challenges. A new hire will have many questions in the early weeks of employment, questions that could be answered easily with a visit to a colleague's desk; the inherent complication of setting up a quick video conference to ask these questions as they arise means they may not get asked at all. The new hire may go without needed information at a crucial time and may make incorrect assumptions about job requirements and procedures. Therefore, Northshore has profited from being thoughtful and intentional about touching base, with staff making themselves available at regularly scheduled standing meetings at the beginning and end of the workday. These meetings are an invaluable opportunity to ask and answer questions or just for staff to check in with a new colleague. Another excellent option, staff workload permitting, is to designate a staff member as an onboarding mentor for all new hires. The mentor serves as a readily available resource for all questions.

Northshore has found that when onboarding new hires in a remote environment, it is important to establish that they have a resource for their questions and that asking those questions is not an imposition, but an expectation. It is just as essential to clarify this point with existing staff: making new staff feel like part of a team, and helping them avoid making guesses about processes and procedures instead of seeking answers, is a vital part of their jobs.

Appendix A:
Relevant Federal Laws

This appendix provides an overview of two important federal laws that govern the records maintained by federal agencies. All information was obtained from the cited websites. Many states have adopted similar laws, regulations, and policies, but it is important to note that state Freedom of Information Act (FOIA) or privacy laws may not include the same exemptions as the federal statutes. It is an agency's responsibility to proactively review and understand the implications of all applicable federal, state, and local legislation.

Freedom of Information Act

(https://www.foia.gov/about.html)

FOIA provides the public the right to request access to records from any federal agency. It is often described as the law that keeps citizens in the know about their government. Federal agencies are required to disclose any information requested under FOIA unless it falls under one of nine exemptions which protect interests such as personal privacy, national security, and law enforcement.

Privacy Act of 1974, 5 U.S.C. § 552a

(https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279)

The purpose of the Privacy Act is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them. The act focuses on four basic policy objectives:

1. To restrict disclosure of personally identifiable records maintained by agencies.
2. To grant individuals increased rights of access to agency records maintained on them.
3. To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.
4. To establish a code of "fair information practices" which required agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

The Privacy Act was amended by the Computer Matching and Privacy Act of 1988 to address the use of records in automated matching programs.

Appendix B: **Putnam County Schools (WV) Acceptable Use Policy (AUP) for Staff Who Supervise Students**

PUTNAM COUNTY SCHOOLS

Technology Acceptable Use Agreement Form

Professional Employees/Classroom Aides/Contracted Service Providers

OVERVIEW

The appropriate use of technology enables students and employees to become life-long learners and positive and effective digital citizens. Successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world and use technology responsibly. They understand that information posted to the Internet is public, permanent and may have a long-term impact on their lives and careers.

Putnam County Schools (PCS) and the West Virginia Department of Education (WVDE) provide a variety of technology tools, resources and services, including Internet and e-mail accounts, to employees who understand how to use them in a responsible manner. The intent of the district is for technology resources to be used as a valuable tool to support the educational process (8.8 Acceptable User of Computer Technology and Networks).

The acceptable and appropriate use of technology and/or access to the Internet and digital resources is an extension of the educator's responsibility in his/her classroom. Educators occupy a position of trust and stand in the place of a parent or guardian while a student is in school. Therefore, it is the educator's responsibility to ensure classroom activities focus on appropriate and specific learning goals and objectives when using Internet-related technologies. It is the educator's responsibility to avoid using technology in a manner that abuses this trust.

Collaboration, resource sharing and dialogue between the educational stakeholders (employees, students and/or parents) may be facilitated by the use of social media and other electronic communication. Such interactivity outside of the school walls can enhance classroom instruction. However, a clear line must be drawn between personal social networking and professional/educational social networking to protect the safety of the students and the integrity of educational professionals and service staff. Use of social media and electronic communication must support the educational process and follow PCS technology procedures. Educators are discouraged from using personal accounts to contact students.

Putnam County Schools and the WVDE reserve the right to monitor, inspect and investigate the content and usage of any technology device, resource or service. No one should have any expectation of privacy when using technology on district property; PCS reserves the right to disclose any information to law enforcement or third parties as appropriate. Personal devices used for school-related information exchange are subject to inspection by legal authorities.

USE OF TECHNOLOGY RESOURCES WITHIN PUTNAM COUNTY SCHOOLS IS A PRIVILEGE, NOT A RIGHT.

USER RESPONSIBILITIES

As the user of technology resources provided by Putnam County Schools, each employee must read, understand and accept all of the following rules stated in this section.

1. I understand and will abide by the generally accepted rules of digital/network etiquette and security.
    - I will be polite in electronic communications, using proper English and appropriate language.
    - I will not reveal any personal information about another individual on any electronic medium without his/her permission.
    - I will keep educational files and e-mail messages within my allotted space limits.
    - I will only publish student pictures or names on class, school or district websites when appropriate, written permission has been received from the parent/guardian in accordance with district's policy (8.9 Web Publishing).
    - I will not use personally owned devices (PODs) to bypass Internet filtering or security. I understand all Internet content for students must be filtered in accordance with the Children's Internet Protection Act (CIPA).
2. I understand that all technology use must be for **educational** purposes when at school or school-related activities.
    - I will use PCS technology resources and telecommunications for purposes that support the educational process. District equipment that is used offsite is subject to the same rules as when used onsite.
    - I will not use PCS network for personal purposes, which include, but are not limited to banking, planning personal travel, personal shopping or participating in online gaming, gambling and auctions.
    - I will not use PCS resources to view, create, modify or disseminate obscene, objectionable, violent, pornographic or illegal material.
    - I will not use PCS resources for commercial or for-profit purposes that include, but are not limited to, home businesses, gambling, advertising, political lobbying or soliciting.
    - I will not use PCS resources for hacking, cracking, vandalizing or any other unlawful online activities.
    - I am responsible for PCS devices given to me as part of my job. If any PCS device is lost, stolen or damaged while in my possession away from school property, I am responsible for replacement/repair costs.
    - I understand that the district assumes no liability for loss, damage or misuse of personally owned devices (PODS) on PCS property or at PCS-sponsored events.

3. I understand the bandwidth available to PCS and WVDE is limited and must be protected for educational purposes.
    - I will not access my personal social networking sites using PCS resources.
    - I will not listen to the radio, watch videos or play games via the PCS network for entertainment purposes.
    - I will only stream audio and video files that have an educational purpose, and I will download and save the content to the computer, server or cache server during non-peak hours when possible.
4. I understand that employees have access to confidential information and files and that I am responsible for protecting the confidentiality of these data.
    - I will log off or lock the computer/network when not using it.
    - I will not use the "remember password" feature of Internet browsers and e-mail clients.
    - I will close student records (gradebooks, West Virginia Education Information System [WVEIS], etc.) when away from my desk.
    - I will not allow students, parents or unauthorized people access to my accounts or gradebooks.
    - I understand that information in WVEIS is to be used only for district business, and I must maintain the confidentiality of student and other personal data in accordance with the Family Educational Rights and Privacy Act (FERPA).
    - I will not attempt to learn other employees' passwords.
    - I will not copy, change, read or use files that belong to other employees without their permission.
5. I understand copyright laws protect a variety of materials (print, non-print and ideas) including those found on the Internet and electronic resources.
    - I will not install any unauthorized software, including personal software, on PCS equipment. Unauthorized software is defined as software outside the legal licensing agreement created by the author of the program.
    - I will not make copies of any software found on the district's equipment or on the Internet to keep, give or sell in violation of the legal license agreement.
    - I will not use shareware beyond the trial period specified by the program unless I purchase it.
    - I will not download any copyrighted materials from the Internet without the permission of the copyright holder. This includes, but is not limited to, music and video files.
6. I understand the importance of maintaining the technology that I use for my job.
    - I will not attempt to bypass or disable any security or antivirus software installed on my device(s) or on the network.
    - I will not knowingly create or introduce any virus to PCS equipment.
    - I will inform my technology support personnel or site administrator about problems with technology and security issues; I will follow the repair process implemented at my work site.
    - I will maintain my devices by allowing periodic updates of operating systems, anti-virus programs and anti-spy/malware software to run when prompted.
    - I will protect my data by performing periodic back-ups to external media.

- **I will not remove any PCS technology device** without the prior approval of the PCS Technology Department.
- I will not attach any wireless access points, routers or modems to the wired or wireless network.
- I will follow PCS policy (8.10 Network Access from Personally Owned Computers and/or Other Web-Enabled Devices) when attaching PODs to the district's wireless network (Internet). I understand that I may not access PCS servers from my POD and will not use a network cable to attach to the network.

USER RESPONSIBILITIES FOR EMPLOYEES WHO SUPERVISE STUDENTS USING TECHNOLOGY

1. A staff member is required to be present and to monitor student use of the Internet or network resources.
2. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist in filtering and acceptable use issues.
3. Student use of the Internet must support the educational learning goals and objectives as defined in WVDE Policy 2520.14.
4. All students must have a signed PCS Acceptable Use Agreement Form on file at school before they access any technology.
5. As part of all Internet lessons and periodically during other technology lessons, acceptable use of technology and telecommunications should be reviewed.
6. Teachers will educate students about appropriate online behavior, including cyber bullying awareness and response and interacting with other individuals on social network sites and in chat rooms. Teachers shall record the instruction of such lessons on WVEIS WOW.
7. At school, students should ONLY use their WVDE provided email account. By fourth grade, all students need e-mail accounts to master the Content Standards Objectives (CSOs).
8. Teachers who utilize Web 2.0 tools (wikis, blogs, pod/vodcasts, etc.) work must adhere to PCS policy 8.9. These tools should be on educational sites that provide protection of user privacy, content monitoring and limit advertising. Information on appropriate sites is available from the PCS and WVDE technology departments.
9. Teachers will instruct students about copyright laws and the fair and appropriate use of information and ideas.
10. An educator who observes a student violating PCS policy (8.8, 8.9 and 8.10) must report the student to the school sysop and/or administration according to the procedures in place at his/her school.
11. Educational web portals, such as approved school websites, are designed to encourage communication between school and home. Use of portals as a primary access point for teachers, students and home communication is encouraged. Sites that actively promote and focus on school fundraising and/or commercial ventures are not permitted. Questions about portals should be addressed to the PCS Technology Department.

Failure to comply with the above rules may result in permanent revocation of technology privileges and/or disciplinary actions involving local, county, state or federal agencies.

I have read and agree to abide by the rules and regulations above. I also understand that any technology device used on the PCS network is subject to random auditing by PCS staff, WVDE staff or software publishing organizations for the purpose of determining the presence of unauthorized software or misuse of technology.

Employee Signature ______________________ Date ______________________

Employee Name (please print) ____

THIS SIGNATURE PAGE MUST BE ON FILE AT THE PERSONNEL OFFICE FOR THE EMPLOYEE TO MAINTAIN TECHNOLOGY ACCESS.

Appendix C: **Putnam County Schools (WV) Acceptable Use Policy (AUP) for Staff Who Do Not Supervise Students**

PUTNAM COUNTY SCHOOLS

Technology Acceptable Use Agreement Form

Service Personnel (except aides)

OVERVIEW

The appropriate use of technology enables PCS staff to be life-long learners and positive and effective digital citizens. Successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world and use technology responsibly. They understand that information posted to the Internet is public, permanent and may have a long-term impact on their lives and careers.

Putnam County Schools (PCS) and the West Virginia Department of Education (WVDE) provide a variety of technology tools, resources and services, including Internet and e-mail accounts, to employees who understand how to use them in a responsible manner. The intent of the district is for technology resources to be used as a valuable tool to support the educational process (8.8 Acceptable User of Computer Technology and Networks).

Collaboration, resource sharing and dialogue between the educational stakeholders (employees, students and/or parents) may be facilitated by the use of social media and other electronic communication. However, a clear line must be drawn between personal social networking and professional/educational social networking to protect the safety of the students and the integrity of educational professionals and service staff. Use of social media and electronic communication must support the educational process and follow PCS technology procedures. Staff are discouraged from using personal accounts to contact students.

Putnam County Schools and the WVDE reserve the right to monitor, inspect and investigate the content and usage of any technology device, resource or service. No one should have any expectation of privacy when using technology on district property; PCS reserves the right to disclose any information to law enforcement or third parties as appropriate. Personal devices used for school-related information exchange are subject to inspection by legal authorities.

USE OF TECHNOLOGY RESOURCES WITHIN PUTNAM COUNTY SCHOOLS IS A PRIVILEGE, NOT A RIGHT.

USER RESPONSIBILITIES

As the user of technology resources provided by Putnam County Schools, each employee must read, understand and accept all of the following rules stated in this section

1. I understand and will abide by the generally accepted rules of digital/network etiquette and security.
    - I will be polite in electronic communications, using proper English and appropriate language.
    - I will not reveal any personal information about another individual on any electronic medium without his/her permission.
    - I will keep educational files and e-mail messages within my allotted space limits.
    - I will only publish student pictures or names on class, school or district websites when appropriate, written permission has been received from the parent/guardian in accordance with district's policy (8.9 Web Publishing).
    - I will not use personally owned devices (PODs) to bypass Internet filtering or security. I understand all Internet content for students must be filtered in accordance with the Children's Internet Protection Act (CIPA).
2. I understand that all technology use must be for **educational** purposes when at school or school-related activities.
    - I will use PCS technology resources and telecommunications for purposes that support the educational process. District equipment that is used offsite is subject to the same rules as when used onsite.
    - I will not use PCS network for personal purposes, which include, but are not limited to banking, planning personal travel, personal shopping or participating in online gaming, gambling and auctions.
    - I will not use PCS resources to view, create, modify or disseminate obscene, objectionable, violent, pornographic or illegal material.
    - I will not use PCS resources for commercial or for-profit purposes that include, but are not limited to, home businesses, gambling, advertising, political lobbying or soliciting.
    - I will not use PCS resources for hacking, cracking, vandalizing or any other unlawful online activities.
    - I am responsible for PCS devices given to me as part of my job. If any PCS device is lost, stolen or damaged while in my possession away from school property, I am responsible for replacement/repair costs.
    - I understand that the district assumes no liability for loss, damage or misuse of personally owned devices (PODs) on PCS property or at PCS-sponsored events.
3. I understand the bandwidth available to PCS and WVDE is limited and must be protected for educational purposes.
    - I will not access my personal social networking sites using PCS resources.
    - I will not listen to the radio, watch videos or play games via the PCS network for entertainment purposes.
    - I will only stream audio and video files that have an educational purpose, and I will download and save the content to the computer, server or cache server during non-peak hours when possible.

4. I understand that employees have access to confidential information and files and that I am responsible for protecting the confidentiality of these data.
    - I will log off or lock the computer/network when not using it.
    - I will not use the “remember password” feature of Internet browsers and e-mail clients.
    - I will close student records (gradebooks, West Virginia Education Information System [WVEIS], etc.) when away from my desk.
    - I will not allow students, parents or unauthorized people access to my accounts or gradebooks.
    - I understand that information in WVEIS is to be used only for district business, and I must maintain the confidentiality of student and other personal data in accordance with the Family Educational Rights and Privacy Act (FERPA).
    - I will not attempt to learn other employees’ passwords.
    - I will not copy, change, read or use files that belong to other employees without their permission.

5. I understand copyright laws protect a variety of materials (print, non-print and ideas), including those found on the Internet and electronic resources.
    - I will not install any unauthorized software, including personal software, on PCS equipment. Unauthorized software is defined as software outside the legal licensing agreement created by the author of the program.
    - I will not make copies of any software found on the district’s equipment or on the Internet to keep, give or sell in violation of the legal license agreement.
    - I will not use shareware beyond the trial period specified by the program unless I purchase it.
    - I will not download any copyrighted materials from the Internet without the permission of the copyright holder. This includes, but is not limited to, music and video files.

6. I understand the importance of maintaining the technology that I use for my job.
    - I will not attempt to bypass or disable any security or antivirus software installed on my device(s) or on the network.
    - I will not knowingly create or introduce any virus to PCS equipment.
    - I will inform my technology support personnel or site administrator about problems with technology and security issues; I will follow the repair process implemented at my work site.
    - I will maintain my devices by allowing periodic updates of operating systems, anti-virus programs and anti-spy/malware software to run when prompted.
    - I will protect my data by performing periodic back-ups to external media.
    - **I will not remove any PCS technology device** without the prior approval of the PCS Technology Department.
    - I will not attach any wireless access points, routers or modems to the wired or wireless network.
    - I will follow PCS policy (8.10 Network Access from Personally Owned Computers and/or Other Web-Enabled Devices) when attaching PODs to the district’s wireless network (Internet). I understand that I may not access PCS servers from my POD and will not use a network cable to attach to the network.

Failure to comply with the above rules may result in permanent revocation of technology privileges and/or disciplinary actions involving local, county, state or federal agencies.

I have read and agree to abide by the rules and regulations above. I also understand that any technology device used on the PCS network is subject to random auditing by PCS staff, WVDE staff or software publishing organizations for the purpose of determining the presence of unauthorized software or misuse of technology.

Employee Signature ______________________ Date ______________________

Employee Name (please print) ____

THIS SIGNATURE PAGE MUST BE ON FILE AT THE PESONNEL OFFICE FOR THE EMPLOYEE TO MAINTAIN TCHNOLOGY ACCESS.

Reference List

Citations

Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule (2009) *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, pp. 17-18. Cited in *SLDS Technical Brief: Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records* (2010). Retrieved December 18, 2020, from https://nces.ed.gov/pubs2011/2011601.pdf.

Common Education Data Standards (CEDS). Retrieved March 31, 2020, from https://ceds.ed.gov/domainEntitySchema.aspx?v=8&ex=Draft.

Montana Secretary of State. (n.d.) "Glossary of Records Management Terms." Retrieved December 18, 2020, from https://sosmt.gov/records/glossary/.

Montana Secretary of State. (n.d.) Retention Schedules. Retrieved December 18, 2020, from https://sosmt.gov/records/toolkit/rim-retention/.

National Research Council. (2009). *Protecting Student Records and Facilitating Education Research: A Workshop Summary*. Washington, DC: The National Academies Press. https://doi.org/10.17226/12514. Cited in Statewide Longitudinal Data System Grant Program. (2010). *SLDS Technical Brief: Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records*. U.S. Department of Education. Washington, DC: National Center for Education Statistics. Retrieved December 18, 2020, from https://nces.ed.gov/pubs2011/2011601.pdf.

Protecting Student Privacy (2019). *Best Practices for Data Destruction*. Retrieved December 18, 2020, from https://studentprivacy.ed.gov/resources/best-practices-data-destruction.

Protecting Student Privacy (2019). "Glossary." Retrieved March 31, 2020, from https://studentprivacy.ed.gov/glossary#glossary-node-227.

U.S. Department of Health & Human Services (2004). "As an employer, I sponsor a group health plan for my employees. Am I a covered entity under HIPAA?" Retrieved March 31, 2020, from https://www.hhs.gov/hipaa/for-professionals/faq/499/am-i-a-covered-entity-under-hipaa/index.html.

Legal Citations

Privacy Act, 5 U.S.C. § 552a (1974).

The Freedom of Information Act, 5 U.S.C. § 552 (2016).

Related Resources

Relevant National Forum on Education Statistics Resources

Forum Guide to Cybersecurity: Safeguarding Your Data (2020)

https://nces.ed.gov/forum/pub_2020137.asp

This resource provides best practice information to help education agencies proactively prepare for, appropriately mitigate, and responsibly recover from a cybersecurity incident. It provides recommendation to help protect agency systems and data before, during, and after a cybersecurity incident and features case studies from state and local education agencies.

Forum Guide to Data Governance (2020)

https://nces.ed.gov/forum/pub_2020083.asp

This resource provides timely and useful best practices, examples, and resources for agencies implementing or updating their data governance programs. It provides an overview of data governance; discusses effective data governance practices, structures, and essential elements; describes how to meet privacy and security requirements while also meeting data accessibility and sharing needs; and includes detailed case studies from education agencies in their data governance efforts.

Forum Guide to Planning for, Collecting, and Managing Data About Students Displaced by a Crisis (2019)

https://nces.ed.gov/forum/pub_2019163.asp

This resource provides timely and useful best practice information for collecting and managing data about students who have enrolled in another school or district because of a crisis. It highlights best practices that education agencies can adopt before, during, and after a crisis and features contributions from agencies that have either experienced a crisis or received students who were displaced by a crisis.

Forum Guide to Technology Management in Education (2019)

https://nces.ed.gov/forum/tec_intro.asp

This resource is designed to assist education agency staff with understanding and applying best practices for selecting and implementing technology to support teaching and learning in the classroom. It addresses the widespread use and integration of technology in modern education systems and focuses on technology governance and planning, technology implementation, integration, maintenance, support, training, privacy, security, and evaluation.

Forum Guide to Education Data Privacy (2016)

https://nces.ed.gov/forum/pub_2016096.asp

This resource provides state and local education agencies (SEAs and LEAs) with best practice information to use in assisting school staff in protecting the confidentiality of student data in instructional and administrative practices. SEAs and LEAs also may find the guide useful in developing privacy programs and related professional development programs.

Forum Guide to Supporting Data Access for Researchers: A Local Education Agency Perspective (2014)

https://nces.ed.gov/forum/pub_2014801.asp

This resource recommends a set of core practices, operations, and templates that can be adopted and adapted by LEAs as they consider how to respond to requests for both new and existing data about the education enterprise.

Forum Guide to Taking Action with Education Data (2013)

https://nces.ed.gov/forum/pub_2013801.asp

This resource provides practical information about the knowledge, skills, and abilities needed to identify, access, interpret, and use data to improve instruction in classrooms and the operation of schools, LEAs, and SEAs.

Forum Guide to the Teacher-Student Data Link: A Technical Implementation Resource (2013)

https://nces.ed.gov/forum/pub_2013802.asp

This resource is intended as a guide to the skillful and appropriate use of education data. It introduces the teacher-student data link (TSDL) and provides information on TSDL components, use cases, and strategies for overcoming implementation challenges.

Forum Guide to Supporting Data Access for Researchers: A State Education Agency Perspective (2012)

https://nces.ed.gov/forum/pub_2012809.asp

This resource recommends a set of core practices, operations, and templates that can be adopted and adapted by SEAs as they consider how to respond to requests for data about the education enterprise, including data maintained in longitudinal data systems.

Traveling Through Time: The Forum Guide to Longitudinal Data Systems (Series)

Book I: What is an LDS? (2010) http://nces.ed.gov/forum/pub_2010805.asp

Book II: Planning and Developing an LDS (2011) http://nces.ed.gov/forum/pub_2011804.asp

Book III: Effectively Managing LDS Data (2011) http://nces.ed.gov/forum/pub_2011805.asp

Book IV: Advanced LDS Usage (2011) http://nces.ed.gov/forum/pub_2011802.asp

The Traveling Through Time series is intended to help SEAs and LEAs meet the many challenges involved in developing robust systems, populating them with quality data, and using this new information to improve the education system. The series introduces important topics, offers best practices, and directs the reader to additional resources.

Forum Curriculum for Improving Education Data: A Resource for Local Education Agencies (2007)

https://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 Building a Culture of Quality Data: A School & District Resource (2005)

https://nces.ed.gov/forum/pub_2005801.asp

This resource was developed to help schools and school districts improve the quality of data they collect and to provide processes for developing a "Culture of Quality Data" by focusing on data entry–getting things right at the source. This resource shows how quality data can be achieved in a school or district through the collaborative efforts of all staff.

Additional Resources

State Resources

Colorado Department of Education Educator Preparation Programs Report

https://www.cde.state.co.us/educatortalent/edprepprogram-report

Delaware Department of Education Educator Preparation Program Reports

https://www.doe.k12.de.us/domain/398

Illinois Freedom of Information Act (FOIA) request

https://www.isbe.net/foia

Kentucky Department of Education Data Requests

https://education.ky.gov/districts/tech/Pages/DataRequests.aspx

Missouri Records Retention Schedule

https://www.sos.mo.gov/CMSImages/LocalRecords/General.pdf

National Association of State Directors of Teacher Education and Certification

Public Educator Lookup Websites

https://www.nasdtec.net/page/PublicEducator_Map

Nebraska Department of Education Staff Reporting

https://www.education.ne.gov/dataservices/staff/

Rhode Island Educator Preparation Index

http://www3.ride.ri.gov/RIEdPrepIndex/Default.aspx