



Forum Guide to Staff Records

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 indicator, 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.