State of Oregon
OREGON DEPARTMENT OF EDUCATION
POLICY MANUAL

AGENCY POLICY 581-101

Effective Date: 10-19-2006
Last Revision Date: 6-1-2022

APPROVED: Signature on File at ODE

RE: Handling Confidential Information

PURPOSE: To provide guidelines for the Oregon Department of Education (Agency) employees, volunteers and contractors about agency responsibility for managing student and local education employee information.

Overview:

Local education employees include employees and volunteers of Oregon public school districts; Education Service Districts; private schools, including Career and Vocational schools; Head Start and other registered child care programs; and employees of contractors of any of these entities.

Agency employees, volunteers and contractors must read and follow the guidelines and requirements for confidentiality in working with student or education employee information.

Guiding Principles:

The following principles apply to the collection, maintenance, transfer, destruction, and use of student and education employee information held by the Agency, its employees, volunteers and contractors:

- Student and education employee information is a valuable asset of the Agency and should be treated as any other valuable asset.
- The Agency manages student and education employee information under its control throughout its lifecycle, from inception to appropriate destruction.
- The Agency is responsible for controlling access to and use of student and education employee information.
- The Agency is responsible for reviewing government policies and regulations in determining what is considered confidential student and education employee information.

The remainder of this document contains the following sections:
- Definition of Confidentiality
- Definition of Disclosure
- Issue Areas

DEFINITIONS:

The resources used as guidance in providing these definitions include Oregon Revised Statutes; Oregon Administrative Rules, Division 21; Oregon Public Records Request Laws;

Federal Education Rights Privacy Act (FERPA); the federal Freedom of Information Act; and U. S. Department of Agriculture and Health Insurance Privacy and Accountability Acts.

Definition of Confidentiality:

Confidentiality is defined as a security principal that works to ensure that information is not disclosed to unauthorized subjects.
Confidential data or information is that which is intended for or restricted to the use of a particular person, group, or office, and which contains information whose unauthorized disclosure could be prejudicial or harmful.

Most individual student educational records, education employee personnel records and most health records are exempt from disclosure and protected under various confidentiality laws.

Data or information that is considered confidential must be handled based on the data classification. The Agency Information Asset Classification Policy (581-309) includes 4 levels of classification for which 2 require strict handling methods.

- Level 3 – Restricted
- Level 4 – Critical

Information directly related to a student and maintained by the Agency is considered confidential. This information includes:

- Family information, such a names, address, phone numbers, birth dates, personal and business financial data, household members' social security numbers, household members' employment information, household Temporary Assistance for Needy Families (TANF), Food Stamp, Food Distribution Program for Indian Reservations (FDPIR) benefits information.
- Personal information such as identification codes, grades, scores, courses taken, other specific information linked directly to a student
- Special Education Records
- Medical and Health Records
- Video tapes and pictures of individuals or groups
- Free or Reduced Price eligibility status of individual students in USDA-funded school lunch, breakfast and milk programs, Summer Food Service Programs, and Child and Adult Care Food Programs
- All information used to determine benefits in USDA Child Nutrition Programs contained in: *Confidential Application for Free and Reduced Price Meals or Free Milk; Confidential Income Statements Direct Certification Documents*
- All information collected to verify information submitted by households on confidential Applications for Free and Reduced Price Meals or Free Milk and Confidential Income Statements.

Information directly related to an education employee and maintained by the Agency is considered confidential. The confidentiality and handling of this type of data is regulated by various state and federal laws, including the Oregon Identity Theft Protection Act. This information includes:

- Family information such as names, addresses, phone numbers, birth dates, personal and business financial data, household members' social security numbers, household members' employment information.
- Personal information such as identification codes, scores, courses taken, other specific information linked directly to an employee,

- Medical and Health records,
- Driving records, and
- Criminal History records.

Definition of Disclosure:

Any time confidential information is revealed or used for a purpose other than for the purpose for which the information was obtained is a disclosure. The term "disclosure," refers to access, release, or transfer of personally identifiable data about individuals by means of print, video, pictures, electronic communication like email or text and other means.

Some information about students is not considered a student education record and therefore is not subject to access or disclosure rules. The following are not subject to disclosure rules;

- Notes by employees which may be used by substitute or replacement personnel;
- Records created by law enforcement units of schools or education agencies maintained separately from education records;
- Employment records about a student employed by a school, education agency or institution. These would fall under employer-employee laws and rules.
- Information obtained about individuals after they are no longer students, except as stated above as members of households.
- Directory information that has been identified through a public notice and approved by a parent/guardian for dissemination. The definition of directory information typically refers to a school or district and is relevant to the Agency only because of its relationship to the Oregon School for the Deaf. This information would not generally be considered harmful or an invasion of privacy if released and could include:
    - ▲ Student's name and school activities
    - ▲ Family members names, addresses and telephone numbers
    - ▲ Pictures and biographical information usually found in yearbooks, school newspapers and other publications

To find a list of student and staff level collections use the ODE websites and applications listed:

Consolidated Collections File Format Page
ODE Collection Catalog
ODE Schedule of Due Dates

ISSUE AREAS:

The table below lists issues where confidentiality concerns may exist and recommends actions that should be taken to resolve these concerns.

Area	Issue	Recommendation to resolve
Servers	Items on servers and shared directories may be vulnerable	File Servers – Work unit management should establish procedures to create directories where confidential information can be stored limiting the access to only those employees needing it to perform their duties. Work unit management should periodically review directories under their control to validate that confidential information is limited to only those employees that require access. Database Servers – Information Technology (IT) will design databases containing confidential information to limit access to only those employees needing it. IT will work with

		appropriate work unit management to allow access to those employees needing it to perform their duties. Training should be provided to employees and employees that access the confidential information should be required to sign-off that they are aware of the responsibilities in working with the information.
Desktops, Laptops, Devices	Risk is relative to exposure if user does not lockdown desktop, laptop, or other devices.	Users, especially users with access to databases containing confidential information need to take care to restrict access to their desktop, laptops, or devices by locking computer, laptop or device prior to leaving unattended. IT is available to instruct users on proper procedures to lock down computers, laptops and devices. No confidential information (see page 2 for a list of confidential information) is to be stored on the local drive (ie, C: Drive), or employee computers, laptops or other devices. No passwords or other user credentials should be stored on the local drive, computers, laptops or other devices, or on paper.
Portable Media	Diskettes, CDs, Zip Disks, Flash Drives, etc. are much like paper files in that they can be misplaced.	Portable Media should not be used to store or transport confidential data under any circumstances without proper encryption/security. See page 2 of this policy for a listing of confidential information. IT can assist if encryption is needed.
Inter/Intranet/ SharePoint	Confidential information posted on the Intranet, SharePoint or Internet.	Care should be taken not to post any individual information on any website maintained by the Agency. This includes information that does not directly relate to an individual, but can be deduced because of the "cell-size" described below. Transmission of secure data is to be done via Secure FTP or SSL ONLY.
Cell Size	Cell size of data could ultimately be used to identify an individual.	Care should be taken in datasets and reports that could potentially violate confidentiality when an individual population is too small. There are several categories of data that will be filtered for student confidentiality, for example: • Assessment Results • Students with an Individualized Education Plan (IEP) • Information on student discipline. • Free and Reduced Lunch For groups where 6 or fewer students can be isolated, there is potential for identification of an individual student. In these cases, the student counts or percentages should be suppressed. In the case of percent as in the Assessment Results where 100 percent of a student population fall into a result category the data will be suppressed. Using < 5% and > 95% to indicate the number or percentage is greater or less than what should be used whenever cell size is too small or to great to publish as is.
Verbal	Oral communication of confidential data – phone conversation, "teams" meetings or calls, zoom meetings or calls.	Conversations over the telephone or in person regarding confidential information should occur in secure areas. Employees should move to an available office or conference room so that the conversation is not overheard. Using online tools (zoom or teams) for video conversations, employees should not share confidential information unless all parties have the rights to that information.
Paper files	Too easily misplaced	Creation and use of paper files containing individual information that is confidential should be limited and if necessary, must be stored in secure areas when not in use. All paper containing Level 3 or 4 data must be properly labeled as per policy 508-309. Papers with confidential information must be secured and when not needed anymore

		should be disposed of properly by disposing in confidential shred bins.
Printer	Confidential data may unintentionally be left on printer, or stored in memory.	Print any confidential document only when user will walk directly to the printer and pick up the hard copy as soon as it prints out. No Agency documents or communications should be printed on a personal printer as per DAS policy.
Emails	Risk of third parties gaining access or misdirection	ODE will instruct all correspondents that email transfer of a confidential document is not permitted. To transfer confidential data, ODE staff and business partners will use the ODE secure FTP web page: https://district.ode.state.or.us/apps/xfers/ When ODE employees receive a confidential document via email, the employee will save the file to a secure drive, if needed, and immediately use the "shift-delete" keyboard function to permanently delete the email from his/her email files. The employee will then notify the sender to inform them that confidential data transmission should be done using the ODE secure FTP web page (URL above).
Faxes	Risk of misdirection and misplacement.	ODE will instruct all correspondents that fax transfer of a confidential document is allowed only when the fax mailer phones in advance to notify the recipient that a confidential document will be faxed at a specific time, are being sent to physical fax machine, and that all faxes containing confidential information will be sent with a cover page that includes the intended recipient's printed full name and the statement, "This fax contains confidential information and is intended only for the addressee. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or the taking of any action in reliance on the contents of this information is strictly prohibited. If you have received this transmission in error, please immediately notify us by telephone to arrange for the return of the documents." In the event an ODE employee receives electronic faxes through ODE's main fax number containing confidential data, the employees will follow recommendations for emails, i.e., Save the confidential data to a secure drive and immediately use the "shift-delete" keyboard function to permanently delete faxes.
Contradictory Regulations	State and federal regulations sometimes appear to be in conflict relative to confidentiality and the release of public information relative to hearings, mediations, etc.	Identify lead person within the agency to maintain vigilance regarding specific legislation or areas of legislation where contradictory legislation/regulations may occur. Follow up with federal or state agencies or entities to provide input regarding contradictions. Use Directors, legal office or program specialists to review proposed changes in regulations/legislation and assure that follow-up occurs.
Directory Information	A policy should be established identifying what is considered "directory information" that will be available for public request.	For the purposes of local school district information collected by ODE, it needs to be established that no such information received by ODE will be considered to be "directory information." ODE has no mandate to publish information in a directory fashion. For purposes of student information maintained by OSD, establish that directory information will be the items listed in the OSD policy manual, section Directory Information.
Destruction of Records	What is the proper method of disposing confidential records?	When you need to destroy documents or files containing confidential data, the following is the recommended method of destruction for the media. **Paper** documents should be shredded (confidential bin).

		CD's should be broken into multiple pieces, or turned into IT for disposal. **Computer files** on your computer should be deleted, and removed from the recycle bin. **Computer files** on network servers should be deleted. For assistance contact the ODE Helpdesk
Offsite Wireless	Safely accessing the ODE network while outside of the office.	Many public wireless Internet connections, such as those available in hotels and coffee shops are not adequately secured. When using a wireless connection, users may only access the ODE network using a secure VPN connection or ODE Direct access.
Instant Messenger, Teams, Zoom, etc.	It is possible to transmit confidential data over Instant Message or online meeting programs.	Use of Instant Messenger and other communication tools like Teams, Zoom and GoTo programs are not limited to interagency communication and therefore confidential data should not be shared in this manner. All communications like chat sessions are saved and can be released via public records request.