

Green River College PRFR Report Appendix 2.C.4

2.C.4 The institution's policies and procedures regarding the secure retention of student records must include provisions related to confidentiality, release, and the reliable backup and retrievability of such records.

Table of Contents

2.C.4 EV.#1 / Section 1.....	4
-------------------------------------	----------

Section 1: Policies and procedures regarding secure retention of student records

- [Family Education Records Privacy Act, FERPA](#)
- [Washington State Preservation and Destruction of Public Records, RCW 40.14](#)
- [Washington State Public Records Act, RCW 42.56](#)
- [Washington State Records and Retrieval Act, WAC 434-610 – 434-690](#)
- [NIST Cybersecurity Framework](#)
- [Gramm-Leach-Bliley Act](#)
- [ctcLink Privacy Agreement](#)
- [state-government-general-records-retention-schedule-v.6.3-\(october-2024\).pdf](#)
- [Data Security Training, Vector Solutions](#)
- [Vector LMS, Higher Education Edition Training : Login](#)
- [Green River Data Handling Guidelines](#)
- [Information Security Program Plan \(section 8.3.1, Enterprise Backup Policies, page 56](#)
- [GRC policy from Catalog: Student Right to Privacy \(FERPA\) \(page 9\)](#)
- [WAC 132J-276 Public Record](#)
- [GA-17 Educational Rights and Privacy Act](#)
- [FERPA in GRC Webpage](#)
- [Educational Records](#)
- [Privacy](#)

2.C.4 EV.#1 / Section 1

Family Education Records Privacy Act, [FERPA](#)

[RESOURCES \(/RESOURCES\)](#) [TRAINING \(/TRAINING\)](#) [BROWSE BY AUDIENCE \(/BROWSE-BY-AUDIENCE\)](#)

[FAQS \(/FREQUENTLY-ASKED-QUESTIONS\)](#) [ESPAÑOL \(/es\)](#)

[ABOUT \(/ABOUT\)](#) [CONTACT \(/CONTACT\)](#) [FILE A COMPLAINT \(/FILE-A-COMPLAINT\)](#)

FERPA

34 CFR PART 99—FAMILY EDUCATIONAL RIGHTS AND PRIVACY

Below are the regulations at 34 CFR Part 99 implementing section 444 of the General Education Provision Act (GEPA), which is commonly referred to as the Family Educational Rights and Privacy Act (FERPA), and Federal Register Notices of amendments to FERPA. They are presented here for your convenience.

The current regulations can also be found at the Electronic Code of Federal Regulations: [Title 34, Part 99-- Family Educational Rights and Privacy \(https://www.ecfr.gov/cgi-bin/text-idx?SID=4b4094c9e8a435c5e9cf4026588c3ffe&mc=true&tpl=/ecfrbrowse/Title34/34cfr99_main_02.tpl\)](https://www.ecfr.gov/cgi-bin/text-idx?SID=4b4094c9e8a435c5e9cf4026588c3ffe&mc=true&tpl=/ecfrbrowse/Title34/34cfr99_main_02.tpl).

The current statutes can be found at [20 U.S.C. 1232g - Family educational and privacy rights \(http://www.govinfo.gov/app/details/USCODE-2017-title20/USCODE-2017-title20-chap31-subchapIII-part4-sec1232g\)](http://www.govinfo.gov/app/details/USCODE-2017-title20/USCODE-2017-title20-chap31-subchapIII-part4-sec1232g).

To learn more about FERPA, please refer to the General Guidance for [Parents \(https://studentprivacy.ed.gov/resources/parent-guide-family-educational-rights-and-privacy-act-ferpa\)](https://studentprivacy.ed.gov/resources/parent-guide-family-educational-rights-and-privacy-act-ferpa) or [Students \(https://studentprivacy.ed.gov/resources/ferpa-general-guidance-students\)](https://studentprivacy.ed.gov/resources/ferpa-general-guidance-students).

Parents and eligible students who wish to file a complaint under FERPA may do so on the [File a Complaint \(https://studentprivacy.ed.gov/file-a-complaint\)](https://studentprivacy.ed.gov/file-a-complaint) page.

The Federal Register Notices of amendments to FERPA regulations can be found here:

[12/2/2011 \(https://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf\)](https://www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf).

[12/9/2008 \(https://www.gpo.gov/fdsys/pkg/FR-2008-12-09/pdf/E8-28864.pdf\)](https://www.gpo.gov/fdsys/pkg/FR-2008-12-09/pdf/E8-28864.pdf).

[4/21/2004 \(https://www.gpo.gov/fdsys/pkg/FR-2004-04-21/pdf/04-9054.pdf\)](https://www.gpo.gov/fdsys/pkg/FR-2004-04-21/pdf/04-9054.pdf).

[7/6/2000 \(https://www.gpo.gov/fdsys/pkg/FR-2000-07-06/pdf/00-17058.pdf\)](https://www.gpo.gov/fdsys/pkg/FR-2000-07-06/pdf/00-17058.pdf).

34 CFR PART 99—FAMILY EDUCATIONAL RIGHTS AND PRIVACY

Contents

Subpart A—General

[§99.1 To which educational agencies or institutions do these regulations apply?](#)

[§99.2 What is the purpose of these regulations?](#)

[§99.3 What definitions apply to these regulations?](#)

[§99.4 What are the rights of parents?](#)

[§99.5 What are the rights of students?](#)

[§99.6 \[Reserved\]](#)

[§99.7 What must an educational agency or institution include in its annual notification?](#)

[§99.8 What provisions apply to records of a law enforcement unit?](#)

Subpart B—What Are the Rights of Inspection and Review of Education Records?

[§99.10 What rights exist for a parent or eligible student to inspect and review education records?](#)

[§99.11 May an educational agency or institution charge a fee for copies of education records?](#)

[§99.12 What limitations exist on the right to inspect and review records?](#)

Subpart C—What Are the Procedures for Amending Education Records?

[§99.20 How can a parent or eligible student request amendment of the student's education records?](#)

[§99.21 Under what conditions does a parent or eligible student have the right to a hearing?](#)

[§99.22 What minimum requirements exist for the conduct of a hearing?](#)

Subpart D—May an Educational Agency or Institution Disclose Personally Identifiable Information From Education Records?

[§99.30 Under what conditions is prior consent required to disclose information?](#)

[§99.31 Under what conditions is prior consent not required to disclose information?](#)

[§99.32 What recordkeeping requirements exist concerning requests and disclosures?](#)

[§99.33 What limitations apply to the redisclosure of information?](#)

[§99.34 What conditions apply to disclosure of information to other educational agencies or institutions?](#)

[§99.35 What conditions apply to disclosure of information for Federal or State program purposes?](#)

[§99.36 What conditions apply to disclosure of information in health and safety emergencies?](#)

[§99.37 What conditions apply to disclosing directory information?](#)

[§99.38 What conditions apply to disclosure of information as permitted by State statute adopted after November 19, 1974, concerning the juvenile justice system?](#)

[§99.39 What definitions apply to the nonconsensual disclosure of records by postsecondary educational institutions in connection with disciplinary proceedings concerning crimes of violence or non-forcible sex offenses?](#)

Subpart E—What Are the Enforcement Procedures?

[§99.60 What functions has the Secretary delegated to the Office and to the Office of Administrative Law Judges?](#)

[§99.61 What responsibility does an educational agency or institution, a recipient of Department funds, or a third party outside of an educational agency or institution have concerning conflict with State or local laws?](#)

[§99.62 What information must an educational agency or institution or other recipient of Department funds submit to the Office?](#)

[§99.63 Where are complaints filed?](#)

[§99.64 What is the investigation procedure?](#)

[§99.65 What is the content of the notice of investigation issued by the Office?](#)

[§99.66 What are the responsibilities of the Office in the enforcement process?](#)

[§99.67 How does the Secretary enforce decisions?](#)

[Appendix A to Part 99—Crimes of Violence Definitions](#)

[Back to Top](#)

Subpart A—General

[Back to Top](#)

§99.1 To which educational agencies or institutions do these regulations apply?

(a) Except as otherwise noted in §99.10, this part applies to an educational agency or institution to which funds have been made available under any program administered by the Secretary, if—

- (1) The educational institution provides educational services or instruction, or both, to students; or
- (2) The educational agency is authorized to direct and control public elementary or secondary, or postsecondary educational institutions.

(b) This part does not apply to an educational agency or institution solely because students attending that agency or institution receive non-monetary benefits under a program referenced in paragraph (a) of this section, if no funds under that program are made available to the agency or institution.

(c) The Secretary considers funds to be made available to an educational agency or institution of funds under one or more of the programs referenced in paragraph (a) of this section—

- (1) Are provided to the agency or institution by grant, cooperative agreement, contract, subgrant, or subcontract; or
- (2) Are provided to students attending the agency or institution and the funds may be paid to the agency or institution by those students for educational purposes, such as under the Pell Grant Program and the Guaranteed Student Loan Program (titles IV-A-1 and IV-B, respectively, of the Higher Education Act of 1965, as amended).

(d) If an educational agency or institution receives funds under one or more of the programs covered by this section, the regulations in this part apply to the recipient as a whole, including each of its components (such as a department within a university).

(Authority: 20 U.S.C. 1232g)

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59295, Nov. 21, 1996; 65 FR 41852, July 6, 2000]

[Back to Top](#)

§99.2 What is the purpose of these regulations?

The purpose of this part is to set out requirements for the protection of privacy of parents and students under section 444 of the General Education Provisions Act, as amended.

(Authority: 20 U.S.C. 1232g)

Note to §99.2: 34 CFR 300.610 through 300.626 contain requirements regarding the confidentiality of information relating to children with disabilities who receive evaluations, services or other benefits under Part B of the Individuals with Disabilities Education Act (IDEA). 34 CFR 303.402 and 303.460 identify the confidentiality of information requirements regarding children and infants and toddlers with disabilities and their families who receive evaluations, services, or other benefits under Part C of IDEA. 34 CFR 300.610 through 300.627 contain the confidentiality of information requirements that apply to personally identifiable data, information, and records collected or maintained pursuant to Part B of the IDEA.

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59295, Nov. 21, 1996; 73 FR 74851, Dec. 9, 2008]

[Back to Top](#)

Appendix 2.C.4 Page 9 of 135

§99.3 What definitions apply to these regulations?

The following definitions apply to this part:

Act means the Family Educational Rights and Privacy Act of 1974, as amended, enacted as section 444 of the General Education Provisions Act.

(Authority: 20 U.S.C. 1232g)

Attendance includes, but is not limited to—

(a) Attendance in person or by paper correspondence, videoconference, satellite, Internet, or other electronic information and telecommunications technologies for students who are not physically present in the classroom; and

(b) The period during which a person is working under a work-study program.

(Authority: 20 U.S.C. 1232g)

Authorized representative means any entity or individual designated by a State or local educational authority or an agency headed by an official listed in §99.31(a)(3) to conduct—with respect to Federal- or State-supported education programs—any audit or evaluation, or any compliance or enforcement activity in connection with Federal legal requirements that relate to these programs.

(Authority: 20 U.S.C. 1232g(b)(1)(C), (b)(3), and (b)(5))

Biometric record, as used in the definition of *personally identifiable information*, means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

(Authority: 20 U.S.C. 1232g)

Dates of attendance. (a) The term means the period of time during which a student attends or attended an educational agency or institution. Examples of dates of attendance include an academic year, a spring semester, or a first quarter.

(b) The term does not include specific daily records of a student's attendance at an educational agency or institution.

(Authority: 20 U.S.C. 1232g(a)(5)(A))

Directory information means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed.

(a) Directory information includes, but is not limited to, the student's name; address; telephone listing; electronic mail address; photograph; date and place of birth; major field of study; grade level; enrollment status (e.g., undergraduate or graduate, full-time or part-time); dates of attendance; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors, and awards received; and the most recent educational agency or institution attended.

(b) Directory information does not include a student's—

(1) Social security number; or

(2) Student identification (ID) number, except as provided in paragraph (c) of this definition.

(c) In accordance with paragraphs (a) and (b) of this definition, directory information includes—

(1) A student ID number, user ID, or other unique personal identifier used by a student for purposes of accessing or communicating in electronic systems, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a personal identification number (PIN), password or other factor known or possessed only by the authorized user; and

(2) A student ID number or other unique personal identifier that is displayed on a student ID badge, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a PIN, password, or other factor known or possessed only by the authorized user.

(Authority: 20 U.S.C. 1232g(a)(5)(A))

Disciplinary action or proceeding means the investigation, adjudication, or imposition of sanctions by an educational agency or institution with respect to an infraction or violation of the internal rules of conduct applicable to students of the agency or institution.

Disclosure means to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record.

(Authority: 20 U.S.C. 1232g(b)(1) and (b)(2))

Early childhood education program means—

(a) A Head Start program or an Early Head Start program carried out under the Head Start Act (42 U.S.C. 9831 *et seq.*), including a migrant or seasonal Head Start program, an Indian Head Start program, or a Head Start program or an Early Head Start program that also receives State funding;

(b) A State licensed or regulated child care program; or

(c) A program that—

(1) Serves children from birth through age six that addresses the children's cognitive (including language, early literacy, and early mathematics), social, emotional, and physical development; and

(2) Is—

(i) A State prekindergarten program;

(ii) A program authorized under section 619 or part C of the Individuals with Disabilities Education Act; or

(iii) A program operated by a local educational agency.

Educational agency or institution means any public or private agency or institution to which this part applies under §99.1(a).

(Authority: 20 U.S.C. 1232g(a)(3))

Education program means any program that is principally engaged in the provision of education, including, but not limited to, early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, and adult education, and any program that is administered by an educational agency or institution.

(Authority: 20 U.S.C. 1232g(b)(3), (b)(5))

Education records. (a) The term means those records that are:

(1) Directly related to a student; and

(2) Maintained by an educational agency or institution or by a party acting for the agency or institution.

(b) The term does not include:

(1) Records that are kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record.

(2) Records of the law enforcement unit of an educational agency or institution, subject to the provisions of §99.8.

(3)(i) Records relating to an individual who is employed by an educational agency or institution, that:

(A) Are made and maintained in the normal course of business;

(B) Relate exclusively to the individual in that individual's capacity as an employee; and

(C) Are not available for use for any other purpose.

(ii) Records relating to an individual in attendance at the agency or institution who is employed as a result of his or her status as a student are education records and not excepted under paragraph (b)(3)(i) of this definition.

(4) Records on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are:

(i) Made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity;

(ii) Made, maintained, or used only in connection with treatment of the student; and

(iii) Disclosed only to individuals providing the treatment. For the purpose of this definition, “treatment” does not include remedial educational activities or activities that are part of the program of instruction at the agency or institution; and

(5) Records created or received by an educational agency or institution after an individual is no longer a student in attendance and that are not directly related to the individual's attendance as a student.

(6) Grades on peer-graded papers before they are collected and recorded by a teacher.

(Authority: 20 U.S.C. 1232g(a)(4))

Eligible student means a student who has reached 18 years of age or is attending an institution of postsecondary education.

(Authority: 20 U.S.C. 1232g(d))

Institution of postsecondary education means an institution that provides education to students beyond the secondary school level; “secondary school level” means the educational level (not beyond grade 12) at which secondary education is provided as determined under State law.

(Authority: 20 U.S.C. 1232g(d))

Parent means a parent of a student and includes a natural parent, a guardian, or an individual acting as a parent in the absence of a parent or a guardian.

(Authority: 20 U.S.C. 1232g)

Party means an individual, agency, institution, or organization.

(Authority: 20 U.S.C. 1232g(b)(4)(A))

Personally Identifiable Information

The term includes, but is not limited to—

- (a) The student's name;
- (b) The name of the student's parent or other family members;
- (c) The address of the student or student's family;
- (d) A personal identifier, such as the student's social security number, student number, or biometric record;
- (e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
- (f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
- (g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

(Authority: 20 U.S.C. 1232g)

Record means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.

(Authority: 20 U.S.C. 1232g)

Secretary means the Secretary of the U.S. Department of Education or an official or employee of the Department of Education acting for the Secretary under a delegation of authority.

(Authority: 20 U.S.C. 1232g)

Student, except as otherwise specifically provided in this part, means any individual who is or has been in attendance at an educational agency or institution and regarding whom the agency or institution maintains education records.

(Authority: 20 U.S.C. 1232g(a)(6))

[53 FR 11943, Apr. 11, 1988, as amended at 60 FR 3468, Jan. 17, 1995; 61 FR 59295, Nov. 21, 1996; 65 FR 41852, July 6, 2000; 73 FR 74851, Dec. 9, 2008; 76 FR 75641, Dec. 2, 2011]

[Back to Top](#)

§99.4 What are the rights of parents?

An educational agency or institution shall give full rights under the Act to either parent, unless the agency or institution has been provided with evidence that there is a court order, State statute, or legally binding document relating to such matters as divorce, separation, or custody that specifically revokes these rights.

(Authority: 20 U.S.C. 1232g)

[Back to Top](#)

§99.5 What are the rights of students?

(a)(1) When a student becomes an eligible student, the rights accorded to, and consent required of, parents under this part transfer from the parents to the student.

(2) Nothing in this section prevents an educational agency or institution from disclosing education records, or personally identifiable information from education records, to a parent without the prior written consent of an eligible student if the disclosure meets the conditions in §99.31(a)(8), §99.31(a)(10), §99.31(a)(15), or any other provision in §99.31(a).

(b) The Act and this part do not prevent educational agencies or institutions from giving students rights in addition to those given to parents.

(c) An individual who is or has been a student at an educational institution and who applies for admission at another component of that institution does not have rights under this part with respect to records maintained by that other component, including records maintained in connection with the student's application for admission, unless the student is accepted and attends that other component of the institution.

(Authority: 20 U.S.C. 1232g(d))

[53 FR 11943, Apr. 11, 1988, as amended at 58 FR 3188, Jan. 7, 1993; 65 FR 41853, July 6, 2000; 73 FR 74852, Dec. 9, 2008]

[Back to Top](#)

§99.6 [Reserved]

[Back to Top](#)

§99.7 What must an educational agency or institution include in its annual notification?

(a)(1) Each educational agency or institution shall annually notify parents of students currently in attendance, or eligible students currently in attendance, of their rights under the Act and this part.

(2) The notice must inform parents or eligible students that they have the right to—

(i) Inspect and review the student's education records;

(ii) Seek amendment of the student's education records that the parent or eligible student believes to be inaccurate, misleading, or otherwise in violation of the student's privacy rights;

(iii) Consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that the Act and §99.31 authorize disclosure without consent; and

(iv) File with the Department a complaint under §§99.63 and 99.64 concerning alleged failures by the educational agency or institution to comply with the requirements of the Act and this part.

(3) The notice must include all of the following:

(i) The procedure for exercising the right to inspect and review education records.

(ii) The procedure for requesting amendment of records under §99.20.

(iii) If the educational agency or institution has a policy of disclosing education records under §99.31(a)(1), a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest.

(b) An educational agency or institution may provide this notice by any means that are reasonably likely to inform the parents or eligible students of their rights.

(1) An educational agency or institution shall effectively notify parents or eligible students who are disabled.

(2) An agency or institution of elementary or secondary education shall effectively notify parents who have a primary or home language other than English.

(Approved by the Office of Management and Budget under control number 1880-0508)

(Authority: 20 U.S.C. 1232g (e) and (f))

[61 FR 59295, Nov. 21, 1996]

[Back to Top](#)

§99.8 What provisions apply to records of a law enforcement unit?

(a)(1) *Law enforcement unit* means any individual, office, department, division, or other component of an educational agency or institution, such as a unit of commissioned police officers or non-commissioned security guards, that is officially authorized or designated by that agency or institution to—

(i) Enforce any local, State, or Federal law, or refer to appropriate authorities a matter for enforcement of any local, State, or Federal law against any individual or organization other than the agency or institution itself; or

(ii) Maintain the physical security and safety of the agency or institution.

(2) A component of an educational agency or institution does not lose its status as a *law enforcement unit* if it also performs other, non-law enforcement functions for the agency or institution, including investigation of incidents or conduct that constitutes or leads to a disciplinary action or proceedings against the student.

(b)(1) Records of a law enforcement unit means those records, files, documents, and other materials that are—

(i) Created by a law enforcement unit;

(ii) Created for a law enforcement purpose; and

(iii) Maintained by the law enforcement unit.

(2) Records of a law enforcement unit does not mean—

- (i) Records created by a law enforcement unit for a law enforcement purpose that are maintained by a component of the educational agency or institution other than the law enforcement unit; or
 - (ii) Records created and maintained by a law enforcement unit exclusively for a non-law enforcement purpose, such as a disciplinary action or proceeding conducted by the educational agency or institution.
- (c)(1) Nothing in the Act prohibits an educational agency or institution from contacting its law enforcement unit, orally or in writing, for the purpose of asking that unit to investigate a possible violation of, or to enforce, any local, State, or Federal law.
- (2) Education records, and personally identifiable information contained in education records, do not lose their status as education records and remain subject to the Act, including the disclosure provisions of §99.30, while in the possession of the law enforcement unit.
- (d) The Act neither requires nor prohibits the disclosure by an educational agency or institution of its law enforcement unit records.

(Authority: 20 U.S.C. 1232g(a)(4)(B)(ii))

[60 FR 3469, Jan. 17, 1995]

[Back to Top](#)

Subpart B—What Are the Rights of Inspection and Review of Education Records?

[Back to Top](#)

§99.10 What rights exist for a parent or eligible student to inspect and review education records?

- (a) Except as limited under §99.12, a parent or eligible student must be given the opportunity to inspect and review the student's education records. This provision applies to—
- (1) Any educational agency or institution; and
 - (2) Any State educational agency (SEA) and its components.
- (i) For the purposes of subpart B of this part, an SEA and its components constitute an educational agency or institution.
- (ii) An SEA and its components are subject to subpart B of this part if the SEA maintains education records on students who are or have been in attendance at any school of an educational agency or institution subject to the Act and this part.
- (b) The educational agency or institution, or SEA or its component, shall comply with a request for access to records within a reasonable period of time, but not more than 45 days after it has received the request.
- (c) The educational agency or institution, or SEA or its component shall respond to reasonable requests for explanations and interpretations of the records.
- (d) If circumstances effectively prevent the parent or eligible student from exercising the right to inspect and review the student's education records, the educational agency or institution, or SEA or its component, shall—
- (1) Provide the parent or eligible student with a copy of the records requested; or
 - (2) Make other arrangements for the parent or eligible student to inspect and review the requested records.
- (e) The educational agency or institution, or SEA or its component shall not destroy any education records if there is an outstanding request to inspect and review the records under this section.
- (f) While an education agency or institution is not required to give an eligible student access to treatment records under paragraph (b)(4) of the definition of *Education records* in §99.3, the student may have those records reviewed by a physician or other appropriate professional of the student's choice.

(Authority: 20 U.S.C. 1232g(a)(1) (A) and (B))

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59296, Nov. 21, 1996]

[Back to Top](#)

§99.11 May an educational agency or institution charge a fee for copies of education records?

- (a) Unless the imposition of a fee effectively prevents a parent or eligible student from exercising the right to inspect and review the student's education records, an educational agency or institution may charge a fee for a copy of an education record which is made for the parent or eligible student.

(b) An educational agency or institution may not charge a fee to search for or to retrieve the education records of a student.

(Authority: 20 U.S.C. 1232g(a)(1))

[Back to Top](#)

§99.12 What limitations exist on the right to inspect and review records?

(a) If the education records of a student contain information on more than one student, the parent or eligible student may inspect and review or be informed of only the specific information about that student.

(b) A postsecondary institution does not have to permit a student to inspect and review education records that are:

(1) Financial records, including any information those records contain, of his or her parents;

(2) Confidential letters and confidential statements of recommendation placed in the education records of the student before January 1, 1975, as long as the statements are used only for the purposes for which they were specifically intended; and

(3) Confidential letters and confidential statements of recommendation placed in the student's education records after January 1, 1975, if:

(i) The student has waived his or her right to inspect and review those letters and statements; and

(ii) Those letters and statements are related to the student's:

(A) Admission to an educational institution;

(B) Application for employment; or

(C) Receipt of an honor or honorary recognition.

(c)(1) A waiver under paragraph (b)(3)(i) of this section is valid only if:

(i) The educational agency or institution does not require the waiver as a condition for admission to or receipt of a service or benefit from the agency or institution; and

(ii) The waiver is made in writing and signed by the student, regardless of age.

(2) If a student has waived his or her rights under paragraph (b)(3)(i) of this section, the educational institution shall:

(i) Give the student, on request, the names of the individuals who provided the letters and statements of recommendation; and

(ii) Use the letters and statements of recommendation only for the purpose for which they were intended.

(3)(i) A waiver under paragraph (b)(3)(i) of this section may be revoked with respect to any actions occurring after the revocation.

(ii) A revocation under paragraph (c)(3)(i) of this section must be in writing.

(Authority: 20 U.S.C. 1232g(a)(1) (A), (B), (C), and (D))

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59296, Nov. 21, 1996]

[Back to Top](#)

Subpart C—What Are the Procedures for Amending Education Records?

[Back to Top](#)

§99.20 How can a parent or eligible student request amendment of the student's education records?

(a) If a parent or eligible student believes the education records relating to the student contain information that is inaccurate, misleading, or in violation of the student's rights of privacy, he or she may ask the educational agency or institution to amend the record.

(b) The educational agency or institution shall decide whether to amend the record as requested within a reasonable time after the agency or institution receives the request.

(c) If the educational agency or institution decides not to amend the record as requested, it shall inform the parent or eligible student of its decision and of his or her right to a hearing under §99.21.

(Authority: 20 U.S.C. 1232g(a)(2))

[53 FR 11943, Apr. 11, 1988; 53 FR 19368, May 27, 1988, as amended at 61 FR 59296, Nov. 21, 1996]

§99.21 Under what conditions does a parent or eligible student have the right to a hearing?

(a) An educational agency or institution shall give a parent or eligible student, on request, an opportunity for a hearing to challenge the content of the student's education records on the grounds that the information contained in the education records is inaccurate, misleading, or in violation of the privacy rights of the student.

(b)(1) If, as a result of the hearing, the educational agency or institution decides that the information is inaccurate, misleading, or otherwise in violation of the privacy rights of the student, it shall:

(i) Amend the record accordingly; and

(ii) Inform the parent or eligible student of the amendment in writing.

(2) If, as a result of the hearing, the educational agency or institution decides that the information in the education record is not inaccurate, misleading, or otherwise in violation of the privacy rights of the student, it shall inform the parent or eligible student of the right to place a statement in the record commenting on the contested information in the record or stating why he or she disagrees with the decision of the agency or institution, or both.

(c) If an educational agency or institution places a statement in the education records of a student under paragraph (b)(2) of this section, the agency or institution shall:

(1) Maintain the statement with the contested part of the record for as long as the record is maintained; and

(2) Disclose the statement whenever it discloses the portion of the record to which the statement relates.

(Authority: 20 U.S.C. 1232g(a)(2))

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59296, Nov. 21, 1996]

[Back to Top](#)

§99.22 What minimum requirements exist for the conduct of a hearing?

The hearing required by §99.21 must meet, at a minimum, the following requirements:

(a) The educational agency or institution shall hold the hearing within a reasonable time after it has received the request for the hearing from the parent or eligible student.

(b) The educational agency or institution shall give the parent or eligible student notice of the date, time, and place, reasonably in advance of the hearing.

(c) The hearing may be conducted by any individual, including an official of the educational agency or institution, who does not have a direct interest in the outcome of the hearing.

(d) The educational agency or institution shall give the parent or eligible student a full and fair opportunity to present evidence relevant to the issues raised under §99.21. The parent or eligible student may, at their own expense, be assisted or represented by one or more individuals of his or her own choice, including an attorney.

(e) The educational agency or institution shall make its decision in writing within a reasonable period of time after the hearing.

(f) The decision must be based solely on the evidence presented at the hearing, and must include a summary of the evidence and the reasons for the decision.

(Authority: 20 U.S.C. 1232g(a)(2))

[Back to Top](#)

Subpart D—May an Educational Agency or Institution Disclose Personally Identifiable Information From Education Records?

[Back to Top](#)

§99.30 Under what conditions is prior consent required to disclose information?

(a) The parent or eligible student shall provide a signed and dated written consent before an educational agency or institution discloses personally identifiable information from the student's education records, except as provided in §99.31.

(b) The written consent must:

- (1) Specify the records that may be disclosed;
- (2) State the purpose of the disclosure; and
- (3) Identify the party or class of parties to whom the disclosure may be made.

(c) When a disclosure is made under paragraph (a) of this section:

- (1) If a parent or eligible student so requests, the educational agency or institution shall provide him or her with a copy of the records disclosed; and
- (2) If the parent of a student who is not an eligible student so requests, the agency or institution shall provide the student with a copy of the records disclosed.

(d) "Signed and dated written consent" under this part may include a record and signature in electronic form that—

- (1) Identifies and authenticates a particular person as the source of the electronic consent; and
- (2) Indicates such person's approval of the information contained in the electronic consent.

(Authority: 20 U.S.C. 1232g (b)(1) and (b)(2)(A))

[53 FR 11943, Apr. 11, 1988, as amended at 58 FR 3189, Jan. 7, 1993; 69 FR 21671, Apr. 21, 2004]

[Back to Top](#)

§99.31 Under what conditions is prior consent not required to disclose information?

(a) An educational agency or institution may disclose personally identifiable information from an education record of a student without the consent required by §99.30 if the disclosure meets one or more of the following conditions:

(1)(i)(A) The disclosure is to other school officials, including teachers, within the agency or institution whom the agency or institution has determined to have legitimate educational interests.

(B) A contractor, consultant, volunteer, or other party to whom an agency or institution has outsourced institutional services or functions may be considered a school official under this paragraph provided that the outside party—

(1) Performs an institutional service or function for which the agency or institution would otherwise use employees;

(2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and

(3) Is subject to the requirements of §99.33(a) governing the use and redisclosure of personally identifiable information from education records.

(ii) An educational agency or institution must use reasonable methods to ensure that school officials obtain access to only those education records in which they have legitimate educational interests. An educational agency or institution that does not use physical or technological access controls must ensure that its administrative policy for controlling access to education records is effective and that it remains in compliance with the legitimate educational interest requirement in paragraph (a)(1)(i)(A) of this section.

(2) The disclosure is, subject to the requirements of §99.34, to officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer.

Note: Section 4155(b) of the No Child Left Behind Act of 2001, 20 U.S.C. 7165(b), requires each State to assure the Secretary of Education that it has a procedure in place to facilitate the transfer of disciplinary records with respect to a suspension or expulsion of a student by a local educational agency to any private or public elementary or secondary school in which the student is subsequently enrolled or seeks, intends, or is instructed to enroll.

(3) The disclosure is, subject to the requirements of §99.35, to authorized representatives of—

(i) The Comptroller General of the United States;

(ii) The Attorney General of the United States;

(iii) The Secretary; or

(iv) State and local educational authorities.

(4)(i) The disclosure is in connection with financial aid for which the student has applied or which the student has received, if the information is necessary for such purposes as to:

(A) Determine eligibility for the aid;

(B) Determine the amount of the aid;

(C) Determine the conditions for the aid; or

(D) Enforce the terms and conditions of the aid.

(ii) As used in paragraph (a)(4)(i) of this section, *financial aid* means a payment of funds provided to an individual (or a payment in kind of tangible or intangible property to the individual) that is conditioned on the individual's attendance at an educational agency or institution.

(Authority: 20 U.S.C. 1232g(b)(1)(D))

(5)(i) The disclosure is to State and local officials or authorities to whom this information is specifically—

(A) Allowed to be reported or disclosed pursuant to State statute adopted before November 19, 1974, if the allowed reporting or disclosure concerns the juvenile justice system and the system's ability to effectively serve the student whose records are released; or

(B) Allowed to be reported or disclosed pursuant to State statute adopted after November 19, 1974, subject to the requirements of §99.38.

(ii) Paragraph (a)(5)(i) of this section does not prevent a State from further limiting the number or type of State or local officials to whom disclosures may be made under that paragraph.

(6)(i) The disclosure is to organizations conducting studies for, or on behalf of, educational agencies or institutions to:

(A) Develop, validate, or administer predictive tests;

(B) Administer student aid programs; or

(C) Improve instruction.

(ii) Nothing in the Act or this part prevents a State or local educational authority or agency headed by an official listed in paragraph (a)(3) of this section from entering into agreements with organizations conducting studies under paragraph (a)(6)(i) of this section and redisclosing personally identifiable information from education records on behalf of educational agencies and institutions that disclosed the information to the State or local educational authority or agency headed by an official listed in paragraph (a)(3) of this section in accordance with the requirements of §99.33(b).

(iii) An educational agency or institution may disclose personally identifiable information under paragraph (a)(6)(i) of this section, and a State or local educational authority or agency headed by an official listed in paragraph (a)(3) of this section may redisclose personally identifiable information under paragraph (a)(6)(i) and (a)(6)(ii) of this section, only if—

(A) The study is conducted in a manner that does not permit personal identification of parents and students by individuals other than representatives of the organization that have legitimate interests in the information;

(B) The information is destroyed when no longer needed for the purposes for which the study was conducted; and

(C) The educational agency or institution or the State or local educational authority or agency headed by an official listed in paragraph (a)(3) of this section enters into a written agreement with the organization that—

(1) Specifies the purpose, scope, and duration of the study or studies and the information to be disclosed;

(2) Requires the organization to use personally identifiable information from education records only to meet the purpose or purposes of the study as stated in the written agreement;

(3) Requires the organization to conduct the study in a manner that does not permit personal identification of parents and students, as defined in this part, by anyone other than representatives of the organization with legitimate interests;

and

(4) Requires the organization to destroy all personally identifiable information when the information is no longer needed for the purposes for which the study was conducted and specifies the time period in which the information must be destroyed.

(iv) An educational agency or institution or State or local educational authority or Federal agency headed by an official listed in paragraph (a)(3) of this section is not required to initiate a study or agree with or endorse the conclusions or results of the study.

(v) For the purposes of paragraph (a)(6) of this section, the term *organization* includes, but is not limited to, Federal, State, and local agencies, and independent organizations.

(7) The disclosure is to accrediting organizations to carry out their accrediting functions.

(8) The disclosure is to parents, as defined in §99.3, of a dependent student, as defined in section 152 of the Internal Revenue Code of 1986.

(9)(i) The disclosure is to comply with a judicial order or lawfully issued subpoena.

(ii) The educational agency or institution may disclose information under paragraph (a)(9)(i) of this section only if the agency or institution makes a reasonable effort to notify the parent or eligible student of the order or subpoena in advance of compliance, so that the parent or eligible student may seek protective action, unless the disclosure is in compliance with—

(A) A Federal grand jury subpoena and the court has ordered that the existence or the contents of the subpoena or the information furnished in response to the subpoena not be disclosed;

(B) Any other subpoena issued for a law enforcement purpose and the court or other issuing agency has ordered that the existence or the contents of the subpoena or the information furnished in response to the subpoena not be disclosed; or

(C) An *ex parte* court order obtained by the United States Attorney General (or designee not lower than an Assistant Attorney General) concerning investigations or prosecutions of an offense listed in 18 U.S.C. 2332b(g)(5)(B) or an act of domestic or international terrorism as defined in 18 U.S.C. 2331.

(iii)(A) If an educational agency or institution initiates legal action against a parent or student, the educational agency or institution may disclose to the court, without a court order or subpoena, the education records of the student that are relevant for the educational agency or institution to proceed with the legal action as plaintiff.

(B) If a parent or eligible student initiates legal action against an educational agency or institution, the educational agency or institution may disclose to the court, without a court order or subpoena, the student's education records that are relevant for the educational agency or institution to defend itself.

(10) The disclosure is in connection with a health or safety emergency, under the conditions described in §99.36.

(11) The disclosure is information the educational agency or institution has designated as “directory information”, under the conditions described in §99.37.

(12) The disclosure is to the parent of a student who is not an eligible student or to the student.

(13) The disclosure, subject to the requirements in §99.39, is to a victim of an alleged perpetrator of a crime of violence or a non-forcible sex offense. The disclosure may only include the final results of the disciplinary proceeding conducted by the institution of postsecondary education with respect to that alleged crime or offense. The institution may disclose the final results of the disciplinary proceeding, regardless of whether the institution concluded a violation was committed.

(14)(i) The disclosure, subject to the requirements in §99.39, is in connection with a disciplinary proceeding at an institution of postsecondary education. The institution must not disclose the final results of the disciplinary proceeding unless it determines that—

(A) The student is an alleged perpetrator of a crime of violence or non-forcible sex offense; and

(B) With respect to the allegation made against him or her, the student has committed a violation of the institution's rules or policies.

(ii) The institution may not disclose the name of any other student, including a victim or witness, without the prior written consent of the other student.

(iii) This section applies only to disciplinary proceedings in which the final results were reached on or after October 7, 1998.

(15)(i) The disclosure is to a parent of a student at an institution of postsecondary education regarding the student's violation of any Federal, State, or local law, or of any rule or policy of the institution, governing the use or possession of alcohol or a controlled substance if—

(A) The institution determines that the student has committed a disciplinary violation with respect to that use or possession; and

(B) The student is under the age of 21 at the time of the disclosure to the parent.

(ii) Paragraph (a)(15) of this section does not supersede any provision of State law that prohibits an institution of postsecondary education from disclosing information.

(16) The disclosure concerns sex offenders and other individuals required to register under section 170101 of the Violent Crime Control and Law Enforcement Act of 1994, 42 U.S.C. 14071, and the information was provided to the educational agency or institution under 42 U.S.C. 14071 and applicable Federal guidelines.

(b)(1) *De-identified records and information.* An educational agency or institution, or a party that has received education records or information from education records under this part, may release the records or information without the consent required by §99.30 after the removal of all personally identifiable information provided that the educational agency or institution or other party has made a reasonable determination that a student's identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information.

(2) An educational agency or institution, or a party that has received education records or information from education records under this part, may release de-identified student level data from education records for the purpose of education research by attaching a code to each record that may allow the

recipient to match information received from the same source, provided that—

(i) An educational agency or institution or other party that releases de-identified data under paragraph (b) (2) of this section does not disclose any information about how it generates and assigns a record code, or that would allow a recipient to identify a student based on a record code;

(ii) The record code is used for no purpose other than identifying a de-identified record for purposes of education research and cannot be used to ascertain personally identifiable information about a student; and

(iii) The record code is not based on a student's social security number or other personal information.

(c) An educational agency or institution must use reasonable methods to identify and authenticate the identity of parents, students, school officials, and any other parties to whom the agency or institution discloses personally identifiable information from education records.

(d) Paragraphs (a) and (b) of this section do not require an educational agency or institution or any other party to disclose education records or information from education records to any party except for parties under paragraph (a)(12) of this section.

(Authority: 20 U.S.C. 1232g(a)(5)(A), (b), (h), (i), and (j)).

[53 FR 11943, Apr. 11, 1988; 53 FR 19368, May 27, 1988, as amended at 58 FR 3189, Jan. 7, 1993; 61 FR 59296, Nov. 21, 1996; 65 FR 41853, July 6, 2000; 73 FR 74852, Dec. 9, 2008; 74 FR 401, Jan. 6, 2009; 76 FR 75641, Dec. 2, 2011]

[Back to Top](#)

§99.32 What recordkeeping requirements exist concerning requests and disclosures?

(a)(1) An educational agency or institution must maintain a record of each request for access to and each disclosure of personally identifiable information from the education records of each student, as well as the names of State and local educational authorities and Federal officials and agencies listed in §99.31(a) (3) that may make further disclosures of personally identifiable information from the student's education records without consent under §99.33(b).

(2) The agency or institution shall maintain the record with the education records of the student as long as the records are maintained.

(3) For each request or disclosure the record must include:

(i) The parties who have requested or received personally identifiable information from the education records; and

(ii) The legitimate interests the parties had in requesting or obtaining the information.

(4) An educational agency or institution must obtain a copy of the record of further disclosures maintained under paragraph (b)(2) of this section and make it available in response to a parent's or eligible student's request to review the record required under paragraph (a)(1) of this section.

(5) An educational agency or institution must record the following information when it discloses personally identifiable information from education records under the health or safety emergency exception in §99.31(a)(10) and §99.36:

(i) The articulable and significant threat to the health or safety of a student or other individuals that formed the basis for the disclosure; and

(ii) The parties to whom the agency or institution disclosed the information.

(b)(1) Except as provided in paragraph (b)(2) of this section, if an educational agency or institution discloses personally identifiable information from education records with the understanding authorized under §99.33(b), the record of the disclosure required under this section must include:

(i) The names of the additional parties to which the receiving party may disclose the information on behalf of the educational agency or institution; and

(ii) The legitimate interests under §99.31 which each of the additional parties has in requesting or obtaining the information.

(2)(i) A State or local educational authority or Federal official or agency listed in §99.31(a)(3) that makes further disclosures of information from education records under §99.33(b) must record the names of the additional parties to which it discloses information on behalf of an educational agency or institution and their legitimate interests in the information under §99.31 if the information was received from:

(A) An educational agency or institution that has not recorded the further disclosures under paragraph (b) (1) of this section; or

(B) Another State or local educational authority or Federal official or agency listed in §99.31(a)(3).

(ii) A State or local educational authority or Federal official or agency that records further disclosures of information under paragraph (b)(2)(i) of this section may maintain the record by the student's class, school, district, or other appropriate grouping rather than by the name of the student.

(iii) Upon request of an educational agency or institution, a State or local educational authority or Federal official or agency listed in §99.31(a)(3) that maintains a record of further disclosures under paragraph (b)(2)(i) of this section must provide a copy of the record of further disclosures to the educational agency or institution within a reasonable period of time not to exceed 30 days.

(c) The following parties may inspect the record relating to each student:

- (1) The parent or eligible student.
- (2) The school official or his or her assistants who are responsible for the custody of the records.
- (3) Those parties authorized in §99.31(a) (1) and (3) for the purposes of auditing the recordkeeping procedures of the educational agency or institution.

(d) Paragraph (a) of this section does not apply if the request was from, or the disclosure was to:

- (1) The parent or eligible student;
- (2) A school official under §99.31(a)(1);
- (3) A party with written consent from the parent or eligible student;
- (4) A party seeking directory information; or
- (5) A party seeking or receiving records in accordance with §99.31(a)(9)(ii)(A) through (C).

(Approved by the Office of Management and Budget under control number 1880-0508)

(Authority: 20 U.S.C. 1232g(b)(1) and (b)(4)(A))

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59297, Nov. 21, 1996; 73 FR 74853, Dec. 9, 2008]

[Back to Top](#)

§99.33 What limitations apply to the redisclosure of information?

(a)(1) An educational agency or institution may disclose personally identifiable information from an education record only on the condition that the party to whom the information is disclosed will not disclose the information to any other party without the prior consent of the parent or eligible student.

(2) The officers, employees, and agents of a party that receives information under paragraph (a)(1) of this section may use the information, but only for the purposes for which the disclosure was made.

(b)(1) Paragraph (a) of this section does not prevent an educational agency or institution from disclosing personally identifiable information with the understanding that the party receiving the information may make further disclosures of the information on behalf of the educational agency or institution if—

- (i) The disclosures meet the requirements of §99.31; and
- (ii)(A) The educational agency or institution has complied with the requirements of §99.32(b); or

(B) A State or local educational authority or Federal official or agency listed in §99.31(a)(3) has complied with the requirements of §99.32(b)(2).

(2) A party that receives a court order or lawfully issued subpoena and rediscloses personally identifiable information from education records on behalf of an educational agency or institution in response to that order or subpoena under §99.31(a)(9) must provide the notification required under §99.31(a)(9)(ii).

(c) Paragraph (a) of this section does not apply to disclosures under §§99.31(a)(8), (9), (11), (12), (14), (15), and (16), and to information that postsecondary institutions are required to disclose under the Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act, 20 U.S.C. 1092(f) (Clery Act), to the accuser and accused regarding the outcome of any campus disciplinary proceeding brought alleging a sexual offense.

(d) An educational agency or institution must inform a party to whom disclosure is made of the requirements of paragraph (a) of this section except for disclosures made under §§99.31(a)(8), (9), (11), (12), (14), (15), and (16), and to information that postsecondary institutions are required to disclose under the Clery Act to the accuser and accused regarding the outcome of any campus disciplinary proceeding brought alleging a sexual offense.

(Authority: 20 U.S.C. 1232g(b)(4)(B))

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59297, Nov. 21, 1996; 65 FR 41853, July 6, 2000; 73 FR 74853, Dec. 9, 2008; 76 FR 75642, Dec. 2, 2011]

[Back to Top](#)

§99.34 What conditions apply to disclosure of information to other educational agencies or institutions?

(a) An educational agency or institution that discloses an education record under §99.31(a)(2) shall:

(1) Make a reasonable attempt to notify the parent or eligible student at the last known address of the parent or eligible student, unless:

(i) The disclosure is initiated by the parent or eligible student; or

(ii) The annual notification of the agency or institution under §99.7 includes a notice that the agency or institution forwards education records to other agencies or institutions that have requested the records and in which the student seeks or intends to enroll or is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer;

(2) Give the parent or eligible student, upon request, a copy of the record that was disclosed; and

(3) Give the parent or eligible student, upon request, an opportunity for a hearing under subpart C.

(b) An educational agency or institution may disclose an education record of a student in attendance to another educational agency or institution if:

(1) The student is enrolled in or receives services from the other agency or institution; and

(2) The disclosure meets the requirements of paragraph (a) of this section.

(Authority: 20 U.S.C. 1232g(b)(1)(B))

[53 FR 11943, Apr. 11, 1988, as amended at 61 FR 59297, Nov. 21, 1996; 73 FR 74854, Dec. 9, 2008]

[Back to Top](#)

§99.35 What conditions apply to disclosure of information for Federal or State program purposes?

(a)(1) Authorized representatives of the officials or agencies headed by officials listed in §99.31(a)(3) may have access to education records in connection with an audit or evaluation of Federal or State supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs.

(2) The State or local educational authority or agency headed by an official listed in §99.31(a)(3) is responsible for using reasonable methods to ensure to the greatest extent practicable that any entity or individual designated as its authorized representative—

(i) Uses personally identifiable information only to carry out an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements related to these programs;

(ii) Protects the personally identifiable information from further disclosures or other uses, except as authorized in paragraph (b)(1) of this section; and

(iii) Destroys the personally identifiable information in accordance with the requirements of paragraphs (b) and (c) of this section.

(3) The State or local educational authority or agency headed by an official listed in §99.31(a)(3) must use a written agreement to designate any authorized representative, other than an employee. The written agreement must—

(i) Designate the individual or entity as an authorized representative;

(ii) Specify—

(A) The personally identifiable information from education records to be disclosed;

(B) That the purpose for which the personally identifiable information from education records is disclosed to the authorized representative is to carry out an audit or evaluation of Federal- or State-supported education programs, or to enforce or to comply with Federal legal requirements that relate to those programs; and

(C) A description of the activity with sufficient specificity to make clear that the work falls within the exception of §99.31(a)(3), including a description of how the personally identifiable information from education records will be used;

(iii) Require the authorized representative to destroy personally identifiable information from education records when the information is no longer needed for the purpose specified;

(iv) Specify the time period in which the information must be destroyed; and

(v) Establish policies and procedures, consistent with the Act and other Federal and State confidentiality and privacy provisions, to protect personally identifiable information from education records from further disclosure (except back to the disclosing entity) and unauthorized use, including limiting use of personally

identifiable information from education records to only authorized representatives with legitimate interests in the audit or evaluation of a Federal- or State-supported education program or for compliance or enforcement of Federal legal requirements related to these programs.

(b) Information that is collected under paragraph (a) of this section must—

(1) Be protected in a manner that does not permit personal identification of individuals by anyone other than the State or local educational authority or agency headed by an official listed in §99.31(a)(3) and their authorized representatives, except that the State or local educational authority or agency headed by an official listed in §99.31(a)(3) may make further disclosures of personally identifiable information from education records on behalf of the educational agency or institution in accordance with the requirements of §99.33(b); and

(2) Be destroyed when no longer needed for the purposes listed in paragraph (a) of this section.

(c) Paragraph (b) of this section does not apply if:

(1) The parent or eligible student has given written consent for the disclosure under §99.30; or

(2) The collection of personally identifiable information is specifically authorized by Federal law.

(Authority: 20 U.S.C. 1232g(b)(1)(C), (b)(3), and (b)(5))

[53 FR 11943, Apr. 11, 1988, as amended at 73 FR 74854, Dec. 9, 2008; 76 FR 75642, Dec. 2, 2011]

[Back to Top](#)

§99.36 What conditions apply to disclosure of information in health and safety emergencies?

(a) An educational agency or institution may disclose personally identifiable information from an education record to appropriate parties, including parents of an eligible student, in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals.

(b) Nothing in this Act or this part shall prevent an educational agency or institution from—

(1) Including in the education records of a student appropriate information concerning disciplinary action taken against the student for conduct that posed a significant risk to the safety or well-being of that student, other students, or other members of the school community;

(2) Disclosing appropriate information maintained under paragraph (b)(1) of this section to teachers and school officials within the agency or institution who the agency or institution has determined have legitimate educational interests in the behavior of the student; or

(3) Disclosing appropriate information maintained under paragraph (b)(1) of this section to teachers and school officials in other schools who have been determined to have legitimate educational interests in the behavior of the student.

(c) In making a determination under paragraph (a) of this section, an educational agency or institution may take into account the totality of the circumstances pertaining to a threat to the health or safety of a student or other individuals. If the educational agency or institution determines that there is an articulable and significant threat to the health or safety of a student or other individuals, it may disclose information from education records to any person whose knowledge of the information is necessary to protect the health or safety of the student or other individuals. If, based on the information available at the time of the determination, there is a rational basis for the determination, the Department will not substitute its judgment for that of the educational agency or institution in evaluating the circumstances and making its determination.

(Authority: 20 U.S.C. 1232g (b)(1)(I) and (h))

[53 FR 11943, Apr. 11, 1988; 53 FR 19368, May 27, 1988, as amended at 61 FR 59297, Nov. 21, 1996; 73 FR 74854, Dec. 9, 2008]

[Back to Top](#)

§99.37 What conditions apply to disclosing directory information?

(a) An educational agency or institution may disclose directory information if it has given public notice to parents of students in attendance and eligible students in attendance at the agency or institution of:

(1) The types of personally identifiable information that the agency or institution has designated as directory information;

(2) A parent's or eligible student's right to refuse to let the agency or institution designate any or all of those types of information about the student as directory information; and

(3) The period of time within which a parent or eligible student has to notify the agency or institution in writing that he or she does not want any or all of those types of information about the student designated as directory information.

(b) An educational agency or institution may disclose directory information about former students without complying with the notice and opt out conditions in paragraph (a) of this section. However, the agency or institution must continue to honor any valid request to opt out of the disclosure of directory information made while a student was in attendance unless the student rescinds the opt out request.

(c) A parent or eligible student may not use the right under paragraph (a)(2) of this section to opt out of directory information disclosures to—

(1) Prevent an educational agency or institution from disclosing or requiring a student to disclose the student's name, identifier, or institutional email address in a class in which the student is enrolled; or

(2) Prevent an educational agency or institution from requiring a student to wear, to display publicly, or to disclose a student ID card or badge that exhibits information that may be designated as directory information under §99.3 and that has been properly designated by the educational agency or institution as directory information in the public notice provided under paragraph (a)(1) of this section.

(d) In its public notice to parents and eligible students in attendance at the agency or institution that is described in paragraph (a) of this section, an educational agency or institution may specify that disclosure of directory information will be limited to specific parties, for specific purposes, or both. When an educational agency or institution specifies that disclosure of directory information will be limited to specific parties, for specific purposes, or both, the educational agency or institution must limit its directory information disclosures to those specified in its public notice that is described in paragraph (a) of this section.

(e) An educational agency or institution may not disclose or confirm directory information without meeting the written consent requirements in §99.30 if a student's social security number or other non-directory information is used alone or combined with other data elements to identify or help identify the student or the student's records.

(Authority: 20 U.S.C. 1232g(a)(5) (A) and (B))

[53 FR 11943, Apr. 11, 1988, as amended at 73 FR 74854, Dec. 9, 2008; 76 FR 75642, Dec. 2, 2011]

[Back to Top](#)

§99.38 What conditions apply to disclosure of information as permitted by State statute adopted after November 19, 1974, concerning the juvenile justice system?

(a) If reporting or disclosure allowed by State statute concerns the juvenile justice system and the system's ability to effectively serve, prior to adjudication, the student whose records are released, an educational agency or institution may disclose education records under §99.31(a)(5)(i)(B).

(b) The officials and authorities to whom the records are disclosed shall certify in writing to the educational agency or institution that the information will not be disclosed to any other party, except as provided under State law, without the prior written consent of the parent of the student.

(Authority: 20 U.S.C. 1232g(b)(1)(J))

[61 FR 59297, Nov. 21, 1996]

[Back to Top](#)

§99.39 What definitions apply to the nonconsensual disclosure of records by postsecondary educational institutions in connection with disciplinary proceedings concerning crimes of violence or non-forcible sex offenses?

As used in this part:

Alleged perpetrator of a crime of violence is a student who is alleged to have committed acts that would, if proven, constitute any of the following offenses or attempts to commit the following offenses that are defined in appendix A to this part:

Arson

Assault offenses

Burglary

Criminal homicide—manslaughter by negligence

Criminal homicide—murder and nonnegligent manslaughter

Destruction/damage/vandalism of property

Kidnapping/abduction

Robbery

Forcible sex offenses.

Alleged perpetrator of a nonforcible sex offense means a student who is alleged to have committed acts that, if proven, would constitute statutory rape or incest. These offenses are defined in appendix A to this part.

Final results means a decision or determination, made by an honor court or council, committee, commission, or other entity authorized to resolve disciplinary matters within the institution. The disclosure of final results must include only the name of the student, the violation committed, and any sanction imposed by the institution against the student.

Sanction imposed means a description of the disciplinary action taken by the institution, the date of its imposition, and its duration.

Violation committed means the institutional rules or code sections that were violated and any essential findings supporting the institution's conclusion that the violation was committed.

(Authority: 20 U.S.C. 1232g(b)(6))

[65 FR 41853, July 6, 2000]

[Back to Top](#)

Subpart E—What Are the Enforcement Procedures?

[Back to Top](#)

§99.60 What functions has the Secretary delegated to the Office and to the Office of Administrative Law Judges?

(a) For the purposes of this subpart, *Office* means the Office of the Chief Privacy Officer, U.S. Department of Education.

(b) The Secretary designates the Office to:

- (1) Investigate, process, and review complaints and violations under the Act and this part; and
- (2) Provide technical assistance to ensure compliance with the Act and this part.

(c) The Secretary designates the Office of Administrative Law Judges to act as the Review Board required under the Act to enforce the Act with respect to all applicable programs. The term *applicable program* is defined in section 400 of the General Education Provisions Act.

(Authority: 20 U.S.C. 1232g (f) and (g), 1234)

[53 FR 11943, Apr. 11, 1988, as amended at 58 FR 3189, Jan. 7, 1993; 82 FR 6253, Jan. 19, 2017]

[Back to Top](#)

§99.61 What responsibility does an educational agency or institution, a recipient of Department funds, or a third party outside of an educational agency or institution have concerning conflict with State or local laws?

If an educational agency or institution determines that it cannot comply with the Act or this part due to a conflict with State or local law, it must notify the Office within 45 days, giving the text and citation of the conflicting law. If another recipient of Department funds under any program administered by the Secretary or a third party to which personally identifiable information from education records has been non-consensually disclosed determines that it cannot comply with the Act or this part due to a conflict with State or local law, it also must notify the Office within 45 days, giving the text and citation of the conflicting law.

(Authority: 20 U.S.C. 1232g(f))

[76 FR 75642, Dec. 2, 2011]

[Back to Top](#)

§99.62 What information must an educational agency or institution or other recipient of Department funds submit to the Office?

The Office may require an educational agency or institution, other recipient of Department funds under any program administered by the Secretary to which personally identifiable information from education records is non-consensually disclosed, or any third party outside of an educational agency or institution to which personally identifiable information from education records is non-consensually disclosed to submit reports, information on policies and procedures, annual notifications, training materials, or other information necessary to carry out the Office's enforcement responsibilities under the Act or this part.

(Authority: 20 U.S.C. 1232g(b)(4)(B), (f), and (g))

[76 FR 75643, Dec. 2, 2011]

[Back to Top](#)

§99.63 Where are complaints filed?

A parent or eligible student may file a written complaint with the Office regarding an alleged violation under the Act and this part. The Office's address is: Family Policy Compliance Office, U.S. Department of Education, 400 Maryland Avenue, SW., Washington, DC 20202.

(Authority: 20 U.S.C. 1232g(g))

[65 FR 41854, July 6, 2000, as amended at 73 FR 74854, Dec. 9, 2008]

[Back to Top](#)

§99.64 What is the investigation procedure?

(a) A complaint must contain specific allegations of fact giving reasonable cause to believe that a violation of the Act or this part has occurred. A complaint does not have to allege that a violation is based on a policy or practice of the educational agency or institution, other recipient of Department funds under any program administered by the Secretary, or any third party outside of an educational agency or institution.

(b) The Office investigates a timely complaint filed by a parent or eligible student, or conducts its own investigation when no complaint has been filed or a complaint has been withdrawn, to determine whether an educational agency or institution or other recipient of Department funds under any program administered by the Secretary has failed to comply with a provision of the Act or this part. If the Office determines that an educational agency or institution or other recipient of Department funds under any program administered by the Secretary has failed to comply with a provision of the Act or this part, it may also determine whether the failure to comply is based on a policy or practice of the agency or institution or other recipient. The Office also investigates a timely complaint filed by a parent or eligible student, or conducts its own investigation when no complaint has been filed or a complaint has been withdrawn, to determine whether a third party outside of the educational agency or institution has failed to comply with the provisions of §99.31(a)(6)(iii)(B) or has improperly redisclosed personally identifiable information from education records in violation of §99.33.

(Authority: 20 U.S.C. 1232g(b)(4)(B), (f) and (g))

(c) A timely complaint is defined as an allegation of a violation of the Act that is submitted to the Office within 180 days of the date of the alleged violation or of the date that the complainant knew or reasonably should have known of the alleged violation.

(d) The Office may extend the time limit in this section for good cause shown.

(Authority: 20 U.S.C. 1232g(b)(4)(B), (f) and (g))

[53 FR 11943, Apr. 11, 1988, as amended at 58 FR 3189, Jan. 7, 1993; 65 FR 41854, July 6, 2000; 73 FR 74854, Dec. 9, 2008; 76 FR 75643, Dec. 2, 2011]

[Back to Top](#)

§99.65 What is the content of the notice of investigation issued by the Office?

(a) The Office notifies in writing the complainant, if any, and the educational agency or institution, the recipient of Department funds under any program administered by the Secretary, or the third party outside of an educational agency or institution if it initiates an investigation under §99.64(b). The written notice—

(1) Includes the substance of the allegations against the educational agency or institution, other recipient, or third party; and

(2) Directs the agency or institution, other recipient, or third party to submit a written response and other relevant information, as set forth in §99.62, within a specified period of time, including information about its policies and practices regarding education records.

(b) The Office notifies the complainant if it does not initiate an investigation because the complaint fails to meet the requirements of §99.64.

(Authority: 20 U.S.C. 1232g(g))

[73 FR 74855, Dec. 9, 2008, as amended at 76 FR 75643, Dec. 2, 2011]

[Back to Top](#)

§99.66 What are the responsibilities of the Office in the enforcement process?

(a) The Office reviews a complaint, if any, information submitted by the educational agency or institution, other recipient of Department funds under any program administered by the Secretary, or third party outside of an educational agency or institution, and any other relevant information. The Office may permit the parties to submit further written or oral arguments or information.

(b) Following its investigation, the Office provides to the complainant, if any, and the educational agency or institution, other recipient, or third party a written notice of its findings and the basis for its findings.

(c) If the Office finds that an educational agency or institution or other recipient has not complied with a provision of the Act or this part, it may also find that the failure to comply was based on a policy or practice of the agency or institution or other recipient. A notice of findings issued under paragraph (b) of this section to an educational agency or institution, or other recipient that has not complied with a provision of the Act or this part—

(1) Includes a statement of the specific steps that the agency or institution or other recipient must take to comply; and

(2) Provides a reasonable period of time, given all of the circumstances of the case, during which the educational agency or institution or other recipient may comply voluntarily.

(d) If the Office finds that a third party outside of an educational agency or institution has not complied with the provisions of §99.31(a)(6)(iii)(B) or has improperly redisclosed personally identifiable information from education records in violation of §99.33, the Office's notice of findings issued under paragraph (b) of this section—

(1) Includes a statement of the specific steps that the third party outside of the educational agency or institution must take to comply; and

(2) Provides a reasonable period of time, given all of the circumstances of the case, during which the third party may comply voluntarily.

(Authority: 20 U.S.C. 1232g(b)(4)(B), (f), and (g))

[76 FR 75643, Dec. 2, 2011]

[Back to Top](#)

§99.67 How does the Secretary enforce decisions?

(a) If an educational agency or institution or other recipient of Department funds under any program administered by the Secretary does not comply during the period of time set under §99.66(c), the Secretary may take any legally available enforcement action in accordance with the Act, including, but not limited to, the following enforcement actions available in accordance with part D of the General Education Provisions Act—

(1) Withhold further payments under any applicable program;

(2) Issue a complaint to compel compliance through a cease and desist order; or

(3) Terminate eligibility to receive funding under any applicable program.

(b) If, after an investigation under §99.66, the Secretary finds that an educational agency or institution, other recipient, or third party has complied voluntarily with the Act or this part, the Secretary provides the complainant and the agency or institution, other recipient, or third party with written notice of the decision and the basis for the decision.

(c) If the Office finds that a third party, outside the educational agency or institution, violates §99.31(a)(6)(iii)(B), then the educational agency or institution from which the personally identifiable information originated may not allow the third party found to be responsible for the violation of §99.31(a)(6)(iii)(B) access to personally identifiable information from education records for at least five years.

(d) If the Office finds that a State or local educational authority, a Federal agency headed by an official listed in §99.31(a)(3), or an authorized representative of a State or local educational authority or a Federal agency headed by an official listed in §99.31(a)(3), improperly rediscloses personally identifiable information from education records, then the educational agency or institution from which the personally identifiable information originated may not allow the third party found to be responsible for the improper redisclosure access to personally identifiable information from education records for at least five years.

(e) If the Office finds that a third party, outside the educational agency or institution, improperly rediscloses personally identifiable information from education records in violation of §99.33 or fails to provide the notification required under §99.33(b)(2), then the educational agency or institution from which the personally identifiable information originated may not allow the third party found to be responsible for the violation access to personally identifiable information from education records for at least five years.

(Authority: 20 U.S.C. 1232g(b)(4)(B) and (f); 20 U.S.C. 1234c)

[76 FR 75643, Dec. 2, 2011]

[Back to Top](#)

Appendix A to Part 99—Crimes of Violence Definitions

Arson

Any willful or malicious burning or attempt to burn, with or without intent to defraud, a dwelling house, public building, motor vehicle or aircraft, personal property of another, etc.

Assault Offenses

An unlawful attack by one person upon another.

Note: By definition there can be no “attempted” assaults, only “completed” assaults.

(a) *Aggravated Assault*. An unlawful attack by one person upon another for the purpose of inflicting severe or aggravated bodily injury. This type of assault usually is accompanied by the use of a weapon or by means likely to produce death or great bodily harm. (It is not necessary that injury result from an aggravated assault when a gun, knife, or other weapon is used which could and probably would result in serious injury if the crime were successfully completed.)

(b) *Simple Assault*. An unlawful physical attack by one person upon another where neither the offender displays a weapon, nor the victim suffers obvious severe or aggravated bodily injury involving apparent broken bones, loss of teeth, possible internal injury, severe laceration, or loss of consciousness.

(c) *Intimidation*. To unlawfully place another person in reasonable fear of bodily harm through the use of threatening words or other conduct, or both, but without displaying a weapon or subjecting the victim to actual physical attack.

Note: This offense includes stalking.

Burglary

The unlawful entry into a building or other structure with the intent to commit a felony or a theft.

Criminal Homicide—Manslaughter by Negligence

The killing of another person through gross negligence.

Criminal Homicide—Murder and Nonnegligent Manslaughter

The willful (nonnegligent) killing of one human being by another.

Destruction/Damage/Vandalism of Property

To willfully or maliciously destroy, damage, deface, or otherwise injure real or personal property without the consent of the owner or the person having custody or control of it.

Kidnapping/Abduction

The unlawful seizure, transportation, or detention of a person, or any combination of these actions, against his or her will, or of a minor without the consent of his or her custodial parent(s) or legal guardian.

Note: Kidnapping/Abduction includes hostage taking.

Robbery

The taking of, or attempting to take, anything of value under confrontational circumstances from the control, custody, or care of a person or persons by force or threat of force or violence or by putting the victim in fear.

Note: Carjackings are robbery offenses where a motor vehicle is taken through force or threat of force.

Sex Offenses, Forcible

Any sexual act directed against another person, forcibly or against that person's will, or both; or not forcibly or against the person's will where the victim is incapable of giving consent.

(a) *Forcible Rape* (Except “Statutory Rape”). The carnal knowledge of a person, forcibly or against that person's will, or both; or not forcibly or against the person's will where the victim is incapable of giving consent because of his or her temporary or permanent mental or physical incapacity (or because of his or her youth).

(b) *Forcible Sodomy*. Oral or anal sexual intercourse with another person, forcibly or against that person's will, or both; or not forcibly or against the person's will where the victim is incapable of giving consent because of his or her youth or because of his or her temporary or permanent mental or physical incapacity.

(c) *Sexual Assault With An Object*. To use an object or instrument to unlawfully penetrate, however slightly, the genital or anal opening of the body of another person, forcibly or against that person's will, or both; or not forcibly or against the person's will where the victim is incapable of giving consent because of his or her youth or because of his or her temporary or permanent mental or physical incapacity.

Note: An “object” or “instrument” is anything used by the offender other than the offender's genitalia. Examples are a finger, bottle, handgun, stick, etc.

(d) *Forcible Fondling*. The touching of the private body parts of another person for the purpose of sexual gratification, forcibly or against that person's will, or both; or not forcibly or against the person's will where the victim is incapable of giving consent because of his or her youth or because of his or her temporary or permanent mental or physical incapacity.

Note: Forcible Fondling includes “Indecent Liberties” and “Child Molesting.”

Nonforcible Sex Offenses (Except “Prostitution Offenses”)

Unlawful, nonforcible sexual intercourse.

(a) *Incest*. Nonforcible sexual intercourse between persons who are related to each other within the degrees wherein marriage is prohibited by law.

(b) *Statutory Rape*. Nonforcible sexual intercourse with a person who is under the statutory age of consent.

(Authority: 20 U.S.C. 1232g(b)(6) and 18 U.S.C. 16)

[65 FR 41854, July 6, 2000]

[Back to Top](#)

FEATURED RESOURCES

[A Parent Guide to the Family Educational Rights and Privacy Act \(FERPA\) \(/resources/parent-guide-family-educational-rights-and-privacy-act-ferpa\)](#)

The Family Educational Rights and Privacy Act or FERPA provides certain rights for parents regarding their children’s education records. This guide provides general information on a parent’s rights under FERPA.

[An Eligible Student Guide to the Family Educational Rights and Privacy Act \(FERPA\) \(/resources/eligible-student-guide-family-educational-rights-and-privacy-act-ferpa\)](#)

The Family Educational Rights and Privacy Act or FERPA provides certain rights for parents regarding their children’s education records. When a student reaches 18 years of age or attends an institution of postsecondary education at any age, the student becomes an “eligible student,” and all rights under FERPA transfer from the parent to the student. This guide provides general information on an eligible student’s rights under FERPA.

Protection of Pupil Rights Amendment (PPRA) **General Guidance (/resources/protection-pupil-rights-amendment-ppra-general-guidance)**

This guidance document reviews parents' rights under the PPRA and education officials' obligations in implementing the PPRA. The PPRA applies to the programs and activities of a State educational agency (SEA), local educational agency (LEA), or other recipient of funds under any program funded by the U.S. Department of Education. (20 U.S.C. § 1232h, 34 CFR Part 98)

RESOURCES

Family Educational Rights and Privacy Act (FERPA) (/ferpa)

Legal Basics (/legal-basics)

Security Best Practices (/topic/security-best-practices)

Glossary (/glossary)

Letters of Importance (/topic/letters-importance)

Historic Findings Letters (/historical-archive-issued-letters)

BROWSE BY AUDIENCE

School Officials K-12 (/audience/school-officials-k-12)

Parents & Students (/audience/parents-and-students)

Postsecondary School Officials (/audience/school-officials-post-secondary)

Early Childhood Educators (/audience/early-childhood-educators)

Vendors (/audience/education-technology-vendors)

Researchers (/audience/researchers)

TRAINING

Online Training Modules (/content/online-training-modules)

Guidance Videos (/content/videos)

Recorded Webinars (/content/recorded-webinars)

OTHER

FAQs (/frequently-asked-questions)

Legal Basics (/legal-basics)

Contact (/contact)

Subscribe to the Student Privacy Newsletter (/subscribe-student-privacy-newsletter)

Request PTAC Training or Technical Assistance (/request-ptac-training-or-technical-assistance)

Privacy Policy (https://www2.ed.gov/notices/privacy/index.html?src=ft)

Washington State Preservation and Destruction of Public Records, [RCW 40.14](#)

Chapter 40.14 RCW
PRESERVATION AND DESTRUCTION OF PUBLIC RECORDS

Sections

- 40.14.010 Definition and classification of public records.
- 40.14.020 Division of archives and records management—State archivist—Powers and duties—Duties of public officials.
- 40.14.022 Division of archives and records management—Imaging account.
- 40.14.024 Division of archives and records management—Local government archives account.
- 40.14.025 Division of archives and records management—Allocation of costs of services—Public records efficiency, preservation, and access account.
- 40.14.026 Division of archives and records management—Competitive grant program to improve technology information systems for public records and related training—Review of program and training services—Public records request log—Agency reporting requirements—Duties of the joint legislative audit and review committee.
- 40.14.027 Local government archives and records management services—Judgment debtor surcharge.
- 40.14.030 Transfer to state archives—Certified copies, cost—Public disclosure.
- 40.14.040 Records officers—Designation—Powers and duties.
- 40.14.050 Records committee—Composition, travel expenses, meetings, powers and duties—Retention schedules.
- 40.14.060 Destruction, disposition of official public records or office files and memoranda—Record retention schedules.
- 40.14.070 Destruction, disposition, donation of local government records—Preservation for historical interest—Local records committee, duties—Record retention schedules—Sealed records—Peace and corrections officer personnel records.
- 40.14.080 Chapter not to affect other laws.
- 40.14.100 Legislative records—Defined.
- 40.14.110 Legislative records—Contribution of papers by legislators and employees.
- 40.14.120 Legislative records—"Clerk," "secretary" defined.
- 40.14.130 Legislative records—Duties of legislative officials, employees and state archivist—Delivery of records—Custody—Availability.
- 40.14.140 Legislative records—Party caucuses to be advised—Information and instructions.
- 40.14.150 Legislative records—Use for research.
- 40.14.160 Legislative records—Rules for access to records.
- 40.14.170 Legislative records—Sound recordings.
- 40.14.180 Legislative records—Construction—Confidentiality of bill drafting records.

Materials specifically authorized to be printed and distributed by secretary of state: RCW 43.07.140.

RCW 40.14.010 Definition and classification of public records.

As used in this chapter, the term "public records" shall include any paper, correspondence, completed form, bound record book, photograph, film, sound recording, map drawing, machine-readable material, compact disc meeting current industry ISO specifications, or other document, regardless of physical form or characteristics, and including such copies thereof, that have been made by or received by any agency of the state of Washington in connection with the transaction of public business, and legislative records as described in RCW 40.14.100.

For the purposes of this chapter, public records shall be classified as follows:

(1) Official public records shall include all original vouchers, receipts, and other documents necessary to isolate and prove the validity of every transaction relating to the receipt, use, and disposition of all public property and public income from all sources whatsoever; all agreements and contracts to which the state of Washington or any agency thereof may be a party; all fidelity, surety, and performance bonds; all claims filed against the state of Washington or any agency thereof; all records or documents required by law to be filed with or kept by any agency of the state of Washington; all legislative records as defined in RCW 40.14.100; and all other documents or records determined by the records committee, created in RCW 40.14.050, to be official public records.

(2) Office files and memoranda include such records as correspondence, exhibits, drawings, maps, completed forms, or documents not above defined and classified as official public records; duplicate copies of official public records filed with any agency of the state of Washington; documents and reports made for the internal administration of the office to which they pertain but not required by law to be filed or kept with such agency; and other documents or records as determined by the records committee to be office files and memoranda. [1996 c 71 s 1; 1982 c 36 s 3; 1981 c 32 s 4; 1971 ex.s. c 102 s 1; 1957 c 246 s 1.]

RCW 40.14.020 Division of archives and records management—State archivist—Powers and duties—Duties of public officials. All public records shall be and remain the property of the state of Washington. They shall be delivered by outgoing officials and employees to their successors and shall be preserved, stored, transferred, destroyed or disposed of, and otherwise managed, only in accordance with the provisions of this chapter. In order to insure the proper management and safeguarding of public records, the division of archives and records management is established in the office of the secretary of state. The state archivist, who shall administer the division and have reasonable access to all public records, wherever kept, for purposes of information, surveying, or cataloguing, shall undertake the following functions, duties, and responsibilities:

(1) To manage the archives of the state of Washington;

(2) To centralize the archives of the state of Washington, to make them available for reference and scholarship, and to insure their proper preservation;

(3) To inspect, inventory, catalog, and arrange retention and transfer schedules on all record files of all state departments and other agencies of state government;

(4) To insure the maintenance and security of all state public records and to establish safeguards against unauthorized removal or destruction;

(5) To establish and operate such state record centers as may from time to time be authorized by appropriation, for the purpose of preserving, servicing, screening and protecting all state public records which must be preserved temporarily or permanently, but which need not be retained in office space and equipment;

(6) To adopt rules under chapter 34.05 RCW:

(a) Setting standards for the durability and permanence of public records maintained by state and local agencies;

(b) Governing procedures for the creation, maintenance, transmission, cataloging, indexing, storage, or reproduction of photographic, optical, electronic, or other images of public documents or records in a manner consistent with current standards, policies, and procedures of Washington technology solutions for the acquisition of information technology;

(c) Governing the accuracy and durability of, and facilitating access to, photographic, optical, electronic, or other images used as public records; or

(d) To carry out any other provision of this chapter;

(7) To gather and disseminate to interested agencies information on all phases of records management and current practices, methods, procedures, techniques, and devices for efficient and economical management and preservation of records;

(8) To operate a central microfilming bureau which will microfilm, at cost, records approved for filming by the head of the office of origin and the archivist; to approve microfilming projects undertaken by state departments and all other agencies of state government; and to maintain proper standards for this work;

(9) To maintain necessary facilities for the review of records approved for destruction and for their economical disposition by sale or burning; directly to supervise such destruction of public records as shall be authorized by the terms of this chapter;

(10) To assist and train state and local agencies in the proper methods of creating, maintaining, cataloging, indexing, transmitting, storing, and reproducing photographic, optical, electronic, or other images used as public records;

(11) To solicit, accept, and expend donations as provided in RCW 43.07.037 for the purpose of the archive program. These purposes include, but are not limited to, acquisition, accession, interpretation, and display of archival materials. Donations that do not meet the criteria of the archive program may not be accepted.

[2024 c 54 s 32; 2011 1st sp.s. c 43 s 727; 2002 c 358 s 4; 1995 c 326 s 1. Prior: 1991 c 237 s 4; 1991 c 184 s 1; 1986 c 275 s 1; 1983 c 84 s 1; 1981 c 115 s 1; 1957 c 246 s 2.]

Effective date—Purpose—2011 1st sp.s. c 43: See notes following RCW 43.19.003.

Effective date—1991 c 237: See note following RCW 44.04.320.

Effective date—1981 c 115: "This act is necessary for the immediate preservation of the public peace, health, and safety, the support of the state government and its existing public institutions, and shall take effect July 1, 1981." [1981 c 115 s 10.]

RCW 40.14.022 Division of archives and records management—Imaging account. The imaging account is created in the custody of the state treasurer. All receipts collected under RCW 40.14.020(8) for contract imaging, micrographics, reproduction, and duplication services provided by the division of archives and records management must be deposited into the account, and expenditures from the account may be used only for these purposes. Only the secretary of state or the secretary's designee may authorize expenditures from the account. The account is subject to allotment procedures under chapter 43.88 RCW, but an appropriation is not required for expenditures. [2003 c 163 s 2.]

RCW 40.14.024 Division of archives and records management—Local government archives account. The local government archives account is created in the state treasury. All receipts collected by the county auditors under RCW 40.14.027 and 36.22.175 for local government services, such as providing records schedule compliance, security microfilm inspection and storage, archival preservation, cataloging, and indexing for local government records and digital data and access to those records and data through the regional branch archives of the division of archives and records management, must be deposited into the account, and expenditures from the account may be used only for these purposes. Any amounts deposited in the account in accordance with RCW 36.22.175(4) may only be expended for the purposes authorized under that provision as follows: No more than fifty percent of funding may be used for the attorney general's consultation program and the state archivist's training services, and the remainder is to be used for the competitive grant program, except that during the 2025-2027 fiscal biennium the competitive grant program may be suspended or reduced and the remainder used for administrative costs of the state archives. [2025 c 424 s 934; 2017 c 303 s 5; 2008 c 328 s 6005; 2003 c 163 s 3.]

Effective date—2025 c 424: See note following RCW 9.46.100.

Part headings not law—Severability—Effective date—2008 c 328: See notes following RCW 43.155.050.

RCW 40.14.025 Division of archives and records management—Allocation of costs of services—Public records efficiency, preservation, and access account. (1) The secretary of state and the director of financial management shall jointly establish a procedure and formula for allocating the costs of services provided by the division of archives and records management to state agencies. The total amount allotted for services to state agencies shall not exceed the appropriation to the *archives and records management account during any allotment period.

(2) There is created the public records efficiency, preservation, and access account in the state treasury which shall consist of all fees and charges collected under this section. The account shall be appropriated exclusively for the payment of costs and expenses incurred in the operation of the division of archives and records management as specified by law.

(3) During the 2025-2027 fiscal biennium, moneys in the account may also be transferred into the Washington state library operations fund. [2025 c 424 s 935; 2011 1st sp.s. c 50 s 932; 2003 c 163 s 1; 1996 c 245 s 3; 1991 sp.s. c 13 s 5; 1985 c 57 s 22; 1981 c 115 s 4.]

***Reviser's note:** The "archives and records management account" was changed to the "public records efficiency, preservation, and access account" by 2011 1st sp.s. c 50 s 932.

Effective date—2025 c 424: See note following RCW 9.46.100.

Effective dates—2011 1st sp.s. c 50: See note following RCW 15.76.115.

Effective date—1996 c 245: "This act takes effect on July 1, 1996." [1996 c 245 s 5.]

Effective dates—Severability—1991 sp.s. c 13: See notes following RCW 18.08.240.

Effective date—1985 c 57: See note following RCW 18.04.105.

Effective date—1981 c 115: See note following RCW 40.14.020.

RCW 40.14.026 Division of archives and records management—Competitive grant program to improve technology information systems for public records and related training—Review of program and training services—Public records request log—Agency reporting requirements—Duties of the joint legislative audit and review committee. (1) The division of archives and records management in the office of the secretary of state must establish and administer a competitive grant program for local agencies to improve technology information systems for public record retention, management, and disclosure, and any related training, except that during the 2025-2027 fiscal biennium the competitive grant program may be suspended or reduced. The division of archives and records management may use up to six percent of amounts appropriated for the program for administration of the grant program.

(2) Any local agency may apply to the grant program. The division of archives and records management in the office of the secretary of state must award grants annually. The division of archives and records management must consult with the chief information officer to develop the criteria for grant recipient selection with a preference given to small local governmental agencies based on the applicant agency's need and ability to improve its information technology systems for public record retention, management, and disclosure. The division of archives and records management may award grants for specific hardware, software, equipment, technology services management and training needs, indexing for local records and digital data, and other resources for improving information technology systems. To the extent possible, information technology systems, processes, training, and other resources for improving information technology systems for records retention and distribution may be replicated and shared with other governmental entities. Grants are provided for one-time investments and are not an ongoing source of revenue for operation or

management costs. A grantee may not supplant local funding with grant funding provided by the office of the secretary of state.

(3) The joint legislative audit and review committee must conduct a review of the attorney general's consultation program and the state archivist's training services created under section 4, chapter 303, Laws of 2017, and the local government competitive grant program created under this section. The review must include:

(a) (i) Information on the number of local governments served, the types of consultation and training provided, and the implementation of any practices adopted from the attorney general's consultation program and the state archivist's training services; and

(ii) The effectiveness of the consultation program and the training services in providing assistance for local governments; and

(b) (i) Information on the number of local governments that applied for and participated in the competitive grant program under this section, the amount of funding awarded through the grant program, and how such funding was used; and

(ii) The effectiveness of the grant program in improving local government technology information systems for public records retention, management, disclosure, and training.

(4) Each agency shall maintain a log of public records requests submitted to and processed by the agency, which shall include but not be limited to the following information for each request: The identity of the requestor if provided by the requestor, the date the request was received, the text of the original request, a description of the records produced in response to the request, a description of the records redacted or withheld and the reasons therefor, and the date of the final disposition of the request. The log must be retained by the agency in accordance with the relevant record retention schedule established under this chapter, and shall be a public record subject to disclosure under chapter 42.56 RCW.

(5) To improve best practices for dissemination of public records, each agency with actual staff and legal costs associated with fulfilling public records requests of at least one hundred thousand dollars during the prior fiscal year must, and each agency with such estimated costs of less than one hundred thousand dollars during the prior fiscal year may, report to the joint legislative audit and review committee by July 1st of each subsequent year the following metrics, measured over the preceding year:

(a) The number of requests where the agency provided the requested records within five days of receiving the request.

(b) The number of requests where the agency provided a time estimate for providing responsive records beyond five days after receiving the request.

(c) The average and median number of days from receipt of request to the date the request is closed.

(d) The number of requests where the agency formally sought additional clarification from the requestor;

(e) The number of requests denied in full or in part and the most common reasons for denying requests;

(f) The number of requests abandoned by requestors;

(g) To the extent the information is known by the agency, requests by type of requestor, including individuals, law firms, organizations, insurers, governments, incarcerated persons, the media, anonymous requestors, current or former employees, and others;

(h) Which portion of requests were fulfilled electronically compared to requests fulfilled by physical records;

(i) The number of requests where the agency scanned physical records electronically to fulfill disclosure;

(j) The total estimated agency staff time spent on each individual request;

(k) The estimated costs incurred by the agency in fulfilling records requests, including costs for staff compensation and legal review, and a measure of the average cost per request;

(l) The number of claims filed alleging a violation of chapter 42.56 RCW or other public records statutes in the past year involving the agency, categorized by type and exemption at issue, if applicable;

(m) The costs incurred by the agency litigating claims alleging a violation of chapter 42.56 RCW or other public records statutes in the past year, including any penalties imposed on the agency;

(n) The costs incurred by the agency with managing and retaining records, including staff compensation and purchases of equipment, hardware, software, and services to manage and retain public records; and

(o) Expenses recovered by the agency from requestors for fulfilling public records requests, including any customized service charges.

(6) The joint legislative audit and review committee must consult with state and local agencies to develop a reporting method and clearly define standardized metrics in accordance with this section.

(7) By December 1, 2019, the joint legislative audit and review committee must report to the legislature on its findings from the review, including recommendations on whether the competitive grant program, the attorney general's consultation program, and the state archivist's training services should continue or be allowed to expire. [2025 c 424 s 936; 2019 c 372 s 1; 2017 c 303 s 6.]

Effective date—2025 c 424: See note following RCW 9.46.100.

RCW 40.14.027 Local government archives and records management services—Judgment debtor surcharge. State agencies shall collect a surcharge of twenty dollars from the judgment debtor upon the satisfaction of a warrant filed in superior court for unpaid taxes or liabilities. The surcharge is imposed on the judgment debtor in the form of a penalty in addition to the filing fee provided in RCW 36.18.012(10). The surcharge revenue shall be transmitted to the state treasurer for deposit in the public records efficiency, preservation, and access account.

Surcharge revenue deposited in the local government archives account under RCW 40.14.024 shall be expended by the secretary of state exclusively for disaster recovery, essential records protection services, and records management training for local government agencies by the division of archives and records management. The secretary of state shall, with local government representatives, establish a committee to advise the state archivist on the local government archives and records management program. [2011 1st sp.s. c 50 s 933; 2003 c 163 s 4; 2001 c 146 s 4; 1996 c 245 s 4; 1995 c 292 s 17; 1994 c 193 s 2.]

Effective dates—2011 1st sp.s. c 50: See note following RCW 15.76.115.

Effective date—1996 c 245: See note following RCW 40.14.025.

Findings—1994 c 193: "The legislature finds that: (1) Accountability for and the efficient management of local government records are in the public interest and that compliance with public records management requirements significantly affects the cost of local government administration; (2) the secretary of state is responsible for insuring the preservation of local government archives and may assist local government compliance with public records statutes; (3) as provided in RCW 40.14.025, all archives and records management services provided by the secretary of state are funded exclusively by a schedule of fees and charges established jointly by the secretary of state and the director of financial management; (4) the secretary of state's costs for preserving and providing public access to local government archives and providing records management assistance to local government agencies have been funded by fees paid by state government agencies; (5) local government agencies are responsible for costs associated with managing, protecting, and providing public access to the records in their custody; (6) local government should help fund the secretary of state's local government archives and records management services; (7) the five dollar fee collected by county clerks for processing warrants for unpaid taxes or liabilities filed by the state of Washington is not sufficient to cover processing costs and is far below filing fees commonly charged for similar types of minor civil actions; (8) a surcharge of twenty dollars would bring the filing fee for warrants for the collection of unpaid taxes and liabilities up to a level comparable to other minor civil filings and should be applied to the support of the secretary of state's local government archives and records services without placing an undue burden on local government; and (9) the process of collecting and transmitting surcharge revenue should not have an undue impact on the operations of the state agencies that file warrants for the collection of unpaid taxes and liabilities or the clerks of superior court who process them." [1994 c 193 s 1.]

Effective date—1994 c 193: "This act shall take effect July 1, 1994." [1994 c 193 s 3.]

RCW 40.14.030 Transfer to state archives—Certified copies, cost—Public disclosure. (1) All public records, not required in the current operation of the office where they are made or kept, and all records of every agency, commission, committee, or any other activity of state government which may be abolished or discontinued, shall be transferred to the state archives so that the valuable historical records of the state may be centralized, made more widely available, and insured permanent preservation: PROVIDED, That this section shall have no application to public records approved for destruction under the subsequent provisions of this chapter.

When so transferred, copies of the public records concerned shall be made and certified by the archivist, which certification shall have the same force and effect as though made by the officer originally in charge of them. Fees may be charged to cover the cost of reproduction. In turning over the archives of his or her office, the officer in charge thereof, or his or her successor, thereby loses none of his or her rights of access to them, without charge, whenever necessary.

(2) Records that are confidential, privileged, or exempt from public disclosure under state or federal law while in the possession of the originating agency, commission, board, committee, or other entity of state or local government retain their confidential, privileged, or exempt status after transfer to the state archives unless the archivist, with the concurrence of the originating jurisdiction, determines that the records must be made accessible to the public according to proper and reasonable rules adopted by the secretary of state, in which case the records may be open to inspection and available for copying after the expiration of seventy-five years from creation of the record. If the originating jurisdiction is no longer in existence, the archivist shall make the determination of availability according to such rules. If, while in the possession of the originating agency, commission, board, committee, or other entity, any record is determined to be confidential, privileged, or exempt from public disclosure under state or federal law for a period of less than seventy-five years, then the record, with the concurrence of the originating jurisdiction, must be made accessible to the public upon the expiration of the shorter period of time according to proper and reasonable rules adopted by the secretary of state. [2011 c 336 s 817; 2003 c 305 s 1; 1957 c 246 s 3.]

Columbia River boundary compact, transfer of records to division of archives: RCW 43.58.070.

RCW 40.14.040 Records officers—Designation—Powers and duties.

Each department or other agency of the state government shall designate a records officer to supervise its records program and to represent the office in all contacts with the records committee, hereinafter created, and the division of archives and records management. The records officer shall:

(1) Coordinate all aspects of the records management program.

(2) Inventory, or manage the inventory, of all public records at least once during a biennium for disposition scheduling and transfer action, in accordance with procedures prescribed by the state archivist and state records committee: PROVIDED, That essential records shall be inventoried and processed in accordance with chapter 40.10 RCW at least annually.

(3) Consult with any other personnel responsible for maintenance of specific records within his or her state organization regarding records retention and transfer recommendations.

(4) Analyze records inventory data, examine and compare divisional or unit inventories for duplication of records, and recommend to the state archivist and state records committee minimal retentions for all copies commensurate with legal, financial, and administrative needs.

(5) Approve all records inventory and destruction requests which are submitted to the state records committee.

(6) Review established records retention schedules at least annually to insure that they are complete and current.

(7) Exercise internal control over the acquisition of filming and file equipment.

If a particular agency or department does not wish to transfer records at a time previously scheduled therefor, the records officer

shall, within thirty days, notify the archivist and request a change in such previously set schedule, including his or her reasons therefor. [2011 c 336 s 818; 1982 c 36 s 4; 1979 c 151 s 51; 1973 c 54 s 3; 1957 c 246 s 4.]

RCW 40.14.050 Records committee—Composition, travel expenses, meetings, powers and duties—Retention schedules. There is created a committee, to be known as the records committee, composed of the archivist, an appointee of the state auditor, an appointee of the attorney general, and an appointee of the director of financial management. Committee members shall serve without additional salary, but shall be entitled to travel expenses incurred in accordance with RCW 43.03.050 and 43.03.060 as now existing or hereafter amended. Such expenses shall be paid from the appropriations made for operation of their respective departments or offices.

The records committee shall meet at least once every quarter or oftener as business dictates. Action by the committee shall be by majority vote and records shall be kept of all committee business.

It shall be the duty of the records committee to approve, modify or disapprove the recommendations on retention schedules of all files of public records and to act upon requests to destroy any public records: PROVIDED, That any modification of a request or recommendation must be approved by the head of the agency originating the request or recommendation.

The division of archives and records management shall provide forms, approved by the records committee, upon which it shall prepare recommendations to the committee in cooperation with the records officer of the department or other agency whose records are involved. [1985 c 192 s 1; 1975-'76 2nd ex.s. c 34 s 83; 1957 c 246 s 5.]

Effective date—Severability—1975-'76 2nd ex.s. c 34: See notes following RCW 2.08.115.

RCW 40.14.060 Destruction, disposition of official public records or office files and memoranda—Record retention schedules.

(1) Any destruction of official public records shall be pursuant to a schedule approved under RCW 40.14.050. Official public records shall not be destroyed unless:

(a) Except as provided under RCW 40.14.070(2)(b), the records are six or more years old;

(b) The department of origin of the records has made a satisfactory showing to the state records committee that the retention of the records for a minimum of six years is both unnecessary and uneconomical, particularly if lesser federal retention periods for records generated by the state under federal programs have been established; or

(c) The originals of official public records less than six years old have been copied or reproduced by any photographic or other process approved by the state archivist which accurately reproduces or forms a durable medium for so reproducing the original.

(2) Any lesser term of retention than six years must have the additional approval of the director of financial management, the state auditor and the attorney general, except when records have federal retention guidelines the state records committee may adjust the

retention period accordingly. An automatic reduction of retention periods from seven to six years for official public records on record retention schedules existing on June 10, 1982, shall not be made, but the same shall be reviewed individually by the state records committee for approval or disapproval of the change to a retention period of six years.

Recommendations for the destruction or disposition of office files and memoranda shall be submitted to the records committee upon approved forms prepared by the records officer of the agency concerned and the archivist. The committee shall determine the period of time that any office file or memorandum shall be preserved and may authorize the division of archives and records management to arrange for its destruction or disposition. [1999 c 326 s 1; 1982 c 36 s 5; 1979 c 151 s 52; 1973 c 54 s 4; 1957 c 246 s 6.]

RCW 40.14.070 Destruction, disposition, donation of local government records—Preservation for historical interest—Local records committee, duties—Record retention schedules—Sealed records—Peace and corrections officer personnel records. (1)(a) Other than those records detailed in subsection (4) of this section, county, municipal, and other local government agencies may request authority to destroy noncurrent public records having no further administrative or legal value by submitting to the division of archives and records management lists of such records on forms prepared by the division. The archivist, a representative appointed by the state auditor, and a representative appointed by the attorney general shall constitute a committee, known as the local records committee, which shall review such lists and which may veto the destruction of any or all items contained therein.

(b) A local government agency, as an alternative to submitting lists, may elect to establish a records control program based on recurring disposition schedules recommended by the agency to the local records committee. The schedules are to be submitted on forms provided by the division of archives and records management to the local records committee, which may either veto, approve, or amend the schedule. Approval of such schedule or amended schedule shall be by unanimous vote of the local records committee. Upon such approval, the schedule shall constitute authority for the local government agency to destroy the records listed thereon, after the required retention period, on a recurring basis until the schedule is either amended or revised by the committee.

(2)(a) Except as otherwise provided by law, and other than the law enforcement records detailed in subsection (4) of this section, no public records shall be destroyed until approved for destruction by the local records committee. Official public records shall not be destroyed unless:

(i) The records are six or more years old;

(ii) The department of origin of the records has made a satisfactory showing to the state records committee that the retention of the records for a minimum of six years is both unnecessary and uneconomical, particularly where lesser federal retention periods for records generated by the state under federal programs have been established; or

(iii) The originals of official public records less than six years old have been copied or reproduced by any photographic,

photostatic, microfilm, miniature photographic, or other process approved by the state archivist which accurately reproduces or forms a durable medium for so reproducing the original.

An automatic reduction of retention periods from seven to six years for official public records on record retention schedules existing on June 10, 1982, shall not be made, but the same shall be reviewed individually by the local records committee for approval or disapproval of the change to a retention period of six years.

The state archivist may furnish appropriate information, suggestions, and guidelines to local government agencies for their assistance in the preparation of lists and schedules or any other matter relating to the retention, preservation, or destruction of records under this chapter. The local records committee may adopt appropriate regulations establishing procedures to be followed in such matters.

Records of county, municipal, or other local government agencies, designated by the archivist as of primarily historical interest, may be transferred to a recognized depository agency.

(b) (i) Records of investigative reports prepared by any state, county, municipal, or other law enforcement agency pertaining to sex offenders contained in chapter 9A.44 RCW or sexually violent offenses as defined in RCW 71.09.020 that are not required in the current operation of the law enforcement agency or for pending judicial proceedings shall, following the expiration of the applicable schedule of the law enforcement agency's retention of the records, be transferred to the Washington association of sheriffs and police chiefs for permanent electronic retention and retrieval. Upon electronic retention of any document, the association shall be permitted to destroy the paper copy of the document.

(ii) Any sealed record transferred to the Washington association of sheriffs and police chiefs for permanent electronic retention and retrieval, including records sealed after transfer, shall be electronically retained in such a way that the record is clearly marked as sealed.

(iii) The Washington association of sheriffs and police chiefs shall be permitted to destroy both the paper copy and electronic record of any offender verified as deceased.

(c) Any record transferred to the Washington association of sheriffs and police chiefs pursuant to (b) of this subsection shall be deemed to no longer constitute a public record pursuant to RCW 42.56.010 and shall be exempt from public disclosure. Such records shall be disseminated only to criminal justice agencies as defined in RCW 10.97.030 for the purpose of determining if a sex offender met the criteria of a sexually violent predator as defined in chapter 71.09 RCW and the end-of-sentence review committee as defined by RCW 72.09.345 for the purpose of fulfilling its duties under RCW 71.09.025 and 9.95.420.

Electronic records marked as sealed shall only be accessible by criminal justice agencies as defined in RCW 10.97.030 who would otherwise have access to a sealed paper copy of the document, the end-of-sentence review committee as defined by RCW 72.09.345 for the purpose of fulfilling its duties under RCW 71.09.025 and 9.95.420, and the system administrator for the purposes of system administration and maintenance.

(3) Except as otherwise provided by law, county, municipal, and other local government agencies may, as an alternative to destroying noncurrent public records having no further administrative or legal

value, donate the public records to the state library, local library, historical society, genealogical society, or similar society or organization.

Public records may not be donated under this subsection unless:

(a) The records are seventy years old or more;

(b) The local records committee has approved the destruction of the public records; and

(c) The state archivist has determined that the public records have no historic interest.

(4) Personnel records for any peace officer or corrections officer must be retained for the duration of the officer's employment and a minimum of 10 years thereafter. Such records include all misconduct and equal employment opportunity complaints, progressive discipline imposed including written reprimands, supervisor coaching, suspensions, involuntary transfers, other disciplinary appeals and litigation records, and any other records needed to comply with the requirements set forth in RCW 43.101.095 and 43.101.135. [2021 c 323 s 19; 2011 c 60 s 18; 2005 c 227 s 1; 2003 c 240 s 1; 1999 c 326 s 2; 1995 c 301 s 71; 1982 c 36 s 6; 1973 c 54 s 5; 1971 ex.s. c 10 s 1; 1957 c 246 s 7.]

Effective date—2011 c 60: See RCW 42.17A.919.

Copying, preserving, and indexing of documents recorded by county auditor: RCW 36.22.160 through 36.22.190.

Destruction and reproduction of court records: RCW 36.23.065 through 36.23.070.

RCW 40.14.080 Chapter not to affect other laws. The provisions of this chapter shall not be construed as repealing or modifying any other acts or parts of acts authorizing the destruction of public records save for those specifically named in *section 9 of this act; nor shall this chapter affect the provisions of chapter 40.07 RCW requiring the deposit of all state publications in the state library. [1983 c 3 s 84; 1957 c 246 s 8.]

***Reviser's note:** "section 9 of this act" refers to 1957 c 246 s 9, which repealed RCW 40.08.010 through 40.08.050 and 40.12.010 through 40.12.110.

RCW 40.14.100 Legislative records—Defined. As used in RCW 40.14.010 and 40.14.100 through 40.14.180, unless the context requires otherwise, "legislative records" shall be defined as correspondence, amendments, reports, and minutes of meetings made by or submitted to legislative committees or subcommittees and transcripts or other records of hearings or supplementary written testimony or data thereof filed with committees or subcommittees in connection with the exercise of legislative or investigatory functions, but does not include the records of an official act of the legislature kept by the secretary of state, bills and their copies, published materials, digests, or multi-copied matter which are routinely retained and otherwise available at the state library or in a public repository, or reports or correspondence made or received by or in any way under the personal

control of the individual members of the legislature. [1971 ex.s. c 102 s 2.]

RCW 40.14.110 Legislative records—Contribution of papers by legislators and employees. Nothing in RCW 40.14.010 and 40.14.100 through 40.14.180 shall prohibit a legislator or legislative employee from contributing his or her personal papers to any private library, public library, or the state archives. The state archivist is authorized to receive papers of legislators and legislative employees and is directed to encourage the donation of such personal records to the state. The state archivist is authorized to establish such guidelines and procedures for the collection of personal papers and correspondence relating to the legislature as he or she sees fit. Legislators and legislative employees are encouraged to contribute their personal papers to the state for preservation. [2011 c 336 s 819; 1971 ex.s. c 102 s 3.]

RCW 40.14.120 Legislative records—"Clerk," "secretary" defined. As used in RCW 40.14.010 and 40.14.100 through 40.14.180 "clerk" means clerk of the Washington state house of representatives and "secretary" means the secretary of the Washington state senate. [1971 ex.s. c 102 s 4.]

RCW 40.14.130 Legislative records—Duties of legislative officials, employees and state archivist—Delivery of records—Custody—Availability. The legislative committee chair, subcommittee chair, committee member, or employed personnel of the state legislature having possession of legislative records that are not required for the regular performance of official duties shall, within ten days after the adjournment sine die of a regular or special session, deliver all such legislative records to the clerk of the house or the secretary of the senate.

The clerk of the house and the secretary of the senate are charged to include requirements and responsibilities for keeping committee minutes and records as part of their instructions to committee chairs and employees.

The clerk or the secretary, with the assistance of the state archivist, shall classify and arrange the legislative records delivered to the clerk or secretary in a manner that he or she considers best suited to carry out the efficient and economical utilization, maintenance, preservation, and disposition of the records. The clerk or the secretary may deliver to the state archivist all legislative records in his or her possession when such records have been classified and arranged and are no longer needed by either house. The state archivist shall thereafter be custodian of the records so delivered, but shall deliver such records back to either the clerk or secretary upon his or her request.

The chair, member, or employee of a legislative interim committee responsible for maintaining the legislative records of that committee shall, on a scheduled basis agreed upon by the chair, member, or employee of the legislative interim committee, deliver to the clerk or secretary all legislative records in his or her possession, as long as such records are not required for the regular performance of official

duties. He or she shall also deliver to the clerk or secretary all records of an interim committee within ten days after the committee ceases to function. [2011 c 336 s 820; 1971 ex.s. c 102 s 5.]

RCW 40.14.140 Legislative records—Party caucuses to be advised—Information and instructions. It shall be the duty of the clerk and the secretary to advise the party caucuses in each house concerning the necessity to keep public records. The state archivist or his or her representative shall work with the clerk and secretary to provide information and instructions on the best method for keeping legislative records. [2011 c 336 s 821; 1971 ex.s. c 102 s 6.]

RCW 40.14.150 Legislative records—Use for research. Committee records may be used by legislative employees for research at the discretion of the clerk or the secretary. [1971 ex.s. c 102 s 7.]

RCW 40.14.160 Legislative records—Rules for access to records. The clerk or the secretary shall, with advice of the state archivist, prescribe rules for access to records more than three years old when such records have been delivered to the state archives for preservation and maintenance. [1971 ex.s. c 102 s 8.]

RCW 40.14.170 Legislative records—Sound recordings. Any sound recording of debate in the house or senate made by legislative employees shall be preserved by the chief clerk of the house and by the secretary of the senate, respectively, for two years from the end of the session at which made, and thereafter shall be transmitted to the state archivist. The chief clerk and the secretary shall catalogue or index the recordings in their custody according to a uniform system, in order to allow easy access to the debate on specific questions before either house, and shall make available to any court of record, at the cost of reproduction, such portions of the recordings as the court may request. [1971 ex.s. c 102 s 9.]

RCW 40.14.180 Legislative records—Construction—Confidentiality of bill drafting records. The provisions of RCW 40.14.010 and 40.14.100 through 40.14.180 shall not be construed as repealing or modifying any other acts or parts of acts authorizing the retention or destruction of public records nor shall RCW 40.14.010 and 40.14.100 through 40.14.180 affect the provisions of chapter 40.07 RCW requiring the deposit of all state publications in the state library nor shall it affect the confidentiality of the bill drafting records of the code reviser's office. [1983 c 3 s 85; 1971 ex.s. c 102 s 10.]

Washington State Public Records Act, RCW 42.56

The following pages show only section titles of this evidence. To view the full file, please refer to the hyperlink

**Chapter 42.56 RCW
PUBLIC RECORDS ACT**

Sections

- 42.56.001 Finding, purpose.
- 42.56.010 Definitions.
- 42.56.020 Short title.
- 42.56.030 Construction.
- 42.56.040 Duty to publish procedures.
- 42.56.050 Invasion of privacy, when.
- 42.56.060 Disclaimer of public liability.
- 42.56.070 Documents and indexes to be made public—Statement of costs.
- 42.56.080 Identifiable records—Facilities for copying—Availability of public records.
- 42.56.090 Times for inspection and copying—Posting on website.
- 42.56.100 Protection of public records—Public access.
- 42.56.110 Destruction of information relating to employee misconduct.
- 42.56.120 Charges for copying.
- 42.56.130 Other provisions not superseded.
- 42.56.140 Public records exemptions accountability committee.
- 42.56.141 Public records exemptions accountability committee—Wolf depredation information exemption.
- 42.56.150 Training—Local elected and statewide elected officials.
- 42.56.152 Training—Public records officers.
- 42.56.155 Assistance by attorney general.
- 42.56.210 Certain personal and other records exempt.
- 42.56.230 Personal information.
- 42.56.235 Religious affiliation exemption.
- 42.56.240 Investigative, law enforcement, and crime victims.
- 42.56.250 Employment and licensing.
- 42.56.260 Real estate transactions.
- 42.56.270 Financial, commercial, and proprietary information.
- 42.56.280 Preliminary drafts, notes, recommendations, intra-agency memorandums.
- 42.56.290 Agency party to controversy.
- 42.56.300 Archaeological sites.
- 42.56.310 Library records.
- 42.56.315 Certain student information.
- 42.56.320 Educational information.
- 42.56.325 Statewide electronic repository for school meals.
- 42.56.330 Public utilities and transportation.
- 42.56.335 Public utility districts and municipally owned electrical utilities—Restrictions on access by law enforcement authorities.
- 42.56.350 Health professionals.
- 42.56.355 Interstate medical licensure compact.
- 42.56.357 Interstate physician assistant licensure compact.
- 42.56.360 Health care.
- 42.56.365 Vital records.
- 42.56.370 Client records of domestic violence programs, or community sexual assault programs or services for underserved populations.

- 42.56.375 Sexual misconduct—Postsecondary educational institutions
—Personal information of witnesses and victims.
- 42.56.380 Agriculture and livestock.
- 42.56.390 Emergency or transitional housing.
- 42.56.395 Affordable housing occupants and tenants.
- 42.56.400 Insurance and financial institutions.
- 42.56.403 Property and casualty insurance statements of actuarial
opinion.
- 42.56.410 Employment security department records, certain purposes.
- 42.56.420 Security.
- 42.56.422 Office of cybersecurity—Reports and information.
- 42.56.423 Cybersecurity advisory committee and technology services
board security subcommittee.
- 42.56.425 Election security.
- 42.56.430 Fish and wildlife.
- 42.56.440 Veterans' discharge papers—Exceptions.
- 42.56.450 Check cashers and sellers licensing applications.
- 42.56.460 Fireworks and explosives.
- 42.56.470 Correctional industries workers.
- 42.56.475 Department of corrections and private detention
facilities.
- 42.56.510 Duty to disclose or withhold information—Otherwise
provided.
- 42.56.520 Prompt responses required.
- 42.56.530 Review of agency denial.
- 42.56.540 Court protection of public records.
- 42.56.550 Judicial review of agency actions.
- 42.56.556 Failure to provide recording of school district board of
directors meeting.
- 42.56.560 Application of RCW 42.56.550.
- 42.56.565 Inspection or copying by persons serving criminal
sentences—Injunction.
- 42.56.570 Explanatory pamphlet—Advisory model rules—Consultation
and training services.
- 42.56.580 Public records officers.
- 42.56.590 Personal information—Notice of security breaches.
- 42.56.592 Personal information—Covered entities.
- 42.56.594 Personal information—Consumer protection.
- 42.56.600 Mediation communications.
- 42.56.610 Certain information from dairies and feedlots limited—
Rules.
- 42.56.615 Enumeration data used by the office of financial
management for population estimates.
- 42.56.620 Cannabis research licensee reports.
- 42.56.625 Medical cannabis authorization database.
- 42.56.630 Registration information of members of cooperatives to
produce and process medical cannabis.
- 42.56.640 Vulnerable individuals, in-home caregivers for vulnerable
populations.
- 42.56.645 Release of public information—2017 c 4 (Initiative
Measure No. 1501).
- 42.56.650 Health carrier data.
- 42.56.655 Explosives exemption report.
- 42.56.660 Agency employee records.
- 42.56.665 Agency employee records—Civil liability.

- 42.56.670 Agency employee records—Model policies.
- 42.56.675 Agency employee records—Lists of names.
- 42.56.680 Residential real property information and borrower personal information.
- 42.56.690 Victim and witness notification program.
- 42.56.692 Victim and witness notification program—Notification enrollment.
- 42.56.695 Intelligent speed assistance devices.
- 42.56.700 Driver training education course voucher program.
- 42.56.900 Purpose—2005 c 274 ss 402-429.
- 42.56.904 Intent—2007 c 391.

Criminal records privacy: Chapter 10.97 RCW.

Restrictions on dissemination of child forensic interview recordings: RCW 26.44.187 and 26.44.188.

RCW 42.56.001 Finding, purpose. The legislature finds that *chapter 42.17 RCW contains laws relating to several discrete subjects. Therefore, the purpose of chapter 274, Laws of 2005 is to recodify some of those laws and create a new chapter in the Revised Code of Washington that contains laws pertaining to public records. [2005 c 274 s 1.]

***Reviser's note:** Provisions in chapter 42.17 RCW relating to public records were recodified in chapter 42.56 RCW by 2005 c 274, effective July 1, 2006. Provisions in chapter 42.17 RCW relating to campaign disclosure and contribution were recodified in chapter 42.17A RCW by 2010 c 204, effective January 1, 2012. Chapter 42.17A RCW was recodified into Title 29B RCW by 2024 c 164, effective January 1, 2026.

RCW 42.56.010 Definitions. The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Agency" includes all state agencies and all local agencies. "State agency" includes every state office, department, division, bureau, board, commission, or other state agency. "Local agency" includes every county, city, town, municipal corporation, quasi-municipal corporation, or special purpose district, or any office, department, division, bureau, board, commission, or agency thereof, or other local public agency. "Agency" does not include a comprehensive cancer center participating in a collaborative arrangement as defined in RCW 28B.10.930 that is operated in conformance with RCW 28B.10.930.

(2) "Person in interest" means the person who is the subject of a record or any representative designated by that person, except that if that person is under a legal disability, "person in interest" means and includes the parent or duly appointed legal representative.

(3) "Public record" includes any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics. For the office of the secretary of the senate and the office of the chief clerk of the house of representatives, public records means legislative records as defined in RCW 40.14.100 and also

Washington State Records and Retrieval Act, WAC
434-610 – 434-690

**Title 434 WAC
SECRETARY OF STATE**

Last Update: 4/23/25

Chapters

434-04	Use of the state seal.
434-12	Trademarks.
434-12A	Public records and rules of procedure.
434-112	Corporations and charities division program services, procedures and fees.
434-120	Charitable solicitation organizations and charitable trusts.
434-166	International student exchange agency registration.
434-208	Elections.
434-209	Citizen's commission on salaries for elected officials.
434-215	Declarations of candidacy and filing procedures.
434-219	Presidential primary.
434-230	Ballots.
434-232	Seventeen year olds participating in the primary—Future voters.
434-235	Service and overseas voters.
434-250	Elections by mail.
434-260	Election review process and certification of election administrators.
434-261	Counting center procedures.
434-262	Canvassing and certification.
434-263	Administrative complaint procedure.
434-264	Recounts.
434-291	Special elections for major public energy project bond measures.
434-324	Statewide voter registration database.
434-335	Voting systems.
434-369	Maps and census correspondence listings.
434-379	Initiatives and referenda.
434-381	State voters' pamphlet.
434-600	Promulgation.
434-610	Definitions.
434-615	Custody of public records.
434-620	Powers and duties of the state archivist.
434-624	Powers and duties of the state records committee.
434-630	Powers and duties of the local records committee.
434-635	Local records disposition authorization.
434-640	Methods of records disposal.
434-660	Standards for the accuracy, durability and permanence of public records.
434-661	Real property electronic recording.
434-662	Preservation of electronic public records.
434-663	Imaging systems, standards for accuracy and durability.
434-670	The Washington state archives local records grant program.
434-677	Security microfilm.
434-690	Archives—Access to public records.
434-750	Combined fund drive.
434-840	Address confidentiality program.

DISPOSITION OF CHAPTERS FORMERLY CODIFIED IN THIS TITLE

**Chapter 434-08
ELECTIONS**

Reviser's note: Later promulgation, see chapter 434-208 WAC.

434-08-010	Advisory election upon contemplation of classification advancement. [Regulation 1, filed 3/24/60.] Decodified by WSR 98-08-010, filed 3/18/98, effective 3/18/98.
434-08-020	Remedial steps—Third class city under mayor-council government. [Regulation 2, filed 3/24/60.] Decodified by WSR 98-08-010, filed 3/18/98, effective 3/18/98.
434-08-030	Determination of original terms of councilmen—Second, third, or fourth class city or town. [Regulation 3, filed 3/24/60.] Decodified by WSR 98-08-010, filed 3/18/98, effective 3/18/98.
434-08-040	Appointment of clerks. [Regulation 4, filed 3/24/60.] Decodified by WSR 98-08-010, filed 3/18/98, effective 3/18/98.
434-08-050	Restrictions on write-in or sticker votes. [Regulation 5, filed 3/24/60.] Decodified by WSR 98-08-010, filed 3/18/98, effective 3/18/98.

NIST Cybersecurity Framework

The following pages show only cover and table of content of this evidence. To view the full file, please refer to the hyperlink



The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology

This publication is available free of charge from: <https://doi.org/10.6028/NIST.CSWP.29>

February 26, 2024



NIST CSWP 29
February 26, 2024

Abstract

The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts. The CSF does not prescribe how outcomes should be achieved. Rather, it links to online resources that provide additional guidance on practices and controls that could be used to achieve those outcomes. This document describes CSF 2.0, its components, and some of the many ways that it can be used.

Keywords

cybersecurity; Cybersecurity Framework (CSF); cybersecurity risk governance; cybersecurity risk management; enterprise risk management; Profiles; Tiers.

Audience

Individuals responsible for developing and leading cybersecurity programs are the primary audience for the CSF. The CSF can also be used by others involved in managing risk — including executives, boards of directors, acquisition professionals, technology professionals, risk managers, lawyers, human resources specialists, and cybersecurity and risk management auditors — to guide their cybersecurity-related decisions. Additionally, the CSF can be useful to those making and influencing policy (e.g., associations, professional organizations, regulators) who set and communicate priorities for cybersecurity risk management.

Supplemental Content

NIST will continue to build and host additional resources to help organizations implement the CSF, including Quick Start Guides and Community Profiles. All resources are made publicly available on the [NIST CSF website](#). Suggestions for additional resources to reference on the NIST CSF website can always be shared with NIST at cyberframework@nist.gov.

Note to Readers

Unless otherwise noted, documents cited, referenced, or excerpted in this publication are not wholly incorporated into this publication.

Before version 2.0, the Cybersecurity Framework was called the “Framework for Improving Critical Infrastructure Cybersecurity.” This title is not used for CSF 2.0.

Acknowledgments

The CSF is the result of a multi-year collaborative effort across industry, academia, and government in the United States and around the world. NIST acknowledges and thanks all of those who have contributed to this revised CSF. Information on the CSF development process can be found on the [NIST CSF website](#). Lessons learned about the use of the CSF can always be shared with NIST at cyberframework@nist.gov.

Table of Contents

1. Cybersecurity Framework (CSF) Overview	1
2. Introduction to the CSF Core.....	3
3. Introduction to CSF Profiles and Tiers	6
3.1. CSF Profiles.....	6
3.2. CSF Tiers	7
4. Introduction to Online Resources That Supplement the CSF	9
5. Improving Cybersecurity Risk Communication and Integration	10
5.1. Improving Risk Management Communication	10
5.2. Improving Integration with Other Risk Management Programs	11
Appendix A. CSF Core.....	15
Appendix B. CSF Tiers.....	24
Appendix C. Glossary	26

List of Figures

Fig. 1. CSF Core structure.....	3
Fig. 2. CSF Functions.....	5
Fig. 3. Steps for creating and using a CSF Organizational Profile.....	6
Fig. 4. CSF Tiers for cybersecurity risk governance and management	8
Fig. 5. Using the CSF to improve risk management communication.....	10
Fig. 6. Cybersecurity and privacy risk relationship	13

Gramm-Leach-Bliley Act

This content is from the eCFR and is authoritative but unofficial.

Title 16 – Commercial Practices

Chapter I – Federal Trade Commission

Subchapter C – Regulations Under Specific Acts of Congress

Part 314 Standards for Safeguarding Customer Information

§ 314.1 Purpose and scope.

§ 314.2 Definitions.

§ 314.3 Standards for safeguarding customer information.

§ 314.4 Elements.

§ 314.5 Effective date.

§ 314.6 Exceptions.

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Authority: 15 U.S.C. 6801(b), 6805(b)(2).

Source: 67 FR 36493, May 23, 2002, unless otherwise noted.

§ 314.1 Purpose and scope.

- (a) **Purpose.** This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.
- (b) **Scope.** This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission (“FTC” or “Commission”) has jurisdiction. Namely, this part applies to those “financial institutions” over which the Commission has rulemaking authority pursuant to section 501(b) of the Gramm-Leach-Bliley Act. An entity is a “financial institution” if its business is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k), which incorporates activities enumerated by the Federal Reserve Board in 12 CFR 225.28 and 225.86. The “financial institutions” subject to the Commission’s enforcement authority are those that are not otherwise subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act, 15 U.S.C. 6805. More specifically, those entities include, but are not limited to, mortgage lenders, “pay day” lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors that are not required to register with the Securities and Exchange Commission, and entities acting as finders. They are

referred to in this part as "You." This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

[67 FR 36493, May 23, 2002, as amended at 86 FR 70304, Dec. 9, 2021]

§ 314.2 Definitions.

- (a) **Authorized user** means any employee, contractor, agent, customer, or other person that is authorized to access any of your information systems or data.
- (b)
 - (1) **Consumer** means an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.
 - (2) For example:
 - (i) An individual who applies to you for credit for personal, family, or household purposes is a consumer of a financial service, regardless of whether the credit is extended.
 - (ii) An individual who provides nonpublic personal information to you in order to obtain a determination about whether he or she may qualify for a loan to be used primarily for personal, family, or household purposes is a consumer of a financial service, regardless of whether the loan is extended.
 - (iii) An individual who provides nonpublic personal information to you in connection with obtaining or seeking to obtain financial, investment, or economic advisory services is a consumer, regardless of whether you establish a continuing advisory relationship.
 - (iv) If you hold ownership or servicing rights to an individual's loan that is used primarily for personal, family, or household purposes, the individual is your consumer, even if you hold those rights in conjunction with one or more other institutions. (The individual is also a consumer with respect to the other financial institutions involved.) An individual who has a loan in which you have ownership or servicing rights is your consumer, even if you, or another institution with those rights, hire an agent to collect on the loan.
 - (v) An individual who is a consumer of another financial institution is not your consumer solely because you act as agent for, or provide processing or other services to, that financial institution.
 - (vi) An individual is not your consumer solely because he or she has designated you as trustee for a trust.
 - (vii) An individual is not your consumer solely because he or she is a beneficiary of a trust for which you are a trustee.
 - (viii) An individual is not your consumer solely because he or she is a participant or a beneficiary of an employee benefit plan that you sponsor or for which you act as a trustee or fiduciary.
- (c) **Customer** means a consumer who has a customer relationship with you.

(d) **Customer information** means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

(e)

(1) **Customer relationship** means a continuing relationship between a consumer and you under which you provide one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.

(2) For example:

(i) **Continuing relationship.** A consumer has a continuing relationship with you if the consumer:

- (A) Has a credit or investment account with you;
- (B) Obtains a loan from you;
- (C) Purchases an insurance product from you;
- (D) Holds an investment product through you, such as when you act as a custodian for securities or for assets in an Individual Retirement Arrangement;
- (E) Enters into an agreement or understanding with you whereby you undertake to arrange or broker a home mortgage loan, or credit to purchase a vehicle, for the consumer;
- (F) Enters into a lease of personal property on a non-operating basis with you;
- (G) Obtains financial, investment, or economic advisory services from you for a fee;
- (H) Becomes your client for the purpose of obtaining tax preparation or credit counseling services from you;
- (I) Obtains career counseling while seeking employment with a financial institution or the finance, accounting, or audit department of any company (or while employed by such a financial institution or department of any company);
- (J) Is obligated on an account that you purchase from another financial institution, regardless of whether the account is in default when purchased, unless you do not locate the consumer or attempt to collect any amount from the consumer on the account;
- (K) Obtains real estate settlement services from you; or
- (L) Has a loan for which you own the servicing rights.

(ii) **No continuing relationship.** A consumer does not, however, have a continuing relationship with you if:

- (A) The consumer obtains a financial product or service from you only in isolated transactions, such as using your ATM to withdraw cash from an account at another financial institution; purchasing a money order from you; cashing a check with you; or making a wire transfer through you;
- (B) You sell the consumer's loan and do not retain the rights to service that loan;
- (C) You sell the consumer airline tickets, travel insurance, or traveler's checks in isolated transactions;

(D) The consumer obtains one-time personal or real property appraisal services from you; or

(E) The consumer purchases checks for a personal checking account from you.

(f) **Encryption** means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.

(g)

(1) **Financial product or service** means any product or service that a financial holding company could offer by engaging in a financial activity under section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) **Financial service** includes your evaluation or brokerage of information that you collect in connection with a request or an application from a consumer for a financial product or service.

(h)

(1) **Financial institution** means any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C. 1843(k). An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution.

(2) Examples of financial institutions are as follows:

(i) A retailer that extends credit by issuing its own credit card directly to consumers is a financial institution because extending credit is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)(4)(F)), and issuing that extension of credit through a proprietary credit card demonstrates that a retailer is significantly engaged in extending credit.

(ii) An automobile dealership that, as a usual part of its business, leases automobiles on a nonoperating basis for longer than 90 days is a financial institution with respect to its leasing business because leasing personal property on a nonoperating basis where the initial term of the lease is at least 90 days is a financial activity listed in 12 CFR 225.28(b)(3) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(iii) A personal property or real estate appraiser is a financial institution because real and personal property appraisal is a financial activity listed in 12 CFR 225.28(b)(2)(i) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(iv) A career counselor that specializes in providing career counseling services to individuals currently employed by or recently displaced from a financial organization, individuals who are seeking employment with a financial organization, or individuals who are currently employed by or seeking placement with the finance, accounting or audit departments of any company is a financial institution because such career counseling activities are financial activities listed in 12 CFR 225.28(b)(9)(iii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

- (v) A business that prints and sells checks for consumers, either as its sole business or as one of its product lines, is a financial institution because printing and selling checks is a financial activity that is listed in 12 CFR 225.28(b)(10)(ii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).
 - (vi) A business that regularly wires money to and from consumers is a financial institution because transferring money is a financial activity referenced in section 4(k)(4)(A) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(A), and regularly providing that service demonstrates that the business is significantly engaged in that activity.
 - (vii) A check cashing business is a financial institution because cashing a check is exchanging money, which is a financial activity listed in section 4(k)(4)(A) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(A).
 - (viii) An accountant or other tax preparation service that is in the business of completing income tax returns is a financial institution because tax preparation services is a financial activity listed in 12 CFR 225.28(b)(6)(vi) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(G).
 - (ix) A business that operates a travel agency in connection with financial services is a financial institution because operating a travel agency in connection with financial services is a financial activity listed in 12 CFR 225.86(b)(2) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(G).
 - (x) An entity that provides real estate settlement services is a financial institution because providing real estate settlement services is a financial activity listed in 12 CFR 225.28(b)(2)(viii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).
 - (xi) A mortgage broker is a financial institution because brokering loans is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).
 - (xii) An investment advisory company and a credit counseling service are each financial institutions because providing financial and investment advisory services are financial activities referenced in section 4(k)(4)(C) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(C).
 - (xiii) A company acting as a finder in bringing together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate is a financial institution because acting as a finder is an activity that is financial in nature or incidental to a financial activity listed in 12 CFR 225.86(d)(1).
- (3) **Financial institution** does not include:
- (i) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 et seq.);
 - (ii) The Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.);

- (iii) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as such institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party other than as permitted by §§ 313.14 and 313.15; or
- (iv) Entities that engage in financial activities but that are not significantly engaged in those financial activities, and entities that engage in activities incidental to financial activities but that are not significantly engaged in activities incidental to financial activities.

(4) Examples of entities that are not significantly engaged in financial activities are as follows:

- (i) A retailer is not a financial institution if its only means of extending credit are occasional “lay away” and deferred payment plans or accepting payment by means of credit cards issued by others.
- (ii) A retailer is not a financial institution merely because it accepts payment in the form of cash, checks, or credit cards that it did not issue.
- (iii) A merchant is not a financial institution merely because it allows an individual to “run a tab.”
- (iv) A grocery store is not a financial institution merely because it allows individuals to whom it sells groceries to cash a check, or write a check for a higher amount than the grocery purchase and obtain cash in return.

(i) **Information security program** means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(j) **Information system** means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing customer information or connected to a system containing customer information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains customer information or that is connected to a system that contains customer information.

(k) **Multi-factor authentication** means authentication through verification of at least two of the following types of authentication factors:

- (1) Knowledge factors, such as a password;
- (2) Possession factors, such as a token; or
- (3) Inherence factors, such as biometric characteristics.

(l)

(1) **Nonpublic personal information** means:

- (i) Personally identifiable financial information; and
- (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

(2) **Nonpublic personal information** does not include:

- (i) Publicly available information, except as included on a list described in paragraph (l)(1)(ii) of this section; or
- (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.

(3) For example:

- (i) Nonpublic personal information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information (that is not publicly available), such as account numbers.
- (ii) Nonpublic personal information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived, in whole or in part, using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

(m) **Notification event** means acquisition of unencrypted customer information without the authorization of the individual to which the information pertains. Customer information is considered unencrypted for this purpose if the encryption key was accessed by an unauthorized person. Unauthorized acquisition will be presumed to include unauthorized access to unencrypted customer information unless you have reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.

(n) **Penetration testing** means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems.

(o)

(1) **Personally identifiable financial information** means any information:

- (i) A consumer provides to you to obtain a financial product or service from you;
- (ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or
- (iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

(2) For example:

- (i) **Information included.** Personally identifiable financial information includes:
 - (A) Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;
 - (B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;
 - (C) The fact that an individual is or has been one of your customers or has obtained a financial product or service from you;

- (D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;
- (E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;
- (F) Any information you collect through an internet "cookie" (an information collecting device from a web server); and
- (G) Information from a consumer report.

(ii) **Information not included.** Personally identifiable financial information does not include:

- (A) A list of names and addresses of customers of an entity that is not a financial institution; and
- (B) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.

(p)

(1) **Publicly available information** means any information that you have a reasonable basis to believe is lawfully made available to the general public from:

- (i) Federal, State, or local government records;
- (ii) Widely distributed media; or
- (iii) Disclosures to the general public that are required to be made by Federal, State, or local law.

(2) You have a reasonable basis to believe that information is lawfully made available to the general public if you have taken steps to determine:

- (i) That the information is of the type that is available to the general public; and
- (ii) Whether an individual can direct that the information not be made available to the general public and, if so, that your consumer has not done so.

(3) For example:

- (i) **Government records.** Publicly available information in government records includes information in government real estate records and security interest filings.
- (ii) **Widely distributed media.** Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper, or a website that is available to the general public on an unrestricted basis. A website is not restricted merely because an internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(iii) **Reasonable basis.**

- (A) You have a reasonable basis to believe that mortgage information is lawfully made available to the general public if you have determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(B) You have a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if you have located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

- (q) **Security event** means an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form.
- (r) **Service provider** means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.
- (s) **You** includes each "financial institution" (but excludes any "other person") over which the Commission has enforcement jurisdiction pursuant to section 505(a)(7) of the Gramm-Leach-Bliley Act.

[86 FR 70304, Dec. 9, 2021, as amended at 88 FR 77508, Nov. 13, 2023]

§ 314.3 Standards for safeguarding customer information.

- (a) **Information security program.** You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. The information security program shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.
- (b) **Objectives.** The objectives of section 501(b) of the Act, and of this part, are to:
 - (1) Insure the security and confidentiality of customer information;
 - (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
 - (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

[67 FR 36493, May 23, 2002, as amended at 86 FR 70307, Dec. 9, 2021]

§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

- (a) Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, "Qualified Individual"). The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent the requirement in this paragraph (a) is met using a service provider or an affiliate, you shall:
 - (1) Retain responsibility for compliance with this part;
 - (2) Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and

- (3) Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.
- (b) Base your information security program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks.
 - (1) The risk assessment shall be written and shall include:
 - (i) Criteria for the evaluation and categorization of identified security risks or threats you face;
 - (ii) Criteria for the assessment of the confidentiality, integrity, and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face; and
 - (iii) Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.
 - (2) You shall periodically perform additional risk assessments that reexamine the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and reassess the sufficiency of any safeguards in place to control these risks.
- (c) Design and implement safeguards to control the risks you identify through risk assessment, including by:
 - (1) Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to:
 - (i) Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and
 - (ii) Limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information;
 - (2) Identify and manage the data, personnel, devices, systems, and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy;
 - (3) Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual;
 - (4) Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing, or storing customer information and procedures for evaluating, assessing, or testing the security of externally developed applications you utilize to transmit, access, or store customer information;
 - (5) Implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls;

(6)

(i) Develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and

(ii) Periodically review your data retention policy to minimize the unnecessary retention of data;

(7) Adopt procedures for change management; and

(8) Implement policies, procedures, and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.

(d)

(1) Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems.

(2) For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct:

(i) Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and

(ii) Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment, at least every six months; and whenever there are material changes to your operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your information security program.

(e) Implement policies and procedures to ensure that personnel are able to enact your information security program by:

(1) Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

(2) Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program;

(3) Providing information security personnel with security updates and training sufficient to address relevant security risks; and

(4) Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

(f) Oversee service providers, by:

- (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;
 - (2) Requiring your service providers by contract to implement and maintain such safeguards; and
 - (3) Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.
- (g) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.
- (h) Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control. Such incident response plan shall address the following areas:
- (1) The goals of the incident response plan;
 - (2) The internal processes for responding to a security event;
 - (3) The definition of clear roles, responsibilities, and levels of decision-making authority;
 - (4) External and internal communications and information sharing;
 - (5) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;
 - (6) Documentation and reporting regarding security events and related incident response activities; and
 - (7) The evaluation and revision as necessary of the incident response plan following a security event.
- (i) Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for your information security program. The report shall include the following information:
- (1) The overall status of the information security program and your compliance with this part; and
 - (2) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's responses thereto, and recommendations for changes in the information security program.
- (j) Notify the Federal Trade Commission about notification events in accordance with paragraphs (j)(1) and (2) of this section.
- (1) **Notification requirement.** Upon discovery of a notification event as described in paragraph (j)(2) of this section, if the notification event involves the information of at least 500 consumers, you must notify the Federal Trade Commission as soon as possible, and no later than 30 days after discovery of the event. The notice shall be made electronically on a form to be located on the FTC's website, <https://www.ftc.gov>. The notice shall include the following:
- (i) The name and contact information of the reporting financial institution;

- (ii) A description of the types of information that were involved in the notification event;
 - (iii) If the information is possible to determine, the date or date range of the notification event;
 - (iv) The number of consumers affected or potentially affected by the notification event;
 - (v) A general description of the notification event; and
 - (vi) Whether any law enforcement official has provided you with a written determination that notifying the public of the breach would impede a criminal investigation or cause damage to national security, and a means for the Federal Trade Commission to contact the law enforcement official. A law enforcement official may request an initial delay of up to 30 days following the date when notice was provided to the Federal Trade Commission. The delay may be extended for an additional period of up to 60 days if the law enforcement official seeks such an extension in writing. Additional delay may be permitted only if the Commission staff determines that public disclosure of a security event continues to impede a criminal investigation or cause damage to national security.
- (2) **Notification event treated as discovered.** A notification event shall be treated as discovered as of the first day on which such event is known to you. You shall be deemed to have knowledge of a notification event if such event is known to any person, other than the person committing the breach, who is your employee, officer, or other agent.

[86 FR 70307, Dec. 9, 2021, as amended at 88 FR 77508, Nov. 13, 2023]

§ 314.5 Effective date.

Section 314.4(j) is effective as of May 13, 2024.

[88 FR 77509, Nov. 13, 2023]

§ 314.6 Exceptions.

Section 314.4(b)(1), (d)(2), (h), and (i) do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers.

[86 FR 70308, Dec. 9, 2021]

ctcLink Privacy Agreement



ctcLink Data Usage and Privacy

[Home](#) / [For College & SBCTC Staff](#) / [IT Support](#) / [ctcLink Support](#) / ctcLink Data Usage and Privacy

Data Usage Resources

- [Data Services](#)
- [Data Governance Committee](#)

The ctcLink system contains college information related to students, employees, and finances. Users with access to data are required to adhere to a data privacy and usage agreement.

Data Usage Overview

All individuals authorized¹ to access data stored within the ctcLink system and infrastructure² are required to sign the [ctcLink Employee Data Privacy and Usage Agreement](#)  agreeing:

- To comply with the policies, guidelines, and procedures set forth in the ctcLink Employee Data Privacy Memorandum of Understanding (MOU).
- That the [ctcLink Employee Data Privacy MOU](#)  was available for adequate review and consideration prior to accessing the ctcLink system.

Definitions

¹ **Individuals with authorized access** include employees, staff, faculty, contractors, subcontractors, and any other party to this agreement.

² **Infrastructure** includes production (live) and development (in progress) environments, as well as replicated ctcLink data stored in the dataLink databases and testing environments.

Policies

- [ctcLink Employee Data Privacy and Usage Agreement](#)  (revised 2022-07-15) – ctcLink users will attest to the policy in an electronic pop-up form at ctcLink log-in. The downloadable document is provided for review.
- [ctcLink Employee Data Privacy and Usage Employee Attestation Implementation](#) 
- [ctcLink Employee Data Privacy MOU](#) 
- [DataBrief - ctcLink Data Usage and Privacy](#) 
- [ctcLink Data Classifications](#) 
- [Protecting Employee Data in HCM](#) 

Contact

Questions? [Email DataServices@sbctc.edu](mailto:DataServices@sbctc.edu) or contact a [Data Services team member](#).

state-government-general-records-retention-
schedule-v.6.3-(october-2024).pdf

The following pages show only front page and table of contents of this evidence. To view the full file, please refer to the hyperlink



**State Government General Records Retention Schedule
Version 6.3 (October 2024)**

This schedule applies to: All State Government Agencies

Scope of records retention schedule

This records retention schedule authorizes the destruction/transfer of public records documenting common functions and activities of state government agencies, including Universities and Community and Technical Colleges. It is to be used in conjunction with the other approved schedules that relate to the unique functions of the agency.

Disposition of public records

Public records covered by records series within this records retention schedule (regardless of format) must be retained for the minimum retention period as specified in this schedule. Washington State Archives strongly recommends the disposition of public records at the end of their minimum retention period for the efficient and effective management of agency resources.

Public records designated as “Archival (Permanent Retention)” must not be destroyed. Records designated as “Archival (Appraisal Required)” must be appraised by the Washington State Archives before disposition. Public records must not be destroyed if they are subject to ongoing or reasonably anticipated litigation. Such public records must be managed in accordance with the agency’s policies and procedures for legal holds. Public records must not be destroyed if they are subject to an existing public records request in accordance with chapter 42.56 RCW. Such public records must be managed in accordance with the agency’s policies and procedures for public records requests.

Revocation of previously issued records retention schedules

All previous versions of the State Government General Records Retention Schedule are revoked. State Agencies must ensure the retention and disposition of public records is in accordance with current, approved records retention schedules.

Authority

This records retention schedule was approved by the State Records Committee in accordance with RCW 40.14.050 on October 2, 2024.

AP Rose

For the State Auditor:
Al Rose

Suzanne Becker

For the Attorney General:
Suzanne Becker

Marie Davis

For the Office of Financial Management:
Marie Davis

Heather Hirota

The State Archivist:
Heather Hirota



REVISION HISTORY

Version	Date of Approval	Extent of Revision
1.0	November 1991	General Update
2.0	July 1997	General Update
3.0	Summer 2001	General Update
3.5	April 2005	General Update
4.0	November 2005	General Update
5.0	October 6, 2010	Changes to format, glossary updated, indexes added, standardized Archival designations and proper citation of RCW's.
5.1	August 3, 2011	All records series reorganized into six functional areas: Agency Management, Asset Management, Financial Management, Human Resource Management, Records Management, and Records With Minimal Retention Value. Major revision to Information Management function. New activities added including Banking, Community Relations, Library Services, Public Disclosure, Publishing, Records Conversion, Risk Management, and Security.
6.0	June 29, 2016	Major revision of entire schedule.
6.1	August 5, 2020	Minor revision to the "Asset Management – Security" section.
6.2	August 4, 2021	Minor revision to the "Human Resource Management – Occupational Health and Safety" section.
6.3	October 2, 2024	Minor revisions throughout the schedule.

For assistance and advice in applying this records retention schedule,
please contact your agency's Records Officer
or Washington State Archives at:
recordsmanagement@sos.wa.gov

TABLE OF CONTENTS

1.	AGENCY ADMINISTRATION AND MANAGEMENT.....	5
1.1	ADVICE AND TECHNICAL ASSISTANCE	5
1.2	AUDITING.....	6
1.3	AUTHORIZATION/CERTIFICATION	14
1.4	CALENDARS	15
1.5	CIVIL RIGHTS COMPLIANCE	16
1.6	COMMUNITY AND EXTERNAL RELATIONS	18
1.7	LEGAL AFFAIRS.....	26
1.8	LEGISLATION AND RULE MAKING	30
1.9	MEETINGS AND BOARD/COMMITTEE SUPPORT	32
1.10	PLANNING, POLICIES, AND PROCEDURES	37
1.11	REPORTING AND STUDIES	44
1.12	RISK MANAGEMENT AND DISASTER PREPAREDNESS/RESPONSE	49
1.13	TRAINING OTHERS.....	52
2.	ASSET MANAGEMENT.....	55
2.1	ACQUISITION AND DISPOSAL	55
2.2	DESIGN AND CONSTRUCTION	57
2.3	INFORMATION SERVICES	61
2.4	INVENTORY.....	65
2.5	MAINTENANCE, INSPECTION, AND MONITORING	66
2.6	OPERATIONS AND USE	70
2.7	SAFETY AND SECURITY	72
3.	FINANCIAL MANAGEMENT.....	75
3.1	ACCOUNTING AND FISCAL	75
3.2	AUTHORIZATION/DELEGATION	81
3.3	BUDGETING	82
3.4	CONTRACTS AND PURCHASING.....	83
3.5	GRANTS MANAGEMENT	87
3.6	TRAVEL	90



**State Government General Records Retention Schedule
Version 6.3 (October 2024)**

4. HR AND PAYROLL MANAGEMENT 91

4.1 ATTENDANCE AND LEAVE 91

4.2 AUTHORIZATION/CERTIFICATION 92

4.3 BENEFITS 93

4.4 LABOR RELATIONS 96

4.5 MISCONDUCT/DISCIPLINE/GRIEVANCES 97

4.6 OCCUPATIONAL HEALTH AND SAFETY 99

4.7 PAYROLL 105

4.8 PERFORMANCE MANAGEMENT 108

4.9 PERSONNEL HISTORY 109

4.10 POSITION DEVELOPMENT AND STAFF STRUCTURE 113

4.11 RECRUITMENT/HIRING 114

4.12 SEPARATION 116

4.13 STAFF DEVELOPMENT 117

5. INFORMATION MANAGEMENT 118

5.1 FORMS MANAGEMENT 118

5.2 LIBRARY SERVICES 119

5.3 MAIL SERVICES 121

5.4 PUBLIC DISCLOSURE/RECORDS REQUESTS 122

5.5 PUBLISHING 124

5.6 RECORDS MANAGEMENT 126

6. RECORDS WITH MINIMAL RETENTION VALUE (TRANSITORY RECORDS) 133

GLOSSARY 143

INDEXES 145

Data Security Training, Vector Solutions



Vector Solutions offers a comprehensive catalog of online courses for higher education faculty and staff.

[Download catalog](#) →

🏠 > [Course Search](#) > [Faculty and Staff Courses](#) > [Security and Risk Mitigation Training](#)

Online Faculty and Staff Security and Risk Mitigation Courses

Vector Solutions' Security and Risk library is designed to help mitigate human error and address the personal and physical security aspects of institutional safety. Increase security awareness, encourage better decision-making, and reduce risk.

[Request a demo](#)



The average cost of a single data breach to an organization is \$3.92 million, equaling losses of over \$8 billion. Approximately 15 million people have their identities stolen every year, equaling losses of over \$50 billion.

[Learn More](#) →



[Learn More](#) →



[Learn More](#) →



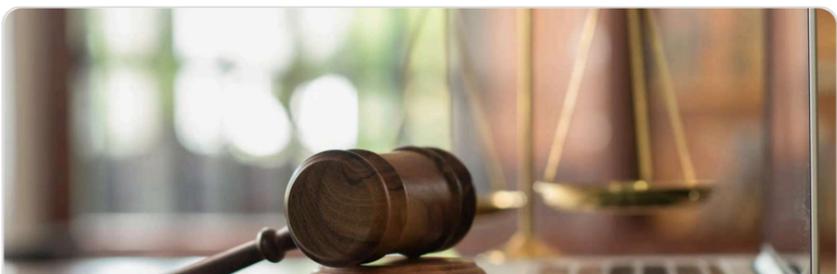
[Learn More](#) →



[Learn More →](#)



[Learn More →](#)



[Learn More →](#)



[Learn More →](#)



[Learn More →](#)



[Learn More →](#)





[Learn More](#) →

[Learn More](#) →



According to a study commissioned by the Citizens Crime Commission of New York City:

437 people were shot in 190 college campus shooting incidents

[Learn More](#) →

[Learn More](#) →



[Learn More](#) →

[Learn More](#) →



[Learn More](#) →

[Learn More](#) →



[Learn More](#) →



[Learn More](#) →



[Learn More](#) →



[Learn More](#) →



[Learn More](#) →



[Learn More](#) →





[Learn More →](#)

[Learn More →](#)



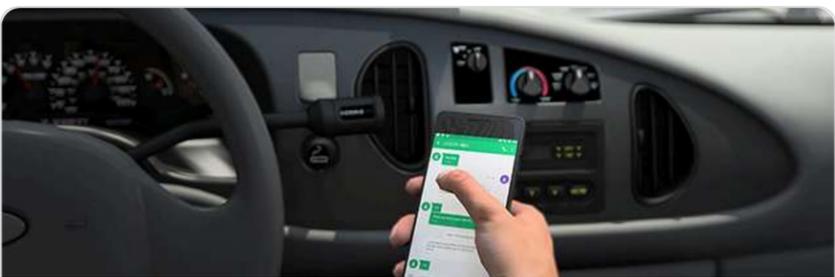
[Learn More →](#)

[Learn More →](#)



[Learn More →](#)

[Learn More →](#)



[Learn More →](#)

[Learn More →](#)



[Learn More](#) →

Full Library Course List

Campus Prevention Network

- [Data Security & Privacy](#)
- [Payment Card Industry Data Security Standard \(PCI DSS\)](#)
- [Social Media & Your Job](#)
- [Social Media for Managers](#)

Human Resources

- [FACTA: Identity Theft and Consumer Protection](#)

Transportation

- [15-Passenger Van Safety](#)
- [Dangers of Distracted Driving](#)
- [Defensive Driving](#)
- [Winter Driving](#)

Cybersecurity

- [Cybersecurity Awareness for Educational Leaders: Creating a Cybersecurity Culture](#)
- [Cybersecurity Awareness for Educational Leaders: Incident Preparedness and Management Planning](#)
- [Cybersecurity Awareness for Educational Leaders: Laws and Global Compliance Standards](#)
- [Cybersecurity Awareness for Educational Leaders: Safeguarding Against Social Engineering Attacks](#)
- [Cybersecurity Awareness for Employees at Educational Institutions: Security Awareness Essentials](#)
- [Cybersecurity Awareness for Employees of Educational Institutions: Classifying and Safeguarding Data for institutional and Personal Use](#)
- [Cybersecurity Awareness for Employees of Educational Institutions: End-User Best Practices](#)
- [Cybersecurity Awareness for Employees of Educational Institutions: Social Engineering](#)

Information Technology

- [Browser Security Basics](#)
- [Copyright Infringement](#)
- [Email and Messaging Safety](#)
- [Password Security Basics](#)
- [Payment Card Industry Data Security Standard \(PCI DSS\) Overview](#)
- [Protection Against Malware](#)

Emergency Management

- [Active Assailant Preparedness](#)
- [Active Shooter: Run, Hide, Fight](#)
- [Crime Prevention through Physical Security](#)
- [Emergency and Disaster Preparedness](#)
- [Terrorism: Awareness and Response](#)

Security

- [Arson Awareness and Prevention](#)
- [Campus Security Authorities: Roles and Responsibilities](#)
- [Copper Theft Awareness](#)
- [Safety Basics for Security Staff](#)
- [Visual Weapons Screening](#)

Connect with Us

Learn more about our online training for higher ed, get pricing, and see our platform.



John	Doe
123-456-7890	Director of Services
State - Please Select ▼	
Industry - Please Select ▼	
Company Name	

[Request a demo](#)



Connect with us



[Log In](#) →

[Contact](#) →

Industries

- [K-12](#)
- [Higher Education](#)
- [Manufacturing](#)
- [Fire Departments](#)
- [EMS](#)
- [Law Enforcement](#)
- [Architecture, Engineering & Construction](#)
- [Facilities Management](#)
- [Casino](#)
- [See all industries](#)

Courses

- [K-12 Courses](#)
- [Higher Education Courses](#)
- [Industrial Courses](#)
- [Firefighter Courses](#)
- [EMS Courses](#)
- [Law Enforcement Courses](#)
- [Architecture, Engineering & Construction Courses](#)
- [Facilities Management Courses](#)
- [Casino Courses](#)
- [See all courses](#)

Resources

- [Resource Center](#)
- [Course Catalogs](#)
- [Whitepapers](#)
- [Webinar](#)
- [Brochures](#)
- [Blog](#)
- [Press Releases](#)
- [In The News](#)

Company

- [About](#)
- [Partners](#)
- [Industry Honors](#)
- [Vector Cares](#)
- [Careers](#)
- [Executive Team](#)
- [Contact us](#)
- [Newsletter](#)

[Terms of Use](#)

[Privacy Policy](#)

[CCPA Privacy Policy](#)

Vector LMS, Higher Education Edition Training:
Login

LOG IN



Provided by
Green River College

The safety of our staff and students is of utmost importance. That's why we're pleased to offer the Vector LMS, Higher Education Edition to our employees. We're confident you'll find these courses to be informative and helpful towards maintaining a safe learning environment.

Username

Password

Log In →

[Forgot Login?](https://greenriver-wa.safecolleges.com/forgot_credentials) (https://greenriver-wa.safecolleges.com/forgot_credentials)

 Username Hint

Sign Up for Our Newsletter



Want to stay informed? Join the 5000+ customers who use Vector LMS, Higher Education Edition Training and sign up for our newsletter to receive monthly emails.

[Sign Up For Our Newsletter](http://www.safecolleges.com/newsletters/) (http://www.safecolleges.com/newsletters/)

What's New? Find out here.



We're always working hard to give you the best training experience. Read about the tools and features we're constantly adding, as well as what's coming soon!

[Read about Updates](https://support.vectortrainingeducation.com/s/topic/0TO4N000000NTMaWAO/product-updates) (https://support.vectortrainingeducation.com/s/topic/0TO4N000000NTMaWAO/product-updates)



<https://greenriver-wa.safecolleges.com/training/assignments>

[Terms of Use](https://greenriver-wa.safecolleges.com/terms) (<https://greenriver-wa.safecolleges.com/terms>) [Privacy Policy](https://greenriver-wa.safecolleges.com/privacy)  (<https://greenriver-wa.safecolleges.com/privacy>) [Contact](#)

© 2025 Vector Solutions



Green River Data Handling Guidelines

Green River Data Handling Guidelines

GRC classifies data (college information) per the SBCTC and WA State OCIO guidelines.

All GRC Data must be stored either physically on a GRC campus or digitally on GRC CTR (i.e., resources provided by GRC either directly or through agreements with contracted entities). GRC Data must not be stored off-campus (other than during approved and temporary travel), on personal equipment or in non-GRC provided or contracted solutions.

Category 2 and higher data requires specific care be taken when transmitting or storing and should not be stored on any non-GRC owned equipment without a signed confidentiality and data sharing agreement. Category 2 and higher data is discoverable.

Per the GRC IT Security Policy:

4.1. Data Classification

GRC classifies data into categories based on the sensitivity of the data. GRC data classifications must translate to or include the following classification categories:

1. Category 1 – Public Information

Public Information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure but does need integrity and availability protection controls.

Public Information data includes the mission/vision/values of an agency, information related to obtaining services, staff phone numbers, work e-mail addresses, budget information, and FERPA “directory information” designated at Green River College as FERPA information at level 1.

Electronic transfer of data in this classification is not restricted.

2. Category 2 – Sensitive Information

Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

Sensitive data should not be transferred outside the GRC network electronically unless on password protected media. You must be specifically authorized to transfer such data outside the agency. Transfer inside the GRC network is allowed.

Specific examples include, but are not limited to:

- Data Warehouse data unless that data falls under a Category 3 or 4 classification
- Student Directory Information as per FERPA regulations can be disclosed to outside organizations with the student's prior consent or released during a public records request of Data Warehouse data.
- Certain personnel records – e.g., misconduct records subject to public disclosure
- Public Employee Financial information, but not salaries as this is public information

- Directory Information includes:
 - Student name
 - Student birthplace and birthdate
 - Student address
 - Student telephone number
 - Student e-mail address
 - Major field of study (EPC) Dates of attendance (YRQ)
 - Degrees and awards received
 - Photograph
 - Participation in officially recognized activities or sports
 - Height and weight of athletes
 - Most recent educational agency or institution attended
 - Other similar information
- Directory information does NOT include:
 - Social security number
 - Student identification number
 - Race
 - Ethnicity
 - Nationality
 - Gender
 - Class schedule
 - Course and Program information not tied directly to a student, such as:
 - Department and Course Number
 - Course Title
 - Course Intent
 - Program Code (EPC)
 - Program Title

3. Category 3 – Confidential Information

Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to:

- Personal information about individuals, regardless of how that information is obtained such as home address, phone number, and personal e-mail address
- Information in employee personnel records including evaluations
- Information regarding IT infrastructure and security of computer and telecommunications systems
- All financial data not included in the Public Employee Financial Information data
- Personal network user information (e.g., usernames and passwords)
- Enrollment information protected under FERPA such as:
 - Student Information Numbers (SIDs)
 - Grades
 - Courses taken
 - Test scores

- Educational services received

This category of data can be transferred internally, with appropriate care – e.g., marked in e-mail as confidential or private, or via secure network folders where everyone with access is authorized to see the data. Confidential data may only be transferred outside the agency via encrypted or password protected media. You must be specifically authorized to transfer such data outside the agency and there must be a signed confidentiality agreement with that individual or company prior to sending the information.

SBCTC Definition of Category 3 Data:

Enrollment information protected under FERPA, personnel and financial data. Category 3 includes all data elements except those explicitly stated in categories 2 and 4. Category 3 data is not distributed unless governed by a contract or data sharing agreement. This information is protected due to:

- a) Sensitivity – Information which must be protected due to proprietary, ethical, contractual or privacy considerations.*
- b) Legal Obligations – Information for which disclosure to persons outside of the SBCTC may be governed by specific standards and controls designed to protect the information such as FERPA.*
- c) Moderate risk – Information which may not be specifically protected by statute, regulations, or other legal obligations or mandates but for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of could cause financial loss, damage to the SBCTC or college reputation, violate an individual's privacy rights, or make legal action necessary.*

This information includes but is not limited to:

- *Student Identification Numbers (SID)*
- *Grades*
- *Courses taken*
- *Test Scores*
- *Educational services received*
- *Bio-demographics (e.g., race, gender, family status, employment status)*
- *All personnel data including salaries*
- *All financial data*

Confidential Information data includes personal network user information, data related to IT security, employee and student personal information such as ID number, home address, phone number, personal email address, including information designated as Green River College FERPA levels 2 & 3.

This category of data can be transferred internally, with appropriate care – e.g., marked in email as confidential or private, or via secure network folders where everyone with access is authorized to see the data. Confidential data may only be transferred outside the college via password protected or encrypted media. You must be specifically authorized to transfer such data outside the college.

Specific examples include, but are not limited to:

- *Personnel records. – e.g., Evaluations*
- *Employee personal Information – e.g., home address, home email, home phone*

Note: Student email (personal or Green River Student Email) is not considered an internal transfer and sensitive data must be sent via encrypted email.

4. Category 4 – Confidential Information Requiring Special Handling

Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

- Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements (such as FERPA, HIPAA, or PCI-DSS)
- Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions

Confidential Information Requiring Special Handling includes employee or student information such as social security number, date of birth, etc., and information designated as Green River College FERPA level 4.

Specific examples include, but are not limited to:

- Banking/Financial Account information
- Records protected by PCI-DSS such as Credit Card Numbers
- Employee and Student Social Security Numbers
- Date of birth
- Student Identification Numbers (SID)
- Academic records of matriculated students
- Educational records protected by FERPA
- Medical records protected by HIPAA
- Medical Records, including psychological/counseling records

This category of data can be transferred internally, with appropriate care – e.g., marked in e-mail as confidential or private, or via secure network folders where everyone with access is authorized to see the data. Confidential data may only be transferred outside the agency via encrypted or password protected media. You must be specifically authorized to transfer such data outside the agency.

Information Security Program Plan (section 8.3.1,
Enterprise Backup Policies, page 56

Each Data Guardian is responsible for overseeing access to and maintenance of the indicated assets, including:

- Training and awareness programs for users with access to sensitive information.
- Authorizing access to view and/or modify data.
- Reviewing and revising respective Data Security Policy Statements.
- Reviewing the Security Program for accuracy

8.2.4 Inventory of IT Assets

Tagged IT equipment that is located at a specific user's desk is tracked as part of the general asset management of the college and assigned to that user. Shared desks have equipment assigned to the appropriate generic user e.g., "Shared Faculty". Major IT equipment like servers and network gear in the server rooms or network closets is tagged as part of the general asset management of the college, is assigned to the "IT Department" with responsibilities assigned to the Executive Director of Information Technology.

8.3 Media Handling and Disposal/Data and Program Backup

8.3.1 Enterprise Backup Policies

Green River College runs a centralized enterprise backup solution to guarantee data security. The basic characteristics of the system are:

1. The primary media are HDD-based storage devices, which employ de-duplication and compression located on campus that then replicates all changed blocks to a secure, off-site, online, hosted storage solution.
2. Centralized monitoring and reporting of backups and restores.
3. Encrypted backup/restores and storage of backups.
4. Policy based retention of backups.
5. Policy based scheduling of backups.
6. Policy applied based on system risk analysis.
7. 24-hour availability of vendor-support.
8. Automated management and tracking of primary and off-site copies and off-site storage.

Internet traffic logs are not part of the enterprise backup solution but are collected and stored by the firewall device. Data from the firewall is archived for a year on a separate HDD based repository.

The retention of data (files, web, database, server, etc.) via the enterprise backup solution is for 30 days. Data on a single server can be archived in the same manner with a single storage policy, or divided between different storage policies. Frequency of backups is based upon the data type. Presently, there are three data retention storage policies:

Green River College IT Security Program Plan

Storage Policy	Data Covered	Description
Internet Logs	All internet logs as captured by the firewall.	Backups captured daily by the firewall and then archived for a year to a separate HDD-based storage repository.
File-Web-Databases	File shares, websites, and databases servers that store business critical data.	Backups captured daily with primary and replicated copies retained for 90 days.
Semi-Static	Application servers and servers that contain data that does not change frequently and does not require long-term archiving. Backups are for disaster/program recovery.	Backups captured every other week with primary and replicated copies retained for 90 days.

In general, each storage policy requires that at a predetermined number of valid restore points exist before “pruning” any old data out of our system.

Backups are automated with “schedule policies” determined by the nature of the data and the recovery modes necessary.

Continuous replication is used for all policies requiring off-site storage.

8.3.2 Backup Media

- Initial backup targets are housed in secure facilities managed by Enterprise Services.
- Physical access to backup targets is limited to Enterprise Services staff and tightly controlled.
- Replicated backup targets are hosted in the cloud in secure locations by vendors that contract to high levels of security and tightly controlled access to their systems.

8.3.3 Media Disposal

The college has a contract with a secure destruction vendor to securely destroy and dispose of media on an ad hoc basis. All media used by Enterprise Services in a secure computer operations area is securely destroyed when it is time to be retired.

8.3.4 Telephony Backup

Daily backups to disk are performed automatically by the enterprise backup solution for the legacy PBX system.

Green River College IT Security Program Plan

The new MS Teams based VOIP telephony system is not backed up beyond the standard resiliency provided by a cloud hosted solution.

8.3.5 Voice mail Backup

Daily backups to disk are performed automatically by the enterprise backup solution for the legacy PBX voice mail system.

Copies of voice mails in the new MS Teams based VOIP telephony system are sent to the user's email inbox which automatically includes them in the email journaling mailbox.

8.3.6 Transporting Data beyond GRC Boundaries

Any media containing information protected against unauthorized access, misuse, or corruption beyond GRC campus boundaries is not allowed.

9. Electronic Commerce

9.1 E-Commerce Strategy

Green River College does not perform any E-Commerce development.

Green River College uses a third-party vendor, Elavon, to process e-commerce transactions for payments on student accounts and other miscellaneous fees. Typical charges paid on student accounts include tuition, parking fees, library fees, etc. Typical miscellaneous payments (generally made by non-students) include admission fees, and event registrations.

Green River College has chosen to outsource e-commerce in the following areas:

- The college accepts payments on student accounts and other related fees via a hosted service provided by Elavon.
- The college bookstore E-commerce site is a hosted service provided by MBS Store Technology Solutions.

Outsourcing of financial transactions is subject to approval and review of the Vice President for Business Administration. The Vice President for Business Administration ensures that a review has been performed by Enterprise Services for appropriate transaction security prior to implementation.

All credit card processing at GRC is performed by systems designed and qualified for presence on and traversal of the public Internet.

GRC policy from Catalog: Student Right to Privacy
(FERPA) (*page 9*)

Note: When numbers 900 or above are assigned, it indicates there is no specific Green River course equivalent for all or part of exam. Credit is awarded by category rather than course specific. The IB Exam for Engl B (ESL) is considered non-transferable to Green River.

Submitting Your IB Transcript

The easiest way to ensure Green River receives your IB transcript is to name Green River as a recipient when you sign up for your IB program exam(s). If you do not name Green River as a recipient when you take your exam, contact the IB Organization to request an official IB transcript be sent directly to the Green River Enrollment Services. When you are admitted to the college, you may be eligible for Green River course credit; if so, the courses and credits awarded will be accessible on your degree audit. You will be notified by email of credit awarded.

Academic Records

Student Right to Privacy (FERPA)

All student educational records are maintained according to the Family Educational Rights and Privacy Act of 1974 (FERPA). FERPA defines what is included in a student record and governs the conditions of disclosure. Students have the right to see their records and to request an amendment to those records. Students at Green River have the right to examine their educational records, and the college may not, without the student's permission, let others examine those records for other than educational purposes, per the Family Educational Rights and Privacy Act (FERPA) policy.

Directory information may include student's name, email address, photographs, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended by the student, and other similar information.

Only directory information can be released without the student's authorization. A student must sign a release in order to have any other information disclosed or to withhold all information. Education information may be released to other institutions that have requested the records and in which the student seeks or intends to enroll. Information may be released to a third party without the student's consent if an emergency situation exists or if information is requested officially by means of a subpoena, court order or legal report. Additionally, Congress requires student information to be released to military recruiters if officially requested.

More information about FERPA is available online at greenriver.edu/FERPA.

Name Changes

It is important a student's name is accurately reflected on their individual record. The Office of the Registrar maintains a confidential record of the student's last name, first name, middle initial and any previous names. It is the student's responsibility to notify the Office of the Registrar of any change.

To report a primary name change on their record, students must:

- Submit the request in writing by completing a [Student Information Change Form](#).
- Show documentation. A copy of a marriage certificate, divorce decree, adoption papers, court order or other legal documents must be attached to the request.

Students may designate a preferred name in ctcLink.

Change of Address

If your mailing address has changed, be sure to change your address in your ctcLink profile.

If you are on financial aid, you must also notify the Financial Aid Office from your Green River email address providing the new address information.

Student Identification Number

All students are assigned a ctcLink ID to use for all transactions at Green River College. Students who forget or lose their assigned ctcLink ID will need to bring picture ID into the Office of the Registrar to obtain their number.

Green River requests social security numbers at the time students make application to the college. As authorized under state law SB5509, the SSN will not be used as the student identification number that would appear on the class rosters and most other documents. Generally, the SSN is stored confidentially in the records and used only for necessary purposes as authorized by law. Those purposes include the following:

- Financial aid, including loan deferments from other colleges or universities.
- Hope scholarship and Lifelong Learning (tuition tax credits).
- Financial aid related to verification through National Student Clearinghouse.
- Workforce or unemployment data matching purposes.

Change of Program

Students planning to change their career/technical program or their intended major (if transferring to a college or university), must visit the Career and Advising Center to update their program of study and be assigned a new advisor, if appropriate.

Transcripts and Obtaining Grades

A transcript of each student's permanent record of grades is maintained in the Office of the Registrar. An official transcript of grades will be sent to any high school, college, university or other agency upon the student's request. Only grades and credits earned at Green River will post to a Green River transcript.

In order to comply with Family Educational Privacy Act 1974 (FERPA), student information (including grades) will not be released to third parties without prior written permission of the student.

Grade discrepancies must be addressed by the student with the issuing faculty member. If the issuing faculty member is no longer at Green River, contact the appropriate division chair or instructional dean.

Obtaining an unofficial transcript:

- Unofficial transcripts in ctcLink can be found on the Student Homepage, in the Academic Records tile.
- Unofficial transcripts in the Legacy system (attendance prior to 2016) must be requested through our [Unofficial Legacy Transcript Order Form](#).

Ordering an official transcript:

- Students can request an official copy of their transcript through Parchment at parchment.com. Hard copy transcripts and digital transcripts are available.
- The cost for an official transcript is \$12 per transcript request.
- Processing takes two to four business days contingent upon completion of the current quarters grading cycle.
- Students can receive their transcript immediately using our in person On-Demand form at the Office of the Registrar. The fee is \$25 per transcript.

Grading Policy

WAC 132J-276 Public Record

[Return to Chapter Listing](#)

Chapter 132J-276 WAC

Last Update: 7/13/15

PUBLIC RECORDS

WAC Sections

132J-276-010	Purpose.
132J-276-020	Definitions.
132J-276-030	Description of central and field organization of College District No. 10.
132J-276-040	Operations and procedures.
132J-276-050	Public records available.
132J-276-060	Public records officer.
132J-276-070	Office hours.
132J-276-080	Requests for public records.
132J-276-090	Copying.
132J-276-100	Exemptions.
132J-276-110	Review of denials of public records requests.
132J-276-120	Protection of public records.
132J-276-130	Records index.
132J-276-140	Adoption of form.
132J-276-900	Appendix "A"—Request for public record to College District No. 10.

132J-276-010

Purpose.

The purpose of this chapter shall be to ensure compliance by College District No. 10 with the provisions of chapter 1, Laws of 1973 (Initiative 276), Disclosure—Campaign finances—Lobbying—Records; and in particular with sections 25-32 of that act, dealing with public records.

[Statutory Authority: RCW **28B.50.140** and **34.02.353** [34.05.353]. WSR 15-15-071, § 132J-276-010, filed 7/13/15, effective 8/13/15; Order 73-2, § 132J-276-010, filed 5/14/73.]

132J-276-020

Definitions.

(1) **Public records.** "Public record" includes any writing containing information relating to the conduct of governmental or the performance of any governmental or proprietary function prepared, owned, used or retained by any state or local agency regardless of physical form or characteristics.

(2) **Writing.** "Writing means handwriting, typewriting, printing, photostating, photographing, and every other means of recording any form of communication or representation, including letters, words, pictures, sounds; or symbols, or combination thereof, and all papers, maps, magnetic or paper tapes, photographic films and prints, magnetic or punched cards, discs, drums and other documents."

(3) **College District No. 10.** College District No. 10 is an agency organized by statute pursuant to RCW **28B.50.040**. College District No. 10 shall hereinafter be referred to as the "district." Where appropriate, the term district also refers to the staff and board of trustees employees of the district.

[Statutory Authority: RCW **28B.50.140** and **34.02.353** [34.05.353]. WSR 15-15-071, § 132J-276-020, filed 7/13/15, effective 8/13/15; Order 73-2, § 132J-276-020, filed 5/14/73.]

132J-276-030

Description of central and field organization of College District No. 10.

District No. 10 is a college district organized under RCW **28B.50.040**. The administrative office of the district and its staff are located at Green River College, 12401 S.E. 320th Street, Auburn, Washington 98002.

[Statutory Authority: RCW **28B.50.140** and **34.02.353** [34.05.353]. WSR 15-15-071, § 132J-276-030, filed 7/13/15, effective 8/13/15; Order 73-2, § 132J-276-030, filed 5/14/73.]

132J-276-040

Operations and procedures.

The district is established under RCW **28B.50.040** to implement the educational purposes established by RCW **28B.50.020**. The college district is operated under the supervision and control of a board of trustees. The board of trustees is made up of five members each appointed by the governor to a term of five years. The trustees meet the third Thursday of each month at 4:00 p.m. in the administration building board room of Green River College, unless public notice is given of a special meeting. At such time the trustees exercise the powers and duties granted it under RCW **28B.50.140**.

[Statutory Authority: RCW **28B.50.140** and **34.02.353** [34.05.353]. WSR 15-15-071, § 132J-276-040, filed 7/13/15, effective 8/13/15; Order 73-2, § 132J-276-040, filed 5/14/73.]

132J-276-050**Public records available.**

All public records of the district, as defined in WAC **132J-276-020** are deemed to be available for public inspection and copying pursuant to these rules, except as otherwise provided by section 31, chapter 1, Laws of 1973 and WAC **132J-276-100**.

[Order 73-2, § 132J-276-050, filed 5/14/73.]

132J-276-060**Public records officer.**

The district's public records shall be in the charge of the public records officer designated by the college president. The person so designated shall be located in the administrative office of the district. The public records officer shall be responsible for the following: The implementation of the district's rules and regulations regarding release of public records, coordinating the staff of the district in this regard, and generally insuring compliance by the staff with the public records disclosure requirements of chapter 1, Laws of 1973.

[Order 73-2, § 132J-276-060, filed 5/14/73.]

132J-276-070**Office hours.**

Public records shall be available for inspection and copying during the customary office hours of the district. For the purposes of this chapter, the customary office hours shall be from 9:00 a.m. to noon and from 1:00 p.m. to 4:00 p.m., Monday through Friday, excluding legal holidays.

[Order 73-2, § 132J-276-070, filed 5/14/73.]

132J-276-080**Requests for public records.**

In accordance with requirements of chapter 1, Laws of 1973 that agencies prevent unreasonable invasions of privacy, protect public records from damage or disorganization, and prevent excessive interference with essential functions of the agency, public records may be inspected or copied or copies of such records may be obtained, by members of the public, upon compliance with the following procedures:

(1) A request shall be made in writing upon a form prescribed by the district which shall be available at its administrative office. The form shall be presented to the public records officer; or to any member of the district's administrative staff, if the public records officer is not available, at the administrative office of the district during customary office hours. The request shall include the following information:

(a) The name of the person requesting the record;

(b) The time of day and calendar date on which the request was made;

(c) The nature of the request;

(d) If the matter requested is referenced within the current index maintained by the records officer, a reference to the requested record as it is described in such current index;

(e) If the requested matter is not identifiable by reference to the district's current index, an appropriate description of the record requested.

(2) In all cases in which a member of the public is making a request, it shall be the obligation of the public records officer or staff member to whom the request is made, to assist the member of the public in appropriately identifying the public record requested.

[Order 73-2, § 132J-276-080, filed 5/14/73.]

132J-276-090**Copying.**

No fee shall be charged for the inspection of public records. The district shall charge a fee of 10¢ per page of copy for providing copies of public records and for use of the district's copy equipment. This charge is the amount necessary to reimburse the district for its actual costs incident to such copying. If a particular request for copies requires an unusually large amount of time, or the use of any equipment not readily available, the district will provide copies at a rate sufficient to cover any additional cost. All fees must be paid by money order, cashier's check or cash in advance.

[Order 73-2, § 132J-276-090, filed 5/14/73.]

132J-276-100**Exemptions.**

(1) The district reserves the right to determine that a public record requested in accordance with the procedures outlined in WAC **132J-276-080** is exempt under the provisions of section 31, chapter 1, Laws of 1973.

(2) In addition, pursuant to section 26, chapter 1, Laws of 1973, the district reserves the right to redact identifying details when it makes available or publishes any public record, in any cases when there is reason to believe that disclosure of such details would be an invasion of personal privacy protected by chapter 1, Laws of 1973. The public records officer will fully justify such redaction in writing.

(3) All denials of requests for public records must be accompanied by a written statement specifying the reason for the denial, including a statement of the specific exemption authorizing the withholding of the record and a brief explanation of how the exemption applies to the records withheld.

[Statutory Authority: RCW **28B.50.140** and **34.02.353** [34.05.353]. WSR 15-15-071, § 132J-276-100, filed 7/13/15, effective 8/13/15; Order 73-2, § 132J-276-100, filed 5/14/73.]

132J-276-110

Review of denials of public records requests.

(1) Any person who objects to the denial of a request for a public record may petition for prompt review of such decision by tendering a written request for review. The written request shall specifically refer to the written statement by the public records officer or other staff member which constituted or accompanied the denial.

(2) Immediately after receiving a written request for review of a decision denying a public record, the public records officer or other administrative staff member denying the request shall refer to the president of the college. The president or designee shall immediately consider the matter and either affirm or reverse such denial or consult with the attorney general to review the denial. In any case, the request shall be returned with a final decision, within two business days following the original denial.

(3) Administrative remedies shall not be considered exhausted until the district has returned the petition with a decision or until the close of the second business day following denial of inspection, whichever occurs first.

[Statutory Authority: RCW **28B.50.140** and **34.02.353** [34.05.353]. WSR 15-15-071, § 132J-276-110, filed 7/13/15, effective 8/13/15; Order 73-2, § 132J-276-110, filed 5/14/73.]

132J-276-120

Protection of public records.

Requests for public records shall be made in the administration building of Green River College. Public records and a facility for their inspection will be provided by the public records officer. Such records shall not be removed from the place designated for their inspection. Copies shall be made at Green River College. If copying facilities are not available at the college, the college will arrange to have copies made commercially according to the provisions of WAC **132J-276-090**.

[Statutory Authority: RCW **28B.50.140** and **34.02.353** [34.05.353]. WSR 15-15-071, § 132J-276-120, filed 7/13/15, effective 8/13/15; Order 73-2, § 132J-276-120, filed 5/14/73.]

132J-276-130

Records index.

(1) **Index.** The district has available to all persons a current index which provides identifying information as to the following records issued, adopted, or promulgated since June 30, 1972.

"(a) Final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases;

(b) Those statements of policy and interpretations of policy, statute and the constitution which have been adopted by the agency;

(c) Administrative staff manuals and instructions to staff that affect a member of the public;

(d) Planning policies and goals, and interim and final planning decisions;

(e) Factual staff reports and studies, factual consultant's reports and studies, scientific reports and studies, and any other factual information derived from tests, studies, reports or surveys, whether conducted by public employees or others; and

(f) Correspondence, and materials referred to therein, by and with the agency relating to any regulatory, supervisory, or enforcement responsibilities of the agency, whereby the agency determines, or opines upon, or is asked to determine or opine upon, the rights of the state, the public, a subdivision of state government, or of any private party."

(2) **Availability.** The current index promulgated by the district shall be available to all persons under the same rules and on the same conditions as are applied to public records available for inspection.

[Order 73-2, § 132J-276-130, filed 5/14/73.]

132J-276-140

Adoption of form.

The district hereby adopts for use by all persons requesting inspection and/or copying or copies of its records, the form attached herein as Appendix A [WAC **132J-276-900**], entitled "request for public record."

[Order 73-2, § 132J-276-140, filed 5/14/73.]

132J-276-900

Appendix "A"—Request for public record to College District No. 10.

APPENDIX "A"

REQUEST FOR PUBLIC RECORD TO COLLEGE DISTRICT NO. 10

(a)
Signature Signature (Please Print)
.

GA-17 Educational Rights and Privacy Act



GA-17 EDUCATIONAL RIGHTS AND PRIVACY ACT

[Home](#) / [Campus](#) / [policies-and-procedures](#) / [general-administrative-policies](#)
/ [GA-17 Educational Rights and Privacy Act](#)

Policy Type: General Administrative

Policy Title: Educational Rights and Privacy Act

Policy Number: GA-17

Scope:

All students and employees of Green River College.

Definitions:

- **Annual Notice:** The notices that the College shall provide to each Student in attendance at the College at least annually of their rights pursuant to FERPA, the procedures for exercising their rights, information about the Directory Information Exception, and the process by which a Student may elect to opt out of the release of the Student's Directory Information under that exception.
- **Consent:** Written or electronic consent, signed by the Student or otherwise verified by the Student if electronic, that is dated and specifies the specific records to be disclosed, the party to whom the records are to be disclosed, and the purpose of the disclosure.
- **De-identified Record:** An Education Record that has been stripped of all identifiers and/or aggregated such that it is not possible to re-identify an individual who is the subject of the record.
- **Directory Information:** Information in a Student's Education Record that would not generally be considered harmful or an invasion of privacy if disclosed. The following information about a Student has been designated by the State Board for Community and Technical Colleges and Green River College as Directory Information:
 - Student's name
 - Major field of study
 - Enrollment status
 - Dates of attendance
 - Participation in recognized sports

College Policies

[Board of Trustees](#)

[Business Administration](#)

[General Administrative](#)

[Information Technology](#)

[Human Resources](#)

[Instruction](#)

[Student Affairs](#)

Title IX Training Documents

Welcome to our Title IX Training Documents section, where transparency meets commitment. We proudly share comprehensive materials rooted in legal compliance and the principles of diversity, equity, and inclusion. These resources, designed for our Title IX Coordinator, are publicly accessible to promote awareness

- Degree or certificate earned
- Term degree or certificate awarded
- Honors
- **Disclosure:** To permit access to, or release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written, or electronic means, to any party except the party identified as the party that provided or created the record.
- **Dates of Attendance:** The period of time during which a student attends or attended the College, not including specific daily records of a student's attendance.
- **Education Program:** Any program that is principally engaged in the provision of education including but not limited to: postsecondary education, job training, career and technical education, and adult education, and any program that is administered by the college.
- **Education Records:** records directly related to a Student that are maintained by or on behalf of the College. Education records do not include:
 - Records of instructional, administrative, and educational personnel that are: in the sole possession of the maker (i.e. file notes of conversations); used only as a personal memory aid; not intended to be accessible or revealed to any individual except, in the case of an instructor, a temporary substitute;
 - Medical records and mental health records, including counseling records created, maintained, and used only in connection with provision of mental health treatment or counseling to the student or provision of accommodations, that are not disclosed to anyone other than the service department.
 - Employment records unrelated to the Student's status as a Student;
 - Records created or received by the College after an individual is no longer a student in attendance and that are not directly related to the individual's attendance as a student;
 - Grades on peer-graded papers before they are collected and recorded by an instructor;
 - Records maintained by the College's Campus Safety department;
 - Alumni records.
- **Personally Identifiable Information:** Information obtained from or contained in an Education Record that can be used to identify a Student to whom the record relates or another Student. It specifically includes information determined by the College to be:
 - Student's name;
 - The name of the student's parent(s) or other family members;
 - The address of the student or student's family members;
 - A personal identifier such as a student's social security number, student ID number, or biometric record;
 - Other indirect identifiers such as the student's date of birth, place of birth, or mother's maiden name;
 - Other information that, alone or in combination, is linked or linkable to a specific Student such that it would allow a reasonable person in the College community who does

and empower our community. Explore the training documents below to support our commitment to a workplace free from discrimination.

[TIX-Advisor Training](#)

[Title IX Coordinator 1-Course Slides](#)

[TIX-Day 1 Slides- Investigative Report Writing Workshop](#)

[TIX-Day 2-April Open Report Writing Workshop](#)

[TIX-Investigation 2 Day-Client Class](#)

[Title IX in a Post Reg World-Day 1](#)

[Title IX in a Post Reg World-Day 2](#)

[TIX-Hearings-Day 1 - Oregon Alliance](#)

[TIX-Hearings-Day 2- Oregon Alliance](#)

[TIX-Aug-Open Training Trauma Informed Investigations Training](#)

[TIX-Book T9 Coordinator-2 Day Client Class](#)

General Administrative Policies

- GA-1 Drug Free Campus
- GA-2 Tobacco Use
- GA-3 Mandatory Reporting of Child Abuse
- GA-4 Use of Photo Release
- GA-5 Prohibited Activities
- GA-6 Trespass
- GA-7 Distribution of Materials

not have personal knowledge of the relevant circumstances, to identify the Student with reasonable certainty; or

- Information requested by a person who the College reasonably believes knows the identity of the Student to whom the Education Record relates.

Unless the context of this policy indicated otherwise, a reference to an Education Records includes Personally Identifiable Information contained in or obtained from an Education Record.

- **Student:** An individual, regardless of age, who is or who has been in attendance at the College. For the purposes of this policy "Attendance" includes a person who has applied and been admitted, is in attendance in person, or by distance learning and the period during which a person is working in a position that requires student status, such as a under a work-study program position.
- **Authorized Representative:** Any entity or individual designated by a state or local educational authority or an agency headed by an official listed in § 99.31(a)(3) to conduct - with respect to federal- or state-supported educational programs - any audit or evaluation, or any compliance or enforcement activity in connection with federal legal requirements that relate to these programs.
- **Biometric Record:** A record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. For example: fingerprints, retina or iris patterns, voice prints, DNA sequence, facial characteristics and handwriting
- **College Official with a Legitimate Educational Interest:** Any person employed by the College in an administrative, supervisory, academic, or support staff position, including a person or company with whom the College has an affiliation or contract (such as a College attorney or auditor, or a clinical facility where a student is participating in an internship); or a person assisting another College Official in performing his or her tasks (such as a volunteer or committee member), if that person or contractor requires access to an Education Record in order to fulfill his or her official responsibilities on behalf of the College.

Policy:

The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g and 34 CFR Part 99 are federal laws and regulations that provide students with the following rights with respect to their education records:

- to inspect and review the student's education records;
 - The College shall not destroy any education records if there any outstanding requests to inspect or review aforementioned records
 - Requests by a Student for Education Records will be processed by the College no more than 45 calendar days after receiving the written request.
 - The College shall respond to reasonable requests for explanations and interpretations of the Records.
- to request amendment of the student's education records to ensure that they are not inaccurate or misleading, or otherwise in violation of the student's privacy rights under FERPA;
 - Substantive judgment of a faculty member about a student's work, expressed in grades and/or evaluations,

- GA-8 State Environmental Policy Act (SEPA)
- GA-9 Hours of Operation
- GA-10 Reasonable Accommodation
- GA-11 Sex Discrimination Grievance Procedure
 - *For incidents reported to have occurred prior to August 1, 2024.*
- GA-12 Tenure
- GA-13 Grant/Contract Proposal Development
- GA-14 Grant/Contract Procedures, Post Award
- GA-15 Human Subjects Research Compliance
- GA-16 Public Records
- GA-17 Educational Rights and Privacy Act
- GA-18 Traffic and Parking
- GA-19 Logo & Trademark Use Guidelines
- GA-21 Redevelopment of Policies
- GA-22 College Publications
- GA-23 Ethics
- GA-25 Student Email Communications
- GA-26 Social Media
- GA-27 Copyright Infringement
- GA-28 On-Campus Outdoor Memorials & Markers

is not within the purview of this right.

- to consent to disclosure of the student's education records to third parties, except to the extent that FERPA authorizes disclosure without consent;
- to be notified of the student's privacy rights under FERPA; and
- to file a complaint with the U.S. Department of Education concerning alleged failures by the College to comply with the requirements of FERPA.

Procedure:

Inspecting and Reviewing the Student's Education

Records: A Student has the right, upon request, to review all materials that are in the Student's Education Records, except:

1. Financial information submitted by the Student's parents;
2. Confidential letters and recommendations associated with admissions, employment or job placement, or honors, to which the student has waived rights of inspection and review or which were made part of the Student's Education Records prior to January 1, 1975, provided those letters were collected under established policies of confidentiality and were used only for the purposes for which they were collected;
3. Education records containing information about more than one Student, in which case the College will permit access only to that part of the record that pertains to the inquiring student; and
4. Records that are subject to an attorney-client privilege which belongs to the College.

Process for Students Requesting Access to Review Their

Education Records: The Registrar is designated as the official custodian of College's Education Records.

1. A student should submit to the Registrar a written request that identifies the record(s) the student wishes to inspect.
2. The school official will make arrangements for access and notify the student of the time and place where the records may be inspected.
3. If the records are not maintained by the school official to whom the request was submitted, that official shall advise the student of the correct official to whom the request should be addressed.

Requesting an Amendment of the Student's Education

Records: A student who wishes to request amendment of education records the student believes is inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA.

1. A student should submit to the Registrar a written request clearly identifying the part of the record the student wants changed and specify why it should be changed.
2. If Green River College decides not to amend the record as requested, the College will notify the student in writing of the decision and the student's right to a hearing regarding the request or amendment. Additional information regarding the hearing procedures will be provided to the student when notified of the right to a hearing.

Consent to Disclosure of the Student's Education Records to Third Parties:

A student may provide written consent for Green River College to disclose Personally Identifiable Information (PII) from their education records.

- GA-29 Web Policy
- GA-30 PCI DSS COMPLIANCE POLICY
- GA-31 Sex Discrimination Investigation Procedure
 - *For incidents reported to have occurred on or after August 1, 2024.*
- GA-32 Employee Sex Discrimination Disciplinary Procedure
 - *For incidents reported to have occurred on or after August 1, 2024.*
- GA-33 Pregnancy and Pregnancy Related Conditions

Exceptions: FERPA permits the disclosure of PII from a student's education record, without consent of the student, if the disclosure meets certain conditions found in § 99.31 of the FERPA regulations. These exceptions include disclosures:

1. To other school officials, including faculty, within Green River College whom the College has determined to have legitimate educational interest. This includes contractors, consultants, volunteers, or other parties to whom the College has outsourced institutional services or functions, provided the conditions listed in § 99.31 are met.
2. To officials of another school where the student seeks or intends to enroll, or where the student is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer, subject to the requirements of § 99.34.
3. To authorized representatives of the U.S. Comptroller General, the U.S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as a State postsecondary authority responsible for supervising the College's State-supported education programs, subject to the requirements of § 99.35.
4. In connection with financial aid for which the student has applied or which the student has received, if the information is necessary to determine eligibility for the aid, determine the amount of aid, determine the conditions of the aid, or enforce the terms and conditions of the aid.
5. To organizations conducting studies for, or on behalf of, the College in order to develop, validate or administer predictive tests; administer student aid programs; or improve instruction.
6. To accrediting organizations to carry out their accrediting functions.
7. To comply with a judicial order or lawfully issued subpoena.
8. To appropriate officials in connections with a health or safety emergency, subject to § 99.36.
9. Information the school has designated as "directory information" under § 99.37.
10. To a victim of an alleged perpetrator of a crime of violence or a non-forcible sex offense, subject to the requirements of § 99.39. The disclosure may only include the final results of the disciplinary proceeding with respect to that alleged crime or offense, regardless of the finding.
11. To the general public, the final results of a disciplinary proceeding, subject to the requirements of § 99.39, if the College determines the student is an alleged perpetrator of a crime of violence or non-forcible sex offense **and** the student has committed a violation of the College's rules or policies with respect to the allegation made against them.
12. To parents of a student regarding the student's violation of any Federal, State, or local law, or of any rule or policy of the College, governing the use or possession of alcohol or a controlled substance if the school determines the student committed a disciplinary violation and the student is under the age of 21.

Record of Disclosures: The College will maintain a record for each disclosure request and each disclosure of Student's Education Records, except disclosures:

1. To the student;
2. Pursuant to the written consent of the student;
3. Pursuant to the exception for School Officials with a Legitimate Educational Interest;

4. Pursuant to a law enforcement subpoena and the issuing court or other issuing agency has ordered that the existence or the contents of the subpoena or the information furnished in response to the subpoena not be disclosed or the order is concerning an authorized investigation or prosecution of domestic or international terrorism; or
5. Of Directory Information.

Notice of Rights under FERPA: The College shall provide Annual Notice to each Student of their rights under FERPA and this policy by publishing this policy in the College catalogues and by sending official notice to students via their preferred email address, as indicated in the College's student information system (ctcLink).

Filing a Complaint: Written complaints regarding alleged violations of the rights accorded students by the Federal Family Educational Rights and Privacy Act (FERPA) may be filed with the Family Policy Compliance Office, US Department of Education, 400 Maryland Avenue, S.W., Washington, D.C. 20202.

Unauthorized Disclosure:

1. Immediately upon discovery of an unauthorized disclosure of student education records or personally identifiable information contained therein, the employee or agent of the college who becomes aware of the breach should take steps to mitigate the breach and prevent any further unauthorized disclosure of information.
2. The employee or agent should notify the college's FERPA officer (the Registrar) and their immediate supervisor, as soon as possible about the breach.
3. The FERPA officer or designee will investigate the incident to determine the nature and scope of the breach, including who accessed the information and how it was disclosed.
4. The FERPA officer or designee will then take appropriate steps to address the breach, such as notifying affected individuals, reviewing and procedures, and providing additional training to the employees and agents involved in the unauthorized disclosure(s).
5. The FERPA officer or designee will maintain records of the incident, including the nature and scope of the breach, the steps taken to address the breach, and any additional actions taken to prevent future breaches.
6. If the breach is likely to result in identity theft or other harm to affected individuals the FERPA officer or designee may also notify the Department of Education.
7. The FERPA officer or designee will periodically review and revise the institution's policies and procedures to ensure ongoing compliance with FERPA regulations and to prevent future breaches.

The institution will provide annual FERPA training to all employees and agents who have access to student education records to ensure that they understand their obligations under FERPA and the institution's policies and procedures for protecting student privacy.

Specific Authority: Family Educational Rights and Privacy Act (FERPA) of 1974; 20 U.S.C. §1232g and 34 CFR Part 99

Law Implemented:

History of Policy or Procedure

Draft Date: April 5, 2023

Reviewed By: Student Affairs Leadership Team

Contact: Jenny Wheeler, director of the office of the registrar, ext 3411

Executive Team Sponsor: Sponsor: David Larsen, Dean of Enrollment and Completion, 253-833-9111, ext. 3307, dlarsen@greenriver.edu

Resources

Contact Us

STUDENT SUPPORT

- ctcLink
- Student Email
- My Green River
- Navigate 360
- Financial Aid
- Holman Library
- Center for Transformational Wellness
- Student Remote Access
- Career & Advising Center
- Office of the Registrar
- Disability Support Services
- Counseling Services
- e-Learning
- Placement & Testing Center
- Register to Vote
- MMIWP / WSP

EMPLOYEE RESOURCES

- Human Resources
- Institutional Effectiveness
- ctcLink Sign In
- GatorNet
- Curriculog (formerly CAR/PAR)
- Faculty eLearning
- Canvas
- Gator News
- Employee Password Reset

CAMPUS SAFETY

- Emergency & Safety Alerts
- Just Report It

CONNECT WITH GREEN RIVER

- [Facebook](#)
- [Twitter](#)
- [Youtube](#)
- [LinkedIn](#)
- [Instagram](#)

FERPA in GRC Webpage



FERPA

Section Menu

[Home](#) / [Students](#) / [Academics](#) / [Office of the Registrar](#) / [ferpa](#)

Family Educational Rights and Privacy Act of 1974

All student educational records are maintained according to the [Family Educational Rights and Privacy Act of 1974 \(FERPA\)](#) concerning the information, which becomes part of the student's permanent record, and governing the conditions of its disclosure. Students have the right to see their records and to request an amendment to those records.

FERPA requires Green River College, with certain exceptions, to obtain written consent prior to the disclosure of personally identifiable information from a student's education record. However, the College may disclose appropriately designated "directory information" without written consent, unless the student has advised the College to the contrary in accordance with College procedures.

Learn more about FERPA

- **Directory Information:** Provides the examples of directory information, [as defined by the State Board of Community and Technical Colleges](#).
- **Disclosure of Records:** Shares examples of when, and why, GRC may disclose personally identifiable information.
- **Educational Records:** Lists examples of the "records, files, documents, and other materials" defined by FERPA.
- **Frequently Asked Questions (FAQ):** Answers to some of the most frequently asked questions that may not have been previously covered on this page.
- **Student Rights:** Discover what rights you have over your educational record.

Resources

[Contact Us](#)

STUDENT SUPPORT

[ctcLink](#)
[Student Email](#)
[My Green River](#)
[Navigate 360](#)
[Financial Aid](#)
[Holman Library](#)

EMPLOYEE RESOURCES

[Human Resources](#)
[Institutional Effectiveness](#)
[ctcLink Sign In](#)
[GatorNet](#)

CAMPUS SAFETY

[Emergency & Safety Alerts](#)
[Just Report It](#)

CONNECT WITH GREEN RIVER

Educational Records



EDUCATIONAL RECORDS

Section Menu ▼

[Home](#) / [Students](#) / [Academics](#) / [Office of the Registrar](#) / [ferpa](#) / Educational Records

Educational Records

FERPA broadly defines education records, encompassing any "records, files, documents, and other materials" that:

- a. contain information directly related to the student; and
- b. are maintained by a school official*, an educational agency or institution, or by a person acting for such agency or institution.

These items are considered part of the student's education records:

- Admission records
- Registration activity
- Cumulative academic records
- Transcript
- Class assignments
- Records of attendance
- Grades or Grade Point Average
- Test scores
- Financial Aid records
- Disciplinary records
- Documentation of special services students receive
- other similar information/records

The following are specifically excluded from the definition of education records by FERPA:

- Records of instructional, supervisory and administrative personnel which are in the sole possession of the maker thereof. (i.e. used only as a personal memory aid; are not accessible or revealed to any other person)
- Records generated and maintained by a physician, psychiatrist, psychologist or other recognized professional paraprofessional acting in his/her capacity.
- Records maintained by a law enforcement unit of the educational institution that were created for the purpose of law enforcement.
- Records relating to an individual who is employed by the institution other than as a result of his/her student status.

- Records created or received by an educational institution after an individual is no longer a student in attendance and that are not directly related to the individual's attendance as a student.
- Grades on peer-graded papers before they are collected and recorded by a teacher.

Education records can be in the form of, but not limited to:

- Handwriting
- Print
- Magnetic Tapes
- Film
- Microfilm
- Microfiche
- Computer media
- Video or audio tape

* "School official" is defined by Green River as any employee of the College acting on behalf of the College with a legitimate educational interest in the student.

* "Legitimate education interest" is defined by Green River as a school official needing to review an educational record in order to fulfill their professional responsibility.

Resources

Contact Us

STUDENT SUPPORT

- ctcLink
- Student Email
- My Green River
- Navigate 360
- Financial Aid
- Holman Library
- Center for Transformational Wellness
- Student Remote Access
- Career & Advising Center
- Office of the Registrar
- Disability Support Services
- Counseling Services
- e-Learning
- Placement & Testing Center
- Register to Vote
- MMIWP / WSP

EMPLOYEE RESOURCES

- Human Resources
- Institutional Effectiveness
- ctcLink Sign In
- GatorNet
- Curriculog (formerly CAR/PAR)
- Faculty eLearning
- Canvas
- Gator News
- Employee Password Reset

CAMPUS SAFETY

- Emergency & Safety Alerts
- Just Report It

CONNECT WITH GREEN RIVER

- Facebook**
- Twitter**
- Youtube**
- LinkedIn**
- Instagram**

Privacy

Select Language

[Current Students](#)[Faculty & Staff](#)[Give to GRC](#) [Quick Links](#)

PRIVACY

AT GREEN RIVER COLLEGE

 Section Menu ▾[Home](#) / [Privacy](#)

Privacy Notice

Section A. Introduction

Thank you for visiting the Green River College Web site and reviewing our Privacy Notice. This statement addresses collection, use and security of and access to information that may be obtained through use of Green River College. This notice covers the following topics:

- Information Collected and How it is Used
- Personal Information and Choice
- Public Access to Information
- Nondisclosure of Certain Personal Information

- Review and Correction of Personally Identifiable Information
- Cookies and applets
- Security
- Disclaimer
- Contact Information

Section B. Information Collected and How it is Used

If you do nothing during your visit to our website but browse, read pages, or download information, we will gather and store certain information about your visit. This information does not identify you personally. We automatically collect and store the following information about your visit:

1. The Internet Protocol Address and domain name used. The Internet Protocol address is a numerical identifier assigned either to your Internet service provider or directly to your computer. We use the Internet Protocol Address to direct Internet traffic to you. This address can be translated to determine the domain name of your service provider (e.g. xcompany.com or yourschool.edu);
2. The type of browser and operating system you used;
3. The date and time you visited this site;
4. The Web pages or services you accessed at this site; and
5. The website you visited prior to coming to this website.

The information we automatically collect or store is logged and used by Green River College only to improve the content of our Web services and to help us understand how people are using our services. Green River College analyzes the Web site logs to determine how our Web site is being used, so that we may continually improve the site's usefulness to the public.

What we collect if you volunteer information

If during your visit to our website you participate in a survey, send an email, or perform some other transaction on-line, the following additional information will be collected:

1. The email address, and contents of email, for those who communicate with us via email.
2. Information volunteered in response to a survey.

3. Information volunteered through an on-line form for any other purpose.

The information collected is not limited to text characters and may include audio, video, and graphic information formats you send us.

We use your email to respond appropriately. This may be to respond to you, to address issues you may identify, to further improve our Web site, or to forward the email to another agency for appropriate action. Survey information is used to gather data on specific topics relevant to the college. Information from other on-line forms is used only for the purpose stated on the form.

Section C. Personal Information and Choice

You may choose whether to provide personal information on-line.

“Personal information” is information about a natural person that is readily identifiable to that specific individual. Personal information includes such things as an individual's name, address, and phone number. A domain name or Internet Protocol address is not considered personal information.

We collect no personal information about you unless you voluntarily provide it to us by sending us email, participating in a survey, or completing an online form. You may choose not to contact us by email, participate in a survey or to provide any personal information using an online form. Your choice to not participate in these activities will not impair your ability to browse the Green River College Web site and read or download any information provided on the site.

If personal information is requested on the Web site or volunteered by the user, state law and the federal Privacy Act of 1974 may protect it. However, this information is a public record once you provide it, and may be subject to public inspection and copying if not protected by federal or state law.

If you believe that your personal information is being used for a purpose other than what was intended when submitted, you may contact the Green River College Office of Public Information as shown in the Contact Information Section of this statement.

Green River College's Web site is a general audience site and we do not knowingly collect any personal information from children. Users are cautioned that the collection of personal information requested from or volunteered by children online or by email will be treated the same as information given by an adult, and may be subject to public access.

Section D. Public Access to Information

In the State Of Washington, laws exist to ensure that government is open and that the public has a right to access appropriate records and information possessed by state government. At the same time, there are exceptions to the public's right to access public records that serve various needs including the privacy of individuals. Exceptions are provided by both state and federal laws.

All of the information collected at this site becomes public records that may be subject to inspection and copying by members of the public, unless an exemption in law exists. [RCW 42.56.070](#) states that:

Each agency, in accordance with published rules, shall make available for public inspection and copying all public records, unless the record falls within the specific exemptions of the Public Records Act or other statute which exempts or prohibits disclosure of specific information or records.

To the extent required to prevent an unreasonable invasion of personal privacy interests protected by RCW 42.56.210 and [42.56.320](#), an agency shall delete identifying details in a manner consistent with [RCW 42.56.210](#) and RCW 42.56.320 when it makes available or publishes any public record; however, in each case, the justification for the deletion shall be explained fully in writing.

In the event of a conflict between this Privacy Notice and the Public Records Act or other law governing the agency's disclosure of records, the Public Records Act or other applicable law will control.

Section E. Nondisclosure of Certain Personal Information

Green River College may require you to provide certain personal information in order to pay tuition and fees online. The information is required in order to verify your identity and to verify your credit card number and its expiration date. You may choose not to provide this

information, but if you choose not to provide it we will be unable to apply tuition and fee payment online, and you will have to pay your tuition and fees in person.

The following laws and regulations may prevent Green River College from disclosing the personal information about you except for directory information. Only directory information can be released without student's authorization. Students must sign a release in order to have any other information disclosed or to withhold all information. Education information may be released to other institutions that have requested the records and in which the student seeks or intends to enroll. Information may be released to a third party without student's consent if an emergency situation exists or if information is requested officially by means of a subpoena, court order or legal report. Additionally, Congress requires student information to be released to military recruiters if officially requested. Directory information may include student's name, address, telephone number, date and place of birth, major fields of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended by the student, and other similar information.<.p>

- **Family Educational Rights and Privacy Act of 1974 (FERPA)** Section 438, Public Law 90-247 Title IV, as amended, 88 Stat 571-574 (20 USC 1232g) otherwise known as the Buckley Amendment Family Educational Rights and Privacy Act
- **RCW 42.17.310** (a) and (ss) exempts the following from public inspection and copying: (a) Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients; (ss) Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers supplied to an agency for the purpose of electronic transfer of funds, except when disclosure is expressly required by law

Degree Audit

Green River College may require you to provide certain personal information in order to perform a degree audit of your records over the Web. The information is required in order to verify your identity. You may choose not to provide this information, but if you choose not to provide it

we will be unable to display a degree audit of your records over the Web, and you will have to request a degree audit in person or by mail.

The following laws and regulations may prevent Green River College from disclosing the personal information about you except for directory information. Only directory information can be released without student's authorization. Students must sign a release in order to have any other information disclosed or to withhold all information. Education information may be released to other institutions that have requested the records and in which the student seeks or intends to enroll. Information may be released to a third party without student's consent if an emergency situation exists or if information is requested officially by means of a subpoena, court order or legal report. Additionally, Congress requires student information to be released to military recruiters if officially requested. Directory information may include student's name, address, telephone number, date and place of birth, major fields of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended by the student, and other similar information.

- **Family Educational Rights and Privacy Act of 1974 (FERPA)** Section 438, Public Law 90-247 Title IV, as amended, 88 Stat 571-574 (20 USC 1232g) otherwise known as the Buckley Amendment Family Educational Rights and Privacy Act
- **RCW 42.17.310** (a) and (ss) exempts the following from public inspection and copying: (a) Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients; (ss) Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers supplied to an agency for the purpose of electronic transfer of funds, except when disclosure is expressly required by law

Financial Aid Inquiry

Green River College may require you to provide certain personal information in order to obtain your financial aid status over the Web. The information is required in order to verify your identity. You may choose not to provide this information, but if you choose not to provide it we will be unable to give you your financial aid status over the Web, and you will have to obtain this information in person or by mail.

The following laws and regulations may prevent Green River College from disclosing the personal information about you except for directory information. Only directory information can be released without student's authorization. Students must sign a release in order to have any other information disclosed or to withhold all information. Education information may be released to other institutions that have requested the records and in which the student seeks or intends to enroll. Information may be released to a third party without student's consent if an emergency situation exists or if information is requested officially by means of a subpoena, court order or legal report. Additionally, Congress requires student information to be released to military recruiters if officially requested. Directory information may include student's name, address, telephone number, date and place of birth, major fields of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended by the student, and other similar information.

- **Family Educational Rights and Privacy Act of 1974 (FERPA)** Section 438, Public Law 90-247 Title IV, as amended, 88 Stat 571-574 (20 USC 1232g) otherwise known as the Buckley Amendment Family Educational Rights and Privacy Act
- **RCW 42.17.310** (a) and (ss) exempts the following from public inspection and copying: (a) Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients; (ss) Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers supplied to an agency for the purpose of electronic transfer of funds, except when disclosure is expressly required by law

Hope and Lifetime Learning Tax Credit

Green River College may require you to provide certain personal information in order to allow you to view and copy course enrollment and payment information. The information is required in order to provide you with the tax information needed for compliance with the Internal Revenue Service reporting requirements for the Hope and Lifetime Learning tax credits. You may choose not to provide this information, but if you choose not to provide it, we will be unable to display your

enrollment and payment information and you will have to obtain a copy of your enrollment and payment records either in person or by mail.

The following laws and regulations may prevent Green River College from disclosing the personal information about you except for directory information. Only directory information can be released without student's authorization. Students must sign a release in order to have any other information disclosed or to withhold all information. Education information may be released to other institutions that have requested the records and in which the student seeks or intends to enroll. Information may be released to a third party without student's consent if an emergency situation exists or if information is requested officially by means of a subpoena, court order or legal report. Additionally, Congress requires student information to be released to military recruiters if officially requested. Directory information may include student's name, address, telephone number, date and place of birth, major fields of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended by the student, and other similar information.

- **Family Educational Rights and Privacy Act of 1974 (FERPA)** Section 438, Public Law 90-247 Title IV, as amended, 88 Stat 571-574 (20 USC 1232g) otherwise known as the Buckley Amendment Family Educational Rights and Privacy Act
- **RCW 42.17.310** (a) and (ss) exempts the following from public inspection and copying: (a) Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients; (ss) Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers supplied to an agency for the purpose of electronic transfer of funds, except when disclosure is expressly required by law

Registration

Green River College may require you to provide certain personal information in order to register for classes over the Web. The information is required in order to verify your identity. You may choose not to provide this information, but if you choose not to provide it you will be unable to register for classes over the Web, and you will have to register for classes in person

The following laws and regulations may prevent Green River College from disclosing the personal information about you except for directory information. Only directory information can be released without student's authorization. Students must sign a release in order to have any other information disclosed or to withhold all information. Education information may be released to other institutions that have requested the records and in which the student seeks or intends to enroll. Information may be released to a third party without student's consent if an emergency situation exists or if information is requested officially by means of a subpoena, court order or legal report. Additionally, Congress requires student information to be released to military recruiters if officially requested. Directory information may include student's name, address, telephone number, date and place of birth, major fields of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended by the student, and other similar information.

- **Family Educational Rights and Privacy Act of 1974 (FERPA)** Section 438, Public Law 90-247 Title IV, as amended, 88 Stat 571-574 (20 USC 1232g) otherwise known as the Buckley Amendment Family Educational Rights and Privacy Act
- **RCW 42.17.310** (a) and (ss) exempts the following from public inspection and copying: (a) Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients; (ss) Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers supplied to an agency for the purpose of electronic transfer of funds, except when disclosure is expressly required by law

Registration Appointments

Green River College may require you to provide certain personal information in order to obtain your registration appointment information over the Web. The information is required in order to verify your identity. You may choose not to provide this information, but if you choose not to provide it we will be unable to display your registration appointment information over the Web, and you will have to obtain your registration appointment information address in person or by mail.

The following laws and regulations may prevent Green River College from disclosing the personal information about you except for directory information. Only directory information can be released without student's authorization. Students must sign a release in order to have any other information disclosed or to withhold all information. Education information may be released to other institutions that have requested the records and in which the student seeks or intends to enroll. Information may be released to a third party without student's consent if an emergency situation exists or if information is requested officially by means of a subpoena, court order or legal report. Additionally, Congress requires student information to be released to military recruiters if officially requested. Directory information may include student's name, address, telephone number, date and place of birth, major fields of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended by the student, and other similar information.

- **Family Educational Rights and Privacy Act of 1974 (FERPA)** Section 438, Public Law 90-247 Title IV, as amended, 88 Stat 571-574 (20 USC 1232g) otherwise known as the Buckley Amendment Family Educational Rights and Privacy Act
- **RCW 42.17.310** (a) and (ss) exempts the following from public inspection and copying: (a) Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients; (ss) Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers supplied to an agency for the purpose of electronic transfer of funds, except when disclosure is expressly required by law

Schedule Planner

Green River College may require you to provide certain personal information in order to check requisites while using schedule planner. The information is required in order to access your academic and testing records. You may choose not to provide this information, but if you choose not to provide it we will be unable to verify your eligibility for enrollment into certain classes and you may be blocked from enrolling into those classes.

The following laws and regulations may prevent Green River College from disclosing the personal information about you except for directory information. Only directory information can be released without student's authorization. Students must sign a release in order to have any other information disclosed or to withhold all information. Education information may be released to other institutions that have requested the records and in which the student seeks or intends to enroll. Information may be released to a third party without student's consent if an emergency situation exists or if information is requested officially by means of a subpoena, court order or legal report. Additionally, Congress requires student information to be released to military recruiters if officially requested. Directory information may include student's name, address, telephone number, date and place of birth, major fields of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended by the student, and other similar information.

- **Family Educational Rights and Privacy Act of 1974 (FERPA)** Section 438, Public Law 90-247 Title IV, as amended, 88 Stat 571-574 (20 USC 1232g) otherwise known as the Buckley Amendment Family Educational Rights and Privacy Act
- **RCW 42.17.310** (a) and (ss) exempts the following from public inspection and copying: (a) Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients; (ss) Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers supplied to an agency for the purpose of electronic transfer of funds, except when disclosure is expressly required by law

Student Address Change

Green River College may require you to provide certain personal information in order to change your address over the Web. The information is required in order to verify your identity. You may choose not to provide this information, but if you choose not to provide it we will be unable to change your address over the Web, and you will have to change your address in person or by mail.

The following laws and regulations may prevent Green River College from disclosing the personal information about you except for directory

information. Only directory information can be released without student's authorization. Students must sign a release in order to have any other information disclosed or to withhold all information. Education information may be released to other institutions that have requested the records and in which the student seeks or intends to enroll. Information may be released to a third party without student's consent if an emergency situation exists or if information is requested officially by means of a subpoena, court order or legal report. Additionally, Congress requires student information to be released to military recruiters if officially requested. Directory information may include student's name, address, telephone number, date and place of birth, major fields of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended by the student, and other similar information.

- **Family Educational Rights and Privacy Act of 1974 (FERPA)** Section 438, Public Law 90-247 Title IV, as amended, 88 Stat 571-574 (20 USC 1232g) otherwise known as the Buckley Amendment Family Educational Rights and Privacy Act
- **RCW 42.17.310** (a) and (ss) exempts the following from public inspection and copying: (a) Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients; (ss) Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers supplied to an agency for the purpose of electronic transfer of funds, except when disclosure is expressly required by law

Student PIN Change

Green River College may require you to provide certain personal information in order to change your personal identification number over the Web. The information is required in order to verify your identity. You may choose not to provide this information, but if you choose not to provide it we will be unable to change your PIN over the Web, and you will have to change your PIN in person or by mail.

The following laws and regulations may prevent Green River College from disclosing the personal information about you except for directory information. Only directory information can be released without student's authorization. Students must sign a release in order to have any other

information disclosed or to withhold all information. Education information may be released to other institutions that have requested the records and in which the student seeks or intends to enroll. Information may be released to a third party without student's consent if an emergency situation exists or if information is requested officially by means of a subpoena, court order or legal report. Additionally, Congress requires student information to be released to military recruiters if officially requested. Directory information may include student's name, address, telephone number, date and place of birth, major fields of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended by the student, and other similar information.

- **Family Educational Rights and Privacy Act of 1974 (FERPA)** Section 438, Public Law 90-247 Title IV, as amended, 88 Stat 571-574 (20 USC 1232g) otherwise known as the Buckley Amendment Family Educational Rights and Privacy Act
- **RCW 42.17.310** (a) and (ss) exempts the following from public inspection and copying: (a) Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients; (ss) Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers supplied to an agency for the purpose of electronic transfer of funds, except when disclosure is expressly required by law

Student Schedule

Green River College may require you to provide certain personal information in order to view your quarterly schedule. The information is required in order to verify your identity. You may choose not to provide this information, but if you choose not to provide it we will be unable to display your quarterly schedule over the Web, and you will have to obtain a copy of your quarterly schedule in person or by mail.

The following laws and regulations may prevent Green River College from disclosing the personal information about you except for directory information. Only directory information can be released without student's authorization. Students must sign a release in order to have any other information disclosed or to withhold all information. Education information may be released to other institutions that have requested the

records and in which the student seeks or intends to enroll. Information may be released to a third party without student's consent if an emergency situation exists or if information is requested officially by means of a subpoena, court order or legal report. Additionally, Congress requires student information to be released to military recruiters if officially requested. Directory information may include student's name, address, telephone number, date and place of birth, major fields of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended by the student, and other similar information.

- **Family Educational Rights and Privacy Act of 1974 (FERPA)** Section 438, Public Law 90-247 Title IV, as amended, 88 Stat 571-574 (20 USC 1232g) otherwise known as the Buckley Amendment Family Educational Rights and Privacy Act
- **RCW 42.17.310** (a) and (ss) exempts the following from public inspection and copying: (a) Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients; (ss) Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers supplied to an agency for the purpose of electronic transfer of funds, except when disclosure is expressly required by law

Unofficial Transcript

Green River College may require you to provide certain personal information in order to view your unofficial transcript over the Web. The information is required in order to verify your identity. You may choose not to provide this information, but if you choose not to provide it we will be unable to display your unofficial transcript over the Web, and you will have to view your unofficial transcript in person or by mail.

The following laws and regulations may prevent Green River College from disclosing the personal information about you except for directory information. Only directory information can be released without student's authorization. Students must sign a release in order to have any other information disclosed or to withhold all information. Education information may be released to other institutions that have requested the records and in which the student seeks or intends to enroll. Information may be released to a third party without student's consent if an

emergency situation exists or if information is requested officially by means of a subpoena, court order or legal report. Additionally, Congress requires student information to be released to military recruiters if officially requested. Directory information may include student's name, address, telephone number, date and place of birth, major fields of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, the most recent previous educational agency or institution attended by the student, and other similar information.

- **Family Educational Rights and Privacy Act of 1974 (FERPA)** Section 438, Public Law 90-247 Title IV, as amended, 88 Stat 571-574 (20 USC 1232g) otherwise known as the Buckley Amendment Family Educational Rights and Privacy Act
- **RCW 42.17.310** (a) and (ss) exempts the following from public inspection and copying: (a) Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients; (ss) Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers supplied to an agency for the purpose of electronic transfer of funds, except when disclosure is expressly required by law.

Section F. Review and Correction of Personally Identifiable Information

You can review any personally identifiable information we collect about you by using the information in the Contact Information section at the end of this Notice. You may recommend changes to your personally identifiable information you believe to be inaccurate by submitting an email or written request that credibly shows the inaccuracy. We will take reasonable steps to verify your identity before granting access or making corrections. ([RCW 43.105.310](#))

Section G. Cookies [and applets]

To better serve our users we are now using "cookies" to customize your browsing experience with the Green River College Web site. Cookies are simple text files stored on your computer by your Web browser.

Cookies created on your computer by using this Web site do not contain personally identifying information and do not compromise your privacy or

security. We use the cookie feature to store to store the following information on your computer:

1. Session login information
2. Limited personal information, such as name

Section H. Security

Green River College, as developer and manager of the Green River College Web site, has taken several steps to safeguard the integrity of its data and prevent unauthorized access to information maintained by Green River College. [For site security purposes and to ensure that this Web site remains available to all users, Green River College employs software to monitor traffic to identify unauthorized attempts to upload or change information or otherwise cause damage to this Web site.] These measures are designed and intended to prevent corruption of data, block unknown or unauthorized access to our systems and information, and to provide reasonable protection of private information in our possession.

This information should not be construed in any way as giving business, legal, or other advice, or warranting as fail proof, the security of information provided via Green River College Web sites.

Section I. Disclaimer

The Green River College Web site has many links to other Web sites. These include links to Web sites operated by other government agencies, nonprofit organizations and private businesses. When you link to another site, you are no longer on the Green River College Web site and this Privacy Notice will not apply. When you link to another Web site, you are subject to the privacy policy of that new site.

Reference in this Web site to any specific commercial products, processes, or services, or the use of any trade, firm, or corporation name is for the information and convenience of the public, and does not constitute endorsement, recommendation, or favoring by the State of Washington, Green River College, or its officers, employees or agents.

Neither the State of Washington, nor any agency, officer, or employee of the State of Washington warrants the accuracy, reliability or timeliness of any information published by this system, nor endorses any content, viewpoints, products, or services linked from this system, and shall not be held liable for any losses caused by reliance on the accuracy,

reliability or timeliness of such information. Portions of such information may be incorrect or not current. Any person or entity that relies on any information obtained from this system does so at its own risk.

Green River College reserves the right to revise and update this Privacy Notice at any time without notice by posting such revised Privacy Notice at the Green River College home page.

Section J. Green River College Contact Information

You may contact Green River College as follows:

To review your personal information, or request correction of your personal information:

Public Information Office
Green River College
12401 SE 320th Street
Auburn, WA 98092
Fax: 253-288-3444
Phone: [253-288-3361](tel:253-288-3361)

Resources

Contact Us

STUDENT SUPPORT

ctcLink
Student Email
My Green River
Navigate 360
Financial Aid
Holman Library
Center for
Transformational

EMPLOYEE RESOURCES

Human
Resources
Institutional
Effectiveness
ctcLink Sign In
GatorNet
Curriculog
(formerly

CAMPUS SAFETY

Emergency &
Safety Alerts
Just Report It

CONNECT WITH GREEN RIVER

Facebook
Twitter